THE COMMON FRAMEWORK:
Overview and Principles
The members of Connecting for Health passionately believe that the private and secure exchange of health information nationwide is essential to the well-being of patients and those who care for them. It has been nearly two years since we published the “Roadmap” report—*Achieving Electronic Connectivity in Healthcare: A Preliminary Roadmap from the Nation’s Public and Private Sector Healthcare Leaders*. Today we take a step further with release of the Common Framework.

The *Roadmap* sketched a bold vision of nationwide health information exchange through a decentralized network of networks united by a “Common Framework” of shared policies and technical standards. The report was groundbreaking not only in its practical vision that put patient privacy first, but also in the diversity of stakeholders that participated in its development. Our members overcame sometimes contradictory viewpoints to find shared solutions to problems that have remained intractable for decades. More than 50,000 copies of the *Roadmap* are now in circulation.

In early 2005 we broadened and deepened the *Roadmap* vision by collaborating on a joint response to a Request for Information issued by the Federal Office of the National Coordinator with an even more diverse group of 13 influential organizations in addition to the 100 or so members of the Steering Group. Through these efforts our vision and words gained greater clarity and reach than we had dreamed possible. But we were determined not to stop at words.

Within the last year we have built a working prototype of the *Roadmap* model—together we have learned how three very different communities, with different hardware, software, and organizational structures, can in fact share information in a private and secure way over the Internet using a Common Framework. Our partners in Mendocino County, CA, Indianapolis, and Boston worked closely with a Connecting for Health Technical Subcommittee and Policy Subcommittee made up of more than 75 people drawn from the Connecting for Health Steering Group plus other recognized experts. The Subcommittees helped to shape and test the prototype, documented the lessons of its implementation, and drafted a first iteration of the Common Framework, which we are releasing today. Although it is just a start, we are confident that it will evolve to meet the needs of a varied and fragmented healthcare system. We invite others to use, adapt, and help us to improve the Common Framework.

As Connecting for Health has been constructing a prototype and Common Framework, several complementary developments have taken place, building on the ongoing efforts of local communities: new communities for health information exchange are forming with great speed, Federal and State governments have put an unprecedented spotlight on the importance of health information technology, the Department of Health and Human Services and the Office of the National Coordinator have provided their leadership and millions of dollars toward a connected healthcare system, and Congress has sponsored many initiatives—all designed to further health information sharing.

Despite these efforts, the road ahead remains long and the precise path is uncertain; we must chart its course together. Connecting for Health and its many partners from across the professions, industry, and the patient community will continue to enable the private, secure, and nationwide exchange of health information. We remain committed to this goal because we know that access to reliable, relevant information where and when it’s needed is essential to the improvement of healthcare safety, efficiency, and quality. A new infrastructure for health information sharing will also provide the foundation for a transformed, 21st century healthcare system in which patients and families can better understand their own health and engage more fully in their care through direct access to their own health information.

---

**A Statement on the Common Framework**

from Members of the Connecting for Health Steering Group:

The members of Connecting for Health passionately believe that the private and secure exchange of health information nationwide is essential to the well-being of patients and those who care for them. It has been nearly two years since we published the “Roadmap” report—*Achieving Electronic Connectivity in Healthcare: A Preliminary Roadmap from the Nation’s Public and Private Sector Healthcare Leaders*. Today we take a step further with release of the Common Framework.

The *Roadmap* sketched a bold vision of nationwide health information exchange through a decentralized network of networks united by a “Common Framework” of shared policies and technical standards. The report was groundbreaking not only in its practical vision that put patient privacy first, but also in the diversity of stakeholders that participated in its development. Our members overcame sometimes contradictory viewpoints to find shared solutions to problems that have remained intractable for decades. More than 50,000 copies of the *Roadmap* are now in circulation.

In early 2005 we broadened and deepened the *Roadmap* vision by collaborating on a joint response to a Request for Information issued by the Federal Office of the National Coordinator with an even more diverse group of 13 influential organizations in addition to the 100 or so members of the Steering Group. Through these efforts our vision and words gained greater clarity and reach than we had dreamed possible. But we were determined not to stop at words.

Within the last year we have built a working prototype of the *Roadmap* model—together we have learned how three very different communities, with different hardware, software, and organizational structures, can in fact share information in a private and secure way over the Internet using a Common Framework. Our partners in Mendocino County, CA, Indianapolis, and Boston worked closely with a Connecting for Health Technical Subcommittee and Policy Subcommittee made up of more than 75 people drawn from the Connecting for Health Steering Group plus other recognized experts. The Subcommittees helped to shape and test the prototype, documented the lessons of its implementation, and drafted a first iteration of the Common Framework, which we are releasing today. Although it is just a start, we are confident that it will evolve to meet the needs of a varied and fragmented healthcare system. We invite others to use, adapt, and help us to improve the Common Framework.

As Connecting for Health has been constructing a prototype and Common Framework, several complementary developments have taken place, building on the ongoing efforts of local communities: new communities for health information exchange are forming with great speed, Federal and State governments have put an unprecedented spotlight on the importance of health information technology, the Department of Health and Human Services and the Office of the National Coordinator have provided their leadership and millions of dollars toward a connected healthcare system, and Congress has sponsored many initiatives—all designed to further health information sharing.

Despite these efforts, the road ahead remains long and the precise path is uncertain; we must chart its course together. Connecting for Health and its many partners from across the professions, industry, and the patient community will continue to enable the private, secure, and nationwide exchange of health information. We remain committed to this goal because we know that access to reliable, relevant information where and when it’s needed is essential to the improvement of healthcare safety, efficiency, and quality. A new infrastructure for health information sharing will also provide the foundation for a transformed, 21st century healthcare system in which patients and families can better understand their own health and engage more fully in their care through direct access to their own health information.
## Members of the Connecting for Health Steering Group

<table>
<thead>
<tr>
<th>Name</th>
<th>Affiliation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carol Diamond, MD, MPH</td>
<td>Markle Foundation, (Chair)</td>
</tr>
<tr>
<td>Daniel Garrett, Computer</td>
<td>Sciences Corporation’s Global Health Solutions Practice, (Vice Chair)</td>
</tr>
<tr>
<td>John R. Lumpkin, MD, MPH</td>
<td>Robert Wood Johnson Foundation, (Vice Chair)</td>
</tr>
<tr>
<td>Herbert Pardes, MD</td>
<td>New York-Presbyterian Hospital, (Vice Chair)</td>
</tr>
<tr>
<td>Peter A. Andersen, MD</td>
<td>Lockheed Martin Information Technology</td>
</tr>
<tr>
<td>Zoë Baird,</td>
<td>Markle Foundation, (ex-officio)</td>
</tr>
<tr>
<td>Robert Bogin, MD</td>
<td>American Cancer Society</td>
</tr>
<tr>
<td>William Braithwaite, MD</td>
<td>eHealth Initiative, (Co-Chair, Policy Subcommittee)</td>
</tr>
<tr>
<td>Claire Broome*, MD</td>
<td>Centers for Disease Control and Prevention</td>
</tr>
<tr>
<td>Gary Christopherson*,</td>
<td>Centers For Medicare and Medicaid Services</td>
</tr>
<tr>
<td>Carolyn Clancy*, MD</td>
<td>Agency for Healthcare Research and Quality, United States Department of Health and Human Services</td>
</tr>
<tr>
<td>Janet Corrigan, PhD</td>
<td>National Committee for Quality Health Care</td>
</tr>
<tr>
<td>Mike Cummins, VHA Inc.</td>
<td></td>
</tr>
<tr>
<td>Francois de Brantes, PhD</td>
<td>Bridges To Excellence and Prometheus</td>
</tr>
<tr>
<td>Mary Jo Deering*, PhD</td>
<td>National Cancer Institute/ National Institutes of Health, United States Department of Health and Human Services</td>
</tr>
<tr>
<td>David A. Epstein, IBM Software Group</td>
<td></td>
</tr>
<tr>
<td>Colin Evans, Intel Corporation</td>
<td></td>
</tr>
<tr>
<td>Mark Frisse, MD, MBA, MSc</td>
<td>Vanderbilt Center for Better Health, (Co-Chair, Policy Subcommittee)</td>
</tr>
<tr>
<td>J. Peter Geerlofs, MD</td>
<td>Allscripts Healthcare Solutions</td>
</tr>
<tr>
<td>John Glaser, PhD, Partners</td>
<td>HealthCare System</td>
</tr>
<tr>
<td>John Halamka, MD, CareGroup</td>
<td>Healthcare System</td>
</tr>
<tr>
<td>Linda Harris*, PhD</td>
<td>National Cancer Institute/National Institutes of Health, United States Department of Health and Human Services</td>
</tr>
<tr>
<td>Joseph Heyman, MD, MD</td>
<td>American Medical Association</td>
</tr>
<tr>
<td>Yin Ho, MD, Pfizer, Inc.</td>
<td></td>
</tr>
<tr>
<td>Kevin Hutchinson,</td>
<td>SureScripts</td>
</tr>
<tr>
<td>Michael Jackman, Eastman</td>
<td>Kodak Company</td>
</tr>
<tr>
<td>William F. Jessee, MD</td>
<td>Medical Group Management Association</td>
</tr>
<tr>
<td>Y. Michele Kang,</td>
<td>Northrop Grumman Corporation</td>
</tr>
<tr>
<td>Michael L. Kappel,</td>
<td>McKesson Provider Technologies</td>
</tr>
<tr>
<td>Brian Keaton, MD, FACEP</td>
<td>American College of Emergency Physicians</td>
</tr>
<tr>
<td>Linda Kloss, RHIA, CAE</td>
<td>American Health Information Management Association</td>
</tr>
<tr>
<td>Allan Korn, MD, FACP</td>
<td>Blue Cross/Blue Shield Association</td>
</tr>
<tr>
<td>David Lansky, PhD,</td>
<td>Markle Foundation, (Chair, Personal Health Technology Council)</td>
</tr>
<tr>
<td>Gail Latimer, MSN, RN</td>
<td>Siemens Corporation</td>
</tr>
<tr>
<td>Jack Lewin, MD, California</td>
<td>Medical Association</td>
</tr>
<tr>
<td>Stephen Lieber, CAE</td>
<td>Healthcare Information and Management Systems Society</td>
</tr>
<tr>
<td>Patricia MacTaggart, EDS</td>
<td>Executive State and Local Government</td>
</tr>
</tbody>
</table>
Janet M. Marchibroda, eHealth Initiative
Howard Messing, Meditech
Arnold Milstein, MD, MPH, The Leapfrog Group
Margaret O’Kane, National Committee for Quality Assurance
Dennis O’Leary, MD, Joint Commission on Accreditation of Healthcare Organizations
J. Marc Overhage, MD, PhD, Indiana Health Information Exchange; Indiana University School of Medicine, Regenstrief Institute for Healthcare
Alison Rein, National Consumers League
Russell J. Ricci, MD, HealthSTAR Communications
Craig Richardson, Johnson and Johnson Health Care Systems, Inc.
Wes Rishel, Gartner Group
William Rollow*, MD, Centers for Medicare and Medicaid Services, United States Department of Health and Human Services
David Schulke, The American Health Quality Association
Steve Shihadeh, Microsoft Corporation
Clay Shirky, New York University, (Chair, Technical Subcommittee)
Steve Sleigh, PhD, International Association of Machine and Aerospace Workers
Ellen Stovall, National Coalition for Cancer Survivorship
Thomas Sullivan, MD, Women’s Health Center Cardiology, AMA-Council on Medical Service, DrFirst.com
Paul Tang, MD, Palo Alto Medical Foundation, American Medical Informatics Association
Randy L. Thomas, IBM Corporation
Robin Thomashauer, Council for Affordable Quality Healthcare
John Tooker, MD, MBA, FACP, American College of Physicians
Micky Tripathi, Massachusetts eHealth Collaborative
Charlene Underwood, Healthcare Information and Management Systems Society, EHR Vendor Association
Scott Wallace, The National Alliance for Health Information Technology
Andrew Wiesenthal, MD, The Permanente Federation
Robert B. Williams, MD, MIS, Deloitte
Rochelle Woolley, RxHub
Hugh Zettel, GE Healthcare Integrated IT Solutions

* Note: Federal employees participate in the Steering Group but make no endorsement.
Many people are enthusiastic about the benefits of using information technology (IT) to manage health information—and rightly so. Prompt, reliable access to health information can improve the quality and efficiency of care, and even save lives. But it is not enough for a single hospital or doctor’s office to use computers to access a patient’s information only from its own internal records. Most patients’ health information is scattered across many facilities—the offices of numerous current and former physicians, labs, pharmacies, and imaging centers. Whether for routine care or in an emergency far from home, patients and their formal and informal caregivers need access to this distributed web of information in order to make well-informed medical decisions. At the same time, the movement of personal health information through a vast electronic network calls for a profound new commitment to protecting each person’s privacy.

One set of obstacles to widespread health information exchange is technical. The United States health system is extremely diverse and highly fragmented. In addition, participants in the system, which encompasses large hospital networks, individual doctors, labs, and others, use a variety of types of computers and software to store patient information, or none at all. Some information systems can’t communicate with others because they lack standard ways of transporting and presenting information.

Another set of obstacles to widespread health information exchange has to do with policy—particularly privacy concerns. Many surveys have shown that Americans are very worried about the privacy of their health information, and for good reason. Inappropriate access to health information can result in discrimination, social embarrassment, or worse. Making any type of information easier to share by storing and exchanging it electronically may increase the risk that it ends up in the wrong hands.

Unfortunately, there is no failsafe answer to the policy problems associated with sharing health information. It is impossible to guarantee 100 percent the privacy of health information—even if it stays in paper files. Similarly, there is no perfect solution to all of the technical challenges. To compound matters, some proposals that provide...
advantages from a technical perspective—such as creating one massive database to hold health information for every American, or giving each person a new ID number for health records—lack practicality and can exacerbate privacy risks.

The Common Framework grew out of the efforts of Connecting for Health—a public-private collaborative led by the Markle Foundation—to find realistic and consistent solutions to the technical and policy challenges associated with health information exchange. Connecting for Health has emphasized the necessity of addressing critical policy and technical questions in parallel and considering both from the outset.

If we are to share health information in a way that is trusted and effective, the policies that establish who has access to health information, what uses of information are acceptable, the extent to which patients can give or withhold access to their information, and the design of privacy and security safeguards must all be crafted in parallel with the design and deployment of the technology. And the technology choices themselves must incorporate policy objectives that protect patients and our society’s values.

The Big Picture—How the Common Framework Works on a Nationwide Basis

The concept underlying the Connecting for Health approach is that information exchange can take place among existing and future health care networks over the Internet if all participants adhere to a small set of shared rules—a “Common Framework” of technical and policy guidelines. The Common Framework recognizes that some information exchange networks are defined regionally—among trusted and well-known local partners, and others may be national in scope (such as a network of pharmacies) or based on other business relationships (such as a network of cancer centers). We call any network that agrees to conform to the Common Framework a “sub-network organization”—indicating that it constitutes one element of the larger network of networks scattered across the nation. The Common Framework is based upon common, non-proprietary technical and policy standards that can work with the information systems already in place, regardless of the particular hardware and software being used. General adherence to this small set of critical requirements will permit rapid attainment of widespread information sharing in support of modern healthcare practice.

The Common Framework approach is desirable from a technical perspective because it enables the establishment of health information exchange by building on rather than replacing existing infrastructure. Because it does not dictate technology choices, it allows great latitude for innovation and for tailoring health information exchange networks to meet diverse needs. It is desirable from a policy perspective because its design protects patients’ privacy. Personal health information remains in the hands of those who collect it: doctors, hospitals, labs, pharmacies, and others. In each health infor-
mation exchange network, an index called a Record Locator Service lets clinicians find out where the patient information they seek is stored so that they can request it directly from its source. Patients and the doctors they trust can decide with whom to share personal health information, and for what purposes.

The key to this approach is the articulation of a small, but necessary set of nationally uniform technical and policy guidelines that every organization that wants to share health information can adopt. The Common Framework is the embodiment of that essential core.

From Principles to Practice—How the Common Framework Has Evolved

Connecting for Health is a collaborative of more than 100 leading private and public organizations, including experts in clinical medicine, information technology, public policy, and patient privacy. The collaborative is led by the Markle Foundation and funded by both Markle and the Robert Wood Johnson Foundation. Its members are committed to bringing about the nationwide sharing of health information for the benefit of patients and those who treat and support them.

The members of Connecting for Health have worked together for several years to tackle some of the most intractable barriers to widespread information sharing. In 2004 the collaborative issued its influential "Roadmap" report, Achieving Electronic Connectivity in Healthcare: A Preliminary Roadmap from the Nation’s Public and Private-Sector Healthcare Leaders (available at: http://www.connectingforhealth.org/resources/cfh_aech_roadmap_072004.pdf). The Roadmap defined a set of policy and implementation constraints that any architecture for health information sharing had to meet—for one, its design had to protect the privacy and security of personal health information. The Connecting for Health Steering Group identified a small number of additional constraints, including the idea that any solution must build on existing infrastructure rather than requiring completely new technologies or information systems (“no rip and replace”). It also sought to define a model of health information exchange that could be demonstrated within one to three years. These objectives led Connecting for Health to avoid proposals that would require large scale disruption or be dependent on large up-front capital investments. Instead, we sketched out a model of nationwide health information exchange that is decentralized, can be achieved without requiring a new unique patient identifier, is capable of working with any underlying hardware and software, and is therefore governed by a small set of technical and policy standards called the Common Framework.

This theoretical model described in the Roadmap was a step forward, but the Connecting for Health Steering Group pressed for a demonstrable test in real world communities engaged in health information exchange. In late 2004, in cooperation with local partners, Connecting for Health embarked on development of a three-state prototype of electronic health information exchange based on the Common Framework in Mendocino County, CA, Indianapolis, and Boston. Within a year this effort successfully exchanged electronic health information both within and among the three sites. The prototype is based on common, open, non-proprietary standards and on the establishment of robust policies to protect the privacy and security of patient information.

Development of the prototype occurred over a period of 18 months in lockstep with the interdependent work of two Connecting for Health Subcommittees—one focused on Technology, the other on Policy. Some of the most highly regarded experts in the nation grappled with the challenges of translating the Roadmap's principles into practice. They collaborated closely with experts in the three sites to both develop and document solutions to problems and the thinking behind them for the benefit of other communities working on health information exchange. An important concept articulated by the Roadmap and proven in the field is that decisions about technical architecture must be guided by policy objectives—not the other way around. Moreover, policy objectives must be considered at the beginning of any technical undertaking. The Connecting for Health Common Framework: Resources for Health Information Exchange is the first product of these efforts. It represents just the initial phase of a continuous process of discovery, discussion, and fieldwork.
Openness and Transparency
There should be a general policy of openness about developments, practices, and policies with respect to personal data. Individuals should be able to know what information exists about them, the purpose of its use, who can access and use it, and where it resides.

Purpose Specification and Minimization
The purposes for which personal data are collected should be specified at the time of collection, and the subsequent use should be limited to those purposes or others that are specified on each occasion of change of purpose.

Collection Limitation
Personal health information should only be collected for specified purposes, should be obtained by lawful and fair means and, where possible, with the knowledge or consent of the data subject.

Use Limitation
Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified.

Individual Participation and Control
Individuals should control access to their personal information:
- Individuals should be able to obtain from each entity that controls personal health data, information about whether or not the entity has data relating to them.
- Individuals should have the right to:
  - Have personal data relating to them communicated within a reasonable time (at an affordable charge, if any), and in a form that is readily understandable;
  - Be given reasons if a request (as described above) is denied, and to be able to challenge such denial; and
  - Challenge data relating to them and have it rectified, completed, or amended.

Data Integrity and Quality
All personal data collected should be relevant to the purposes for which they are to be used and should be accurate, complete, and current.

Security Safeguards and Controls
Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure.

Accountability and Oversight
Entities in control of personal health data must be held accountable for implementing these information practices.

Remedies
Legal and financial remedies must exist to address any security breaches or privacy violations.
Connecting for Health’s Technology Principles

**Make it “Thin”**
Only the minimum number of rules and protocols essential to widespread exchange of health information should be specified as part of a Common Framework. It is desirable to leave to the local systems those things best handled locally, while specifying at a national level those things required as universal in order to allow for exchange among subordinate networks.

**Avoid “Rip and Replace”**
Any proposed model for health information exchange must take into account the current structure of the healthcare system. While some infrastructure may need to evolve, the system should take advantage of what has been deployed today. Similarly, it should build on existing Internet capabilities, using appropriate standards for ensuring secure transfer of information.

**Separate Applications from the Network**
The purpose of the network is to allow authorized persons to access data as needed. The purpose of applications is to display or otherwise use that data once received. The network should be designed to support any and all useful types of applications, and applications should be designed to take data in from the network in standard formats. This allows new applications to be created and existing ones upgraded without re-designing the network itself.

**Decentralization**
Data stay where they are. The decentralized approach leaves clinical data in the control of those providers with a direct relationship with the patient, and leaves judgments about who should and should not see patient data in the hands of the patient and the physicians and institutions that are directly involved with his or her care.

**Federation**
The participating members of a health network must belong to and comply with agreements of a federation. Federation, in this view, is a response to the organizational difficulties presented by the fact of decentralization. Formal federation with clear agreements builds trust that is essential to the exchange of health information.

**Flexibility**
Any hardware or software can be used for health information exchange as long as it conforms to a Common Framework of essential requirements. The network should support variation and innovation in response to local needs. The network must be able to scale and evolve over time.

**Privacy and Security**
All health information exchange, including in support of the delivery of care and the conduct of research and public health reporting, must be conducted in an environment of trust, based upon conformance with appropriate requirements for patient privacy, security, confidentiality, integrity, audit, and informed consent.

**Accuracy**
Accuracy in identifying both a patient and his or her records with little tolerance for error is an essential element of health information exchange. There must also be feedback mechanisms to help organizations to fix or “clean” their data in the event that errors are discovered.
These technology and policy principles guided the specific, practical decisions about the architecture, specifications, and policies that support private and secure sharing of health information across the nation. From these, Connecting for Health has developed a skeletal framework of technology and policy guides; at this early stage, we have only put flesh on a few of the bones.

**With regard to technical guides:**
- We have provided documentation for the Record Locator Service and the Inter-SNO (sub-network organization) Bridge—the only novel pieces of infrastructure we propose. The Record Locator Service forms the basis of a decentralized model and describes the architectural elements needed for sharing information within communities. The Inter-SNO Bridge provides the architecture for sharing information among communities or sub-networks.
- We have documented clinical data exchange for two “use cases” only: retrieving a patient’s medication history and retrieving a patient’s laboratory results. Other use cases and guides will continue to stress test and evolve the model and will need to be developed and published in the future.

**With regard to policy guides:**
- The Connecting for Health Policy Subcommittee developed a list of significant topics based on its members’ experience with early information exchange networks and their own expertise in law, health privacy, health care delivery, administration, and technology. The Subcommittee developed recommended policies in each area of significant concern. The Subcommittee’s work assumes underlying compliance with both HIPAA and existing state laws; its work looked at health information exchange in the context of this already existing structure for protecting health privacy.
- As with the technical work, the Policy Subcommittee’s work is in no way comprehensive. In many areas, the Subcommittee recognized the need for further policy development but felt it important to establish a foundational consensus on key principles before tackling more complex issues; in other areas, the Subcommittee simply did not have time to conduct the necessary research and build consensus. The development of necessary policies will need to continue alongside the evolution of technical work.

**With regard to model contractual language:**
- We have distinguished those issues which need to be addressed uniformly across all health information exchanges from those that can be evaluated and implemented according to local preference. Connecting for Health has developed a “Model Contract for Health Information Exchange” that offers a business framework for leveraging national standards while accommodating local needs.

Following is a schematic of the Common Framework resources, followed by a brief description of each of them.
Policy Guides: How Information is Protected

The Architecture for Privacy in a Networked Health Information Environment—A foundational policy architecture for privacy and health information technology in a networked environment, based on nine principles. The Connecting for Health approach dictates that these nine principles be balanced together and considered as part of one package—elevating certain principles over others will weaken any overall architectural solution to privacy protection in a networked health information environment.

Model Privacy Policies and Procedures for Health Information Exchange—Model privacy policies designed as a starting point for those working to establish sub-network organizations that will utilize a Record Locator Service. The policies establish baseline privacy protections designed to apply to all individuals receiving care from an institution participating in a SNO. The model policies and procedures are intended to accompany and complement the “Model Contract for Health Information Exchange.” Issues addressed in the document include, inter alia, policies regarding acceptable uses and disclosures of individual health care information, ensuring individual participation in and control of their health information, and how to handle individual health information that may be subject to special protections.

Correctly Matching Patients with Their Records—A review of methods for optimizing the likelihood of finding as many of a patient’s records as possible through the Record Locator Service, while minimizing false matches. False matches, in which records associated with one patient are erroneously linked to another patient, can result in “incidental disclosures” of information, which compromise patient privacy. The policies addressed also include whether and how such incidental disclosures should be handled under the Connecting for Health Common Framework.

Authentication of System Users—Recommended approaches for sub-network organization (SNO) participants to establish user identity for the purpose of access to health information sharing networks.

Patients’ Access to Their Own Health Information—The discussion includes a review of the state of the current law on individuals’ access to their own health care information and then makes recommendations regarding such policies in the context of a Record Locator Service and a health information sharing environment.

Auditing Access to and Use of a Health Information Exchange—The advantages and disadvantages of audit logs, some criteria for successful audit logs, and issues that sub-network organizations should consider in implementing successful audit systems.

Breaches of Confidential Health Information—Recommended policies for addressing breaches in confidentiality of personal health information.
The Common Framework: Technical Issues and Requirements for Implementation — A high-level description of the technical philosophy embodied in the Connecting for Health prototype. This document discusses the basic design principles adopted by Connecting for Health, the technical constraints governing the work, what subsequent choices were made, and why those choices were made.

Health Information Exchange: Architecture Implementation Guide — The core technical document, governing the message standards required for exchange of Common Framework-compliant messages between participating entities within a sub-network organizations (SNO), and exchange of messages between entities in different SNOs. This document covers the design of the standard messages used in network communication, as well as the operation names used to invoke the required services, and the design of the Patient Identification segment used in queries for patient data. In addition, access to the technical code and test servers created for the prototype is available through www.connectingforhealth.org/commonframework/prototypes.html. In order to make the basic workings of the prototype visible, we have provided the source code, related files, and test servers developed in each of the three Connecting for Health prototype sites.

Connecting for Health, in collaboration with the participating sites, has left the test servers available for those who would like to experiment with formatting valid queries and parsing the results. In addition, each region is making the source code used to handle the incoming queries available for download from the same server hosting the test interface.

Medication History Standards—The standards for expressing a patient’s medication history. The exchange of medication history was one of two use cases tested in the prototype; we adopted a version of the National Council for Prescription Drug Programs (NCPDP) proposed standard. There is considerable work on medication history standards, and we anticipate that there will be future changes to this standard in the near term. Because the Common Framework maintains a separation between data description and transport, updates to the medication history standard will not require re-engineering the network to accommodate the new standard.

Background Issues on Data Quality — A review of the issues raised by dirty, incomplete, and inaccurate healthcare data, and mechanisms that could be developed and implemented to address these issues. This framework also describes the importance of establishing accountability among those responsible for the reliability of data.

Laboratory Results Standards—Describes desired future changes to the Laboratory Results Standard to make it more compatible with a multi-use networked environment. Includes a web link to the Laboratory Results Standard used in exchanges of data in the prototype test (proposed ELINCS 2.0 standard). There is considerable work on lab results standards, and we anticipate that there will be future changes to this standard in the near term. Because the Common Framework maintains a separation between data description and transport, updates to the lab results standard will not require re-engineering the network to accommodate the new standard.

Record Locator Service: Technical Background from the Massachusetts Prototype Community — Discussion of the technical and design issues of the Record Locator Service, as constructed in Massachusetts. Provides background on the initial technical conversations; the current state of the architecture is documented in “The Common Framework: Technical Issues and Requirements for Implementation” and “Health Information Exchange: Architecture Implementation Guide.”
Model Contractual Language

Key Topics in a Model Contract for Health Information Exchange—A brief overview of the elements covered in the full “Model Contract for Health Information.” It is intended to provide a general approach to the issues that health information sharing networks must address to increase the likelihood of success of their own electronic health information exchanges.

A Model Contract for Health Information Exchange—A model contractual agreement containing sample language and descriptive notes regarding issues that both regional and affinity-based networks must address to increase the likelihood of success of their own electronic health information exchanges. The Model addresses such contractual topics as the implementation of user agreements, general disclaimers, insurance requirements, and enforcement requirements.

The Model is intended to assist in the organization of a sub-network organization by providing a basis upon which to begin drafting that sub-network organization’s Terms and Conditions. All language provided in the Model is intended for illustrative purposes only. Each sub-network organization will have to draft its Terms and Conditions based upon its own organization, operations, system and services, regulatory environment, etc. Some of the Model’s terms will be inapplicable to some sub-network organizations. The Model shows where some of these variations might be expected to occur.
Connecting for Health is a large collaborative of volunteers and staff who have achieved an enormous task in this first release of the Common Framework. The technical and policy aspects of the Common Framework were developed by two dedicated Subcommittees that worked tirelessly to find common ground on solutions to the tough challenges associated with this work. Without the leadership provided by the Subcommittee Chairs, Clay Shirky, Bill Braithwaite, and Mark Frisse, it could not have been accomplished. We extend our thanks also to the Connecting for Health staff, especially to David Lansky, Lygeia Ricciardi, Jennifer De Pasquale, and Stuart Schear. We appreciate their insights and ability to coordinate and convey the value of our complex work with alacrity. We also recognize Melissa Goldstein, who managed the large body of policy work, painstakingly attending to every detail.

Please share your suggestions and feedback with us at: www.connectingforhealth.org.
The Architecture for Privacy in a Networked Health Information Environment
The Architecture for Privacy in a Networked Health Information Environment
The document you are reading is part of *The Connecting for Health Common Framework*, which is available in full and in its most current version at: [http://www.connectingforhealth.org/](http://www.connectingforhealth.org/). The Common Framework will be revised and expanded over time. As of October 2006, the Common Framework included the following published components:
The Architecture for Privacy in a Networked Health Information Environment*

Executive Summary

Introduction and Overview
A networked health information-sharing environment has the potential to enable decision support anywhere at any time, improving public and individual health, and reducing cost. Consumers and patients can benefit directly when their personal information is available to health care providers, and indirectly when their information is available in the aggregate to researchers seeking new ways to prevent, manage, or cure health problems. At the same time, the potential benefits must be weighed against the risks of privacy and security violations, which may increase if not addressed at the outset.

The accompanying document begins from the premise that any new health network needs to take into account the potential for such violations, and to build privacy and information security into its architecture from the outset, not as an afterthought. The document provides background on the issues at stake, explains the current status of health privacy, considers new challenges and opportunities in an electronic environment, and offers some solutions for a comprehensive response to those challenges.

I. What is at Stake?
The paper begins by examining why privacy matters, both in an online and offline environment. It first considers privacy as a matter of individual liberty, autonomy, and even a fundamental human right. All these perspectives remain applicable in a health context, but in addition, breaches of confidentiality are harmful because they can lead to so-called “privacy protective behavior,” in which patients avoid seeking health care in order to protect their personal information. Such behavior has a toll on both individual health and, more generally, on public health. It suggests just one important reason why we need to build confidentiality and security into a networked environment.

II. Health Privacy: Definitions and Underlying Concepts
This section considers the concept of privacy, both as it applies to a general environment and more specifically to the medical context. It begins by considering the historical evolution of the term. In 1890, Samuel Warren and Louis Brandeis famously argued that privacy should be defined as “the right to be let alone.” Today, definitions tend more closely to resemble Alan Westin’s notion of “informational privacy,” which suggests that the concept should be understood as an individual’s right to control personal information.

Such a definition is particularly important in a global information age, and this section identifies two considerations that are repeatedly voiced regarding the handling of medical data. The first concerns the almost unlimited uses for medical information. Data gathered in a medical context and used for other purposes, it is argued, poses serious privacy risks. The second concern emphasizes the benefits that can be accrued through medical data. This section points to these tremendous benefits, and argues that, while confidentiality of information is essential, patients may miss out on some of the benefits if data controls in the name of confidentiality over-restrict the uses and dissemination of information. The solution is to find a balance between the potential harms and the potential benefits represented by medical

* Connecting for Health thanks Stefaan Verhulst, Chief of Research, Markle Foundation, for drafting this paper.

©2006, Markle Foundation
This work was originally published as part of The Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange and is made available subject to the terms of a license (License) which may be viewed in its entirety at: http://www.connectingforhealth.org/license.html. You may make copies of this work; however, by copying or exercising any other rights to the work, you accept and agree to be bound by the terms of the License. All copies of this work must reproduce this copyright information and notice.
data. That balance can be achieved through a careful deployment of appropriate technologies, combined with strong laws and other forms of confidentiality protection.

III. Health Privacy in a Digital Health Information Networked Environment: What is Different?
This section argues that existing notions of medical privacy are somewhat outdated in a networked health information exchange environment. It discusses six risks increased by such an environment, arguing that these risks require new and innovative solutions. While some of these risks exist in an offline world, they have become more pronounced, in large part due to the scale of data transactions and the relatively greater ease of collecting, linking, and disseminating information over a network, and to a reduced ability to “leave the past behind” and to shield sensitive information. Among the increased risks include:

1. **Commercial misuses of data**, including the use of medical data to deny or restrict insurance coverage; restrict credit or other financial benefits; or in unsolicited marketing;
2. **Government misuses of data**, including secondary use of personal health information by government agencies (for employment and other purposes) and the need to balance national security with health privacy considerations;
3. **Criminal misuses of data**, including fraudulent acts that result in financial or other harm;
4. **Security breaches**, including hacking and other criminal activities that lead to “data leakage”;
5. **Data quality issues**, including data corruption and loss; and
6. **Harmful social consequences**, including stigma, exposure, and embarrassment.

IV. Defining a Comprehensive Privacy Architecture: Establishing Trust in the Network
This section defines some principles for responding to the above risks and protecting medical privacy in a networked environment. It begins by discussing existing privacy protection principles adopted in the United States, the Organisation for Economic Co-operation and Development (OECD), and Canada. It then argues for the following nine principles:

1. **Openness and Transparency**
2. **Purpose Specification and Minimization**
3. **Collection Limitation**
4. **Use Limitation**
5. **Individual Participation and Control**
6. **Data Integrity and Quality**
7. **Security Safeguards and Controls**
8. **Accountability and Oversight**
9. **Remedies**

Together, these nine principles amount to a comprehensive privacy protective architecture that can—and should—be applied in a networked environment.

V. Current Laws and Guidelines and How They Integrate an Architectural Approach
This section includes a brief overview of existing privacy protection laws in the United States. It begins by discussing federal protections, and in particular protections built into the Health Insurance Portability and Accountability Act of 1996 (HIPAA). It then discusses the patchwork of state laws, pointing out that these generally fall into three categories: constitutional protections, common law protections, and statutory protections. Finally, it discusses the emergence of, and potential difficulties and opportunities posed by, new community based health networks.

VI. Conclusion
The conclusion offers a summary of the preceding discussion. In particular, it revisits the nine principles and argues that they need to be considered together, as part of an integrated and comprehensive approach to medical privacy.
Introduction and Overview

As we move towards the creation of a health information environment, the potential for privacy intrusions increases, with potentially devastating impact on quality and access to health care. Any up-front planning should take privacy and security into consideration. This paper starts from the belief that it is possible—and necessary—to build privacy into health information technology (HIT) applications so that its benefits can be maximized. It aims to provide background on what is at stake, what has already been achieved in health privacy, what makes the current environment different, and how to provide for a comprehensive response. The paper provides for nine privacy architectural principles that should guide the design of policies, practices, and technologies to protect privacy in a networked environment. In addition it briefly provides an overview of current attempts to address the privacy and security issues within the context of a networked health information environment.

I. What is at Stake?

Individual Liberty and Autonomy: An International Approach

In many countries and treaties, privacy is considered a fundamental right, equivalent to other basic individual liberties such as freedom of speech and thought. Both the United Nations Declaration of Human Rights and the International Covenant on Civil and Political Rights, for example, recognize the right to privacy. In these treaties, privacy is recognized as a form of autonomy, a way to ensure protection from “arbitrary interference” by the state or other entities. In addition, several broad, international principles exist that have been adopted (and adapted) by a variety of countries. For example, as we shall see, in its 1995 Directive on Protection of Personal Data, the Organisation for Economic Co-operation and Development (OECD) led the way in defining several principles for privacy protection. The European Union (EU) and other countries have subsequently adopted these. Interestingly, this directive differs significantly from the US approach in that it takes a broad, omnibus approach to privacy protection rather than the sector and often state specific approaches adopted in the United States.

Understood in this broad way, as a fundamental human right, a violation of privacy can be considered a serious violation of an individual’s basic rights, equivalent, perhaps, to imprisonment without trial or the denial of free expression. Naser and Alpert (1999) point out that this violation is particularly serious in a medical context, where patients are often already somewhat helpless and in a position of dependence. They write: “When patients ... disclose intimate secrets about themselves they also become more vulnerable. Patients who are ill already have a diminished sense of autonomy” (22). In such instances, robbing individuals of their privacy is tantamount to a serious violation of their individual liberty.

Privacy Protective Behavior in a Medical Context

In addition to a violation of individual rights, the loss of privacy in a medical context has other negative consequences, some of which can be understood as collective harms. Social scientists have frequently established that surveillance, not just in the medical field, but across fields, can have a “chilling effect” on individual behavior (Alpert 2003; Goffman 1966; Westin 1967). In the medical field, this chilling effect can lead to what experts call “privacy protective behavior” (Goldman 1998, 49). Such behavior includes hiding evidence of pre-existing conditions from doctors or insurance companies; paying out-of-pocket for treatment; or simply avoiding treatment altogether.

Goldman, in a paper on the importance of medical privacy, lists four negative consequences of such privacy protective behavior (Goldman 1998, 49):

---

1 United Nations, Universal Declaration of Human Rights, Article 12. Available at: h\t\t\t\tp://www.nps.gov/elro/teach-er-vk/documents/udhr.htm.

2 The EU Directives mentioned above similarly treat medical violations of privacy as particularly egregious cases.
The patient may receive poor-quality care, risking undetected and untreated conditions.

The doctor's abilities to diagnose and treat accurately are jeopardized by a lack of complete and reliable information from the patient.

A doctor may skew diagnosis or treatment codes on claim forms, keep separate records for internal uses only, or send incomplete information for claims processing to encourage a patient to communicate more fully.

The integrity of the data flowing out of the doctor’s office may be undermined. The information the patient provides, as well as the resulting diagnosis and treatment, may be incomplete, inaccurate, and not fully representative of the patient's care or health status.

Survey Evidence
These negative consequences are not mere hypotheticals. A large number of surveys over the years have consistently shown that the public is concerned about breaches in confidentiality, and that “privacy protective behavior” is a very real phenomenon. For example, as reported by Janeli and Hudson (141), a 2000 survey of Internet users found that 75 percent of respondents were worried that health sites shared information without consent; and that a full 17 percent would not seek health information on the web due to privacy concerns. Another poll, also conducted in 2000, found that 61 percent of Americans felt that “too many people have access to their medical records.”

Overall, concern about privacy seems to have increased over time: while a Harris Interactive Inc. poll conducted in 1978 found that 64 percent of respondents were concerned about privacy, a similar poll conducted in 1995 by Harris found the number had increased to 82 percent (Goldman 1998, 50).

The surveys also show that such concerns frequently lead to privacy protective behavior. For example, in a survey conducted by the California HealthCare Foundation, more than one out of six adults said they had done something “out of the ordinary” to hide private medical information (Alpert 305). In another survey conducted by Harris in 1993, 11 percent of respondents said they sometimes chose not to file an insurance claim, and 7 percent said they sometimes neglected to seek care in order to avoid damaging their “job prospects or other life opportunities” (Goldman 1998, 50).

Such behaviors do not just cause potential damage to an individual patient's health. They also impose a collective burden, leading to greater costs and public health problems that an already overstretched health system can ill-afford.

II. Health Privacy: Definitions and Underlying Concepts
Understanding the concept of privacy is essential to designing better policies, practices, and technologies to protect consumer and individual privacy. The trouble, however, as one observer points out, is that “privacy is a notoriously vague, ambiguous, and controversial term that embraces a confusing knot of problems, tensions, rights, and duties” (Bennett 1992, 11-12). In an effort to lay the foundations for our following discussion of policies and principles, this section attempts to provide a certain amount of conceptual clarity to the idea of privacy.

Privacy as a General Concept
One of the earliest definitions of privacy was published in 1890, in a Harvard Law Review article by Samuel Warren and Louis Brandeis. In that article, entitled “The Right to Privacy,” Warren and Brandeis argued that privacy could be defined as “the right to be let alone.” The article was drafted in response to concerns over the potential privacy violations that would occur as a result of a new technology. Warren and

---

3 These and more survey results can be found at: http://www.epic.org/privacy/survey/.

4 While much of this discussion refers to broad federal approaches to privacy, it is essential to recognize that privacy protections in the United States have been far more localized and sector-specific. Indeed, the states, not the federal government, have generally led the way in protecting privacy.
Brandeis were writing about the modern press, and particularly the instantaneous photograph, which they felt invaded “the sacred precincts of private and domestic life.”

More than 100 years later, we continue to grapple with difficult problems surrounding privacy, and once again, the concern is largely driven by technology. The now-classic definition of privacy in the information age was supplied by Alan Westin, who in his 1967 book, Privacy and Freedom, argued that: “Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others” (7).

Westin’s definition of privacy is probably the most prevalent, and widely-accepted, today. It is sometimes referred to as “informational privacy,” and it is easy to see why this notion of privacy would have particular relevance in the digital era. In 1971, Harvard professor Arthur Miller predicted that all individuals would eventually be the subjects of a “womb-to-tomb dossier.” Westin himself argued that, in the information era, every individual was accompanied by a “data shadow” which could reveal even the most intimate and apparently mundane details about his or her life.

**Privacy is Not a Static Concept**

Such a data shadow, if it indeed materialized, could seriously threaten individual privacy and, by extension, a host of other liberties that citizens in modern Western democracies take for granted. Michael Froomkin, for example, has predicted the “death of privacy.” It is important to recognize that the notion of privacy is not static. It changes with time, as the evolution from Warren and Brandeis’ concept to Westin’s definition makes clear; and it changes depending on the field or environment to which it is applied. This means that privacy is a malleable concept; its treatment and protection can be changed to suit public concerns. In the following sections of this paper, we show how certain protections can be established in response to current concerns over privacy. First, it is important to understand how the concept of privacy is context-sensitive. It is sensitive to particular historical moments. In a more recent article, Westin argues that post-war understandings of privacy have undergone four distinct phases (2003, 434). These include:

- A Privacy Baseline Phase, which ran from 1945 to 1960, and was marked by a relative inattention to, and lack of concern regarding, privacy issues;
- The First Era of Contemporary Privacy Development (1961-1979), which for the first time “marked the rise of information privacy as an explicit social, political, and legal issue”;
- The Second Era of Privacy Development (1980-1989), which continued some of the concern begun in the First Era, but overall, “can be seen now as a period of relative calm before the storm”;
- And finally, the Third Era of Privacy Development (1990-2002), which “is the period when privacy became a first-level social and political issue in the United States, assumed global proportions, and was impacted by 9/11 and its aftermath.”

**Privacy and Health**

In addition to these well-defined periods, privacy can also be applied to a range of distinct issues; it is sensitive, too, to the field or realm within which it is applied. National security, commerce, and fraud all have privacy dimensions. Although many of these may overlap, there might also be some differences. It is therefore useful to spend some time on the trajectory of privacy as a medical concern. This is particularly important because, as Westin points out, health plays a critical role in his Third Era. Indeed, Westin explicitly points to the rise of genetic testing and the possibility of electronic health records as concerns in this new era (2003, 442).

Although health may have risen to the top of the privacy agenda in recent years, it has long been a topic for privacy advocates and policymakers. As pointed out in a recent report...
by the Health Privacy Working Group, an initiative, comprised of diverse health care stakeholders (plans, providers, accreditors, and scholars), located at Georgetown University and directed by the Health Privacy Project, national attention to medical privacy can be traced back at least to 1973, when "there were calls for increased attention to the privacy concerns presented by the use of computers in the health care industry" (10).6 Janlori Goldman also points out that the guidelines and codes of practice developed by the US Department of Health, Education, and Welfare in 1973 continue to serve as the underpinnings for a variety of privacy laws across sectors, suggesting the central role always occupied by concerns over medical privacy (1999, 103). The Privacy Protection Study Commission, created by the Privacy Act, expressed some of those concerns in 1977. "It appears," wrote the Commission, "that the importance of medical-record information to those outside of the medical-care relationship, and their demands for access to it, will continue to grow ... There appears to be no natural limit to the potential uses of medical-record information for purposes quite different from those for which it was originally collected." 7

In these and other discussions of health as a privacy concern, at least two distinct themes can be identified. The first, pointed out by Sheri Alpert in a wide-ranging review of the literature on medical privacy, is evident in the above quote, and particularly in the Privacy Protection Study Commission's concern that "there appears to be no natural limit" to the uses of private medical data. As Alpert puts it, there is a recurring concern in the literature over the potential "harm that can befall patients if their medical information is disclosed either in ways that exceed their expectations or if information reaches the hands of people who should not have access to it" (Alpert, 304). She cites a number of authors expressing concern over such potential misuse, and argues that the primary purpose for a patient's personal health information is—and should be—"the clinical diagnosis, treatment, and care of that patient" (305).

The second recurring theme is somewhat contradictory. It provides a counter-argument to Alpert's point, emphasizing the tremendous potential benefits that can be accrued through medical data. Briefly, it is anticipated that the use of medical data, particularly when enabled by electronic health records, has the potential to transform the way patients receive care, and to introduce a far greater degree of efficiency and effectiveness in our nation's medical care system.

Individuals recognize these potential benefits. The same surveys that reveal concern over privacy also show that people are eager to exploit the potential benefits of new technologies. A study conducted by Foundation for Accountability (FACCT) for Connecting for Health revealed that while 70 percent believe a personal health record would improve quality of health care, almost all respondents (91%) indicated that they were very concerned about privacy and keeping their health information secure.8 Likewise, a 2005 survey conducted by the consulting firm Accenture found that an overwhelming number of respondents thought medical care would improve if doctors had access to electronic medical records (EMRs); at the same time, asked to rank their top five concerns with EMRs, respondents put privacy at the top of the list.9 In recent congressional testimony, Westin stated that "surveys show that most consumers want the opportunities and benefits of our consumer-service and marketing-driven society. With proper notice and choice, more than three out of four consider it acceptable that businesses compile profiles of their interests and communicate offers to them." He pointed out that some 63 percent of Americans, or 125 million people, can be classified as "Privacy Pragmatists": they are willing to share a certain amount of information in the interests of greater efficiency and service,

---

6 For a copy of the report, see http://www.healthprivacy.org/usr_doc/33807.pdf.
8 Available at: http://www.connectingforhealth.org/.
as long as they know their information will be safeguarded with privacy protections.10

One of the central challenges confronting privacy advocates is to find a balance between these two themes—what Westin, writing on the concept of privacy generally, calls the “distinctive balance between the private sphere and the public order” (2003, 432). Much as it is essential to protect confidentiality of information, so it is essential for our privacy and information laws to maximize the potential benefits that can be offered by medical data. Patients must not feel that their information is misused in any way that violates their privacy; but equally, if information is not shared or disseminated at all, then patients themselves will be the losers.

The solution to achieving this balance lies in well-defined principles that protect information while permitting it to be shared in a meaningful and productive way. Building on the recommendations of the Health Privacy Working Group (many of which were included in HIPAA Privacy Regulations), this backgrounder discusses steps to “integrate privacy protections as part of information practices” (8). This process of integration, in which confidentiality and security protections are built into the architecture of electronic health records and other means of using data, is the best way to ensure that the full benefits of information technology are realized while at the same time protecting the confidentiality and security of personal health information.

III. Health Privacy in a Digital Health Information Networked Environment: What is Different?

We have seen that conventional notions of privacy are today equated with the right to protect information about one’s self. The right to privacy may therefore be thought of as a right to secrecy, and privacy protections, whether legal or otherwise, commonly designed to remedy “invasions of secrecy”, for example, through illegal entry into an individual’s home. Such protections are often designed with reference to an individual’s “right to consent” i.e., confidentiality is typically protected by the principle that individuals must give their consent before information about them is allowed to leave the protected domain.

As we shall see, these principles are somewhat outdated in the context of an electronic network. In particular, the widespread availability of databases containing personal information challenges the “right to consent” and “invasion” principles upon which so many privacy protections are currently based. For example, when an individual’s personal health information is aggregated with other patients’ data and resold as part of a database, no opportunity is given to the individual in question to provide consent on reuse of that information. Indeed, in many cases an individual will not even know that his or her personal health information has been reused.

The new environment poses a host of additional challenges to existing privacy protections and principles. If we are to develop effective solutions, it is essential to better understand these new challenges. It needs to be clear, at the outset, that while a digital and networked environment offers much potential and many opportunities, it also poses several new categories of risk. This section will explore some of those risks.

After exploring those new risks, this section will discuss some privacy architectural principles to deal with those risks. A central principle of this backgrounder is that new privacy challenges cannot be addressed solely by focusing on post-violation remedies and penalties, but also (and more importantly) through network architectures that govern the information flows and the handling of personal information. Such architectures must be designed in a way to protect privacy before violations occur. Therefore, after outlining the new risks, we argue that privacy in a digital setting requires structural and systemic approaches.

New Environment, New Risks

1. Commercial Misuses of Data

Perhaps the most serious—and probably pervasive—privacy violations in the information age stem from the potential for commercial

---

misuse of data. In recent years, an extensive data market has developed, driven largely by data aggregators or “data brokers.” These data brokers collect, repackaged, and sell information that is either available in the public domain, or they illicitly aggregate data that was collected for another purpose from that for which it is ultimately used.\textsuperscript{11} Deborah Platt Majoras, Chairman of the Federal Trade Commission, described the general data market of personal information in recent Senate testimony:

> The information industry is large and complex and includes companies of all sizes. Some collect information from original sources, others resell data collected by others, and many do both. Some provide information only to government agencies or large companies, while others sell information to small companies or the general public.\textsuperscript{12}

The emergence of data as a commodity, traded in often-opaque information markets, has led to serious concerns about privacy. In No Place to Hide, Robert O’Harrow describes in vivid detail the wealth of information that now exists on individuals, and the various and frequently harmful ways in which it can be used, often without the individual’s knowledge or consent. Some possible harms include:

- **Denial or Restrictions on Insurance Coverage and Other Benefits:** Information acquired in one medical setting (for example, routine testing) can become part of an individual’s data shadow and later be acquired by insurance companies to deny or otherwise restrict coverage. At least two companies, the Medical Information Bureau (MIB) and AllClaims, currently offer databases of patient medical records to insurance companies and others. Such commercial use of data represents a serious problem in part because inadequate insurance cover creates new and potentially serious public health problems. It is also a serious concern because, as we have seen, knowledge of such risks leads to privacy protective behavior on the part of individuals that can pose further health problems.

- **Restrictions by Credit or Other Agencies:** Medical data can also be acquired commercially and used by non-medical agencies like credit card companies or banks. If such data points, for example, to a serious underlying medical condition, it can lead to denial of credit, mortgages, or other financial services. This “leakage” of information from a medical to non-medical setting is a serious problem in an era of data aggregation; it shows the need not only to build privacy protections within the health care sector, but also to develop strict procedures to control transmission of information across sectors.

- **Unsolicited Marketing:** Data acquired commercially can also be used by pharmaceutical companies and others to market drugs based on information about individuals’ medical condition. Two notable cases of such marketing occurred in 1998, when CVS and Giant Food, two pharmacy chains, offered patient prescription records to private companies that later used the records as the basis for marketing. In addition to the underlying privacy violation involved in making the data available, it can also be argued that the unsolicited marketing itself represents a privacy violation.\textsuperscript{13}

2. **Government Misuses of Data**

The debate over privacy and data aggregation often refers to commercial uses of data. However, the state also makes frequent use of an individual’s medical data shadow for law enforcement purposes.

\textsuperscript{11} The illicit use of data is not particular to the networked environment. What has changed is the scope of potential violations: As the network expands and as the amount of data increases, so does the possibility of confidentiality violations. In addition, a networked environment facilitates the illicit acquisition (e.g., through theft) and dissemination of data. This is in large part due to digitalization of information, which is easier to store, and to steal without its original owner even noticing.\textsuperscript{12} http://judiciary.senate.gov/testimony.cfm?id=1437&wit_id=4161.

\textsuperscript{13} Goldman (1998, 10).
enforcement and other purposes. In 1998, for example, police in Virginia, investigating a car theft from a parking garage near a drug treatment center, collected 200 medical records as part of their investigation; they later acknowledged their actions as an unnecessary violation of patient privacy. State welfare agencies and the Immigration & Naturalization Service (INS) have also used welfare and immigrant health records in the administration of their respective programs.\textsuperscript{14}

An emerging category of risk that is particularly worth highlighting stems from the increasing capability of governments to indulge in surveillance activities. A recent report, jointly issued by the American Civil Liberties Union (ACLU), Focus on the Global South, Friends Committee (US), International Civil Liberties Monitoring Group (Canada), and Statewatch, highlights the risk.\textsuperscript{15} It argues that individual pieces of information on travel and other practices that are currently being collected could lead to an international surveillance framework that "dwarfs any previous system and makes Orwell’s book Nineteen Eighty-Four look quaint." These individual pieces include registration of foreigners, national ID policies, and biometric identification methods.

The report also points out that much of this information is collected in the name of national security. The authors argue that the information will not fulfill its stated purpose, but the stated reason for collection does point to a complication in addressing privacy violations by the state, namely, that government collection and use of data often has legitimate and vital national security purposes. In a post-9/11 environment, in particular, data can be useful in stopping terrorist attacks before they occur. A national information network is today considered critical to enhancing the nation’s intelligence programs. As many—including the Markle Foundation—have argued, however, it is essential that such a network be designed with built-in protections for privacy.

Such protections would be both architectural (i.e., built into the design of the network), practices, and policy-based. We discuss architectural solutions below. One important policy step involves reform of the 1974 Privacy Act. In recent Senate testimony, James Dempsey, the Executive Director of the Center for Democracy & Technology (CDT), pointed out that government use of data is susceptible to privacy violations due to shortcomings in that act, which requires government agencies to collect and use data subject to the provisions of the Fair Information Practices. But as Dempsey further pointed out, such protections are only relevant to "federal 'systems of records', [meaning] ... that the government can bypass the Privacy Act by accessing existing private sector databases, rather than collecting the information itself." He went on to describe the possible negative consequences that can occur when the government accesses private data without the restrictions of the Fair Information Practices:

\begin{quote}
[Although the Privacy Act requires notice to and consent from individuals when the government collects and shares information about them, gives citizens the right to see whatever information the government has about them, and holds government databases to certain accuracy standards, none of those rules applies when the government accesses commercial information without pulling that data into a government database. Currently, the government need not ensure (or even evaluate) the accuracy of the data; it need not allow individuals to review and correct the data; and the government is not limited in how it interprets or characterizes the data.\textsuperscript{16}]
\end{quote}

3. Criminal Misuses of Data
Both commercial and government uses of data have legitimate purposes; generally, misuses and privacy violations represent the exception rather than the norm. But digital data, medical or otherwise, is also susceptible to criminal misuse, which can result in serious violations of privacy, considerable financial expense, and even physical injury and death.

\textsuperscript{14} Health Privacy Working Group (1999, 10).
\textsuperscript{15} http://www.theregister.co.uk/2005/04/21/icam_surveillance_report/.
\textsuperscript{16} http://judiciary.senate.gov/testimony.cfm?id=1437&wit_id=2875.
Identify theft, in which criminals acquire Social Security numbers or other identifying information, represents a particularly serious problem. In 2003, the Federal Trade Commission (FTC) estimated that 10 million Americans (nearly 5 percent of the adult population) were victims of some form of identity theft. According to the FBI, the Internet Crime Complaint Center (IC3), a joint project between the FBI and the National White Collar Crime Center, received more than 100,000 complaints regarding identity theft in the 5-year period between its opening in 2000 and 2005. It estimated the costs of identity theft as nearly $40 billion annually, not including credit card fraud.

For all its seriousness, identity theft represents just one possible instance of criminal misuse of data. It imposes substantial financial costs, but other types of illegal activity can result in even more dangerous consequences. Consider the following two examples:

- In 1999, a woman named Amy Boyer was murdered as the direct result of her data shadow. She was killed when a man purchased her Social Security number, address, and other information from a data broker called Docusearch (the man paid just $154). The information was used by the man, who had been obsessed with Boyer since her youth, to find her place of work and kill her.
- Concerns about similar criminal misuse of data were also raised in a 2005 case brought by a Juneau, Alaska nurse who sought to have her address removed from public records, a licensing condition for all nurses. Expressing a fear of stalkers, she argued, with the assistance of the ACLU, that making her address publicly available posed a serious threat not only to her privacy, but also to her physical safety.

4. Security Breaches
As the above examples illustrate, data can be acquired and misused by criminals in two ways:

- Through legal means, by following or purchasing a legitimate data trail. In such cases, it is the subsequent misuse that is illegal, not the acquisition of the data itself.
- Through criminal acquisition and use of data, in which the way the data is collected is itself illegal. Such criminal acquisition frequently arises as a result of security breaches, discussed in this section.

Security breaches, sometimes referred to as “data leakage,” represent a serious category of risk in the information age. They are not unique to the information age, but digital records and networks present particular vulnerabilities that do not exist in a paper-based world. These risks include the relatively greater ease of remotely hacking a network than physically breaking into a paper records depot; and the fact that large quantities of data are stored on servers and hard disks that are connected to the world, protected only by firewalls or other imperfect security protocols. In addition, digital data is much easier to replicate, and such replication can be done without damaging or removing the original, making it easier to acquire data illegally without the owner even being aware.

These and other factors make it easy to steal or criminally acquire data in the information age. Recent examples suggest that criminals are well aware of network vulnerabilities and that criminal acquisition of data is a growing risk. Recently, for instance, Ameritrade, an online broker, announced that it had lost a tape backup containing data on 200,000 current and former customers. This followed announcements by Lexis Nexis that up to 310,000 customer records may have been hacked; and reports by ChoicePoint, a data aggregator, of similar violations.

Such examples highlight the inherent vulnerabilities of networks and information stored in a digital format. While we have
outlined some of the security vulnerabilities, many more exist. Of course it is impossible to fully protect a network against all forms of intrusion—the best we can hope for is to minimize intrusions.\(^{22}\) The important point is that the existence of such vulnerabilities requires architectural solutions that build security protections from the start, rather than post-fact remedies. We discuss some possible architectural solutions in the following section.

5. Data Quality Issues

In addition to introducing a greater potential for security breaches, a digital environment also introduces potential data quality issues. Problems with data quality, which include data loss or corruption, are not traditionally thought of as privacy violations, but are closely interrelated with current privacy concerns.

Consider, for example, some recent anecdotes regarding the wrongful inclusion of individuals on national no-fly lists or other terror databases. Inclusion in such databases can be considered a privacy violation on at least two counts. First, it can automatically lead to private data being viewed by a range of agencies and groups, which could claim access on national security grounds. For example, if an individual is wrongly placed on a federal no-fly list, local law-enforcement agencies might also gain access to that individual’s information based on law-enforcement sharing procedures.

Second, and more relevant to a discussion of medical privacy, it is important to recognize that much as individuals can be placed by mistake on no-fly lists, so they can be included in medical databases with false identifying information. Patients could, for example, be denied insurance based on mistaken information regarding medical conditions; similarly, they could be forced to pay higher life insurance or other premia.

It is important to acknowledge that, for the moment, such risks remain often theoretical, and that they are not particular to the online world, but also exist in a paper-based system of records. Nonetheless, they highlight the need not only to build strong privacy protections into network architecture, but also remedies and means of appeal against data quality issues. If patients are not able to have privacy or data quality grievances addressed in a quick and clearly identifiable manner, there is a danger that those grievances will be compounded. In addition, a comprehensive approach to data quality must include procedures to ensure information integrity to prevent errors from occurring in the first place.

6. Harmful Social Consequences

Finally, while much analysis of privacy focuses on adverse economic or health consequences, it is important to recognize that privacy violations can impose a very real social cost on individuals, making it difficult for them to live meaningful lives within their communities. One notable example occurred in 1998, when a San Diego pharmacist revealed a man’s HIV-positive condition to his ex-wife. The man, who was locked in a custody battle with the woman in question, ultimately settled the case rather than face the stigma of his condition being made public.\(^{23}\)

The need to carefully control such social consequences is all the more apparent when we consider that societies also use such “shaming” techniques as regular tools for law-enforcement procedures. Consider the widespread use of so-called Megan’s Laws to maintain public sex offender registries. The use of such legitimate and legal shaming techniques makes it essential to draw up strict rules to differentiate between acceptable disclosures of personal information in the public domain, and unacceptable disclosures.

Writing more than 200 years ago, Adam Smith, often considered the father of modern economics, argued that material well-being was just as important to human happiness as “the right to appear in public without shame.” This argument is as true today as it was then, and it draws attention to the very real need for controls on how information about an individual is released into the public domain, and shared with a community.

\(^{22}\) See for instance Paul Clayton (Chair): For the Record: Protecting Electronic Information; National Academy Press, 1997.

\(^{23}\) Health Privacy Working Group (1999, 10).
IV. Defining a Comprehensive Privacy Architecture: Establishing Trust in the Network

The previous section described some of the categories of risk represented by new technologies and methods of information dissemination. Clearly, these risks and vulnerabilities require new responses. These responses, moreover, must not be ad-hoc or post-fact, but designed in a systematic and comprehensive manner. At the core of adequate privacy protection in the digital age is that it must be supported by policy, practice, and the architecture of the network.

The purpose of this section is to provide privacy architectural principles for the policy, technology and, more generally, for the social and economic context within which the technology is used. In what follows, we present nine core principles of privacy protection based upon Fair Information Practice Principles (FIPPs) and explain how they must be built into the way information is collected and shared. Before that, we review currently existing Fair Information Practice Principles.

Throughout this discussion, we must keep in mind that to be effective, the scope of the protection will need to be determined and defined. This requires considering whether different kinds of protections should apply for different kinds of data; the kind of relationship and the level of trust (either socially, contractually, or legally determined) one aims to address and achieve. In addition, one needs to focus on the various systems of records or the information flow and any third party that maintains those systems.

Fair Information Practice Principles

Before discussing our core principles for a networked environment, it may be useful to briefly consider some existing principles for privacy protection. These principles provide a useful template, but they are not optimized for a network-driven world. Many were designed long before the age of the Internet, data brokers, and data aggregation. As such, they may need to be tailored, adapted, and, in some cases, expanded to address the specific risk management challenges posed by the digital age in general, and the rise of EMRs in particular.

The Privacy Rights Clearinghouse, a nonprofit consumer group located in California, provides a useful review of existing Fair Information Practices. Here, we provide a summary, based on that review, of existing privacy laws in three jurisdictions:

1. The United States, including the 1973 Fair Information Principles and the 1974 Privacy Act;
2. The OECD, including the 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data; and

1. The United States

The Fair Information Practices were implemented over thirty years ago (1973), when the US Department of Health Education and Welfare (HEW) formed a task force to consider the privacy effects of the spread of computer medical records. The Code of Fair Information Practices developed by this task force includes the following principles:

1. **Collection limitation:** There must be no personal data record keeping systems whose very existence is secret.
2. **Disclosure:** There must be a way for individuals to find out what information about them is in a record and how it is used.
3. **Secondary usage:** There must be a way for individuals to prevent information about them that was obtained for one purpose from being used or made available for other purposes without their consent.
4. **Record correction:** There must be a way for individuals to correct or amend a record of identifiable information about them.
5. **Security:** Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the

24 See [http://www.privacyrights.org/ar/fairinfo.htm](http://www.privacyrights.org/ar/fairinfo.htm) for a full discussion.
reliability of the data for their intended use and must take precautions to prevent misuse of the data.

It is important to note that, unlike many other industrialized countries, these practices have not been put into law at the federal level. While they have been codified at the state and sectoral levels, no blanket safeguards exist to implement and oversee these protections at the national level.

One notable exception is the Privacy Act of 1974. However, as noted earlier, this law only applies to systems of records that exist within government agencies. A major weakness is that it allows agencies to use private sector data without applying any of the protections contained in the law.

2. The OECD
Unlike the United States, many European countries have adopted broad, omnibus privacy protections that apply across sectors and jurisdictions. The OECD developed its Fair Information Practices as far back as 1980, and the European Union (EU) has adopted many of these principles. In particular, they were codified in the European Union’s Directive on Protection of Personal Data, implemented in 1995. The privacy guidelines adopted by the OECD include the following eight principles:

1. Collection Limitation: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2. Data quality principle: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete, and kept up-to-date.

3. Purpose specification: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. Use limitation principle: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:
   (a) with the consent of the data subject; or
   (b) by the authority of law.

5. Security safeguards principle: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data.

6. Openness principle: There should be a general policy of openness about developments, practices, and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity about usual residence of the data controller.

7. Individual participation principle: Individuals should have the right:
   (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them;
   (b) to have communicated to them, data relating to them
      1) within a reasonable time;
      2) at a charge, if any, that is not excessive;
      3) in a reasonable manner; and
      4) in a form that is readily intelligible;
   (c) to be given reasons if a request made under subparagraphs (a) and (b) is

---

26 E.g., in the form of the Fair Credit Reporting Act, the Right to Financial Privacy Act, the Electronic Communications Privacy Act, and the Video Privacy Protection Act.
28 Para 9 of the OECD Privacy Guidelines states: “The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.” See http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.
denied, and to be able to challenge such denial; and
(d) to challenge data relating to them and, if the challenge is successful, to have the data erased; rectified, completed, or amended.

8. **Accountability principle:** A data controller should be accountable for complying with measures which give effect to the principles stated above.

### 3. Canada

Canada has adopted a unique model when it comes to privacy protections. Its privacy guidelines have been formulated not by the state, but by a nonprofit entity, the Canadian Standards Association (CSA), which in 1995 adopted the “*Model Code for the Protection of Personal Information*.”

This Code, which includes the 10 principles listed below, can be adopted on a voluntary basis by companies or other entities.

1. **Accountability:** An organization is responsible for personal information under its control and shall designate a person who is accountable for the organization's compliance with the following principles.

2. **Identifying purposes:** The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

3. **Consent:** The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, with certain exceptions.

4. **Limiting collection:** The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

5. **Limiting use, disclosure, and retention:** Personal information shall not be used or disclosed for purposes other than those for which it was collected except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

6. **Accuracy:** Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

7. **Safeguards:** Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

8. **Openness:** An organization shall make readily available to individuals specific information about its policies and practices relating to its handling of personal information.

9. **Individual access:** Upon request, an individual shall be informed of the existence, use, and disclosure of personal information about the individual and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. **Challenging compliance:** An individual shall be able to challenge compliance with the above principles with the person who is accountable within the organization.

As in many countries, these 10 principles are substantially similar to the OECD guidelines described above. However, it is worth noting that two principles in particular have been strengthened in Canada:

- **Consent:** As Principle 10 suggests, consent in Canada includes not just the right to limit access to one's personal data (number 3), but also the right to challenge an entities’ compliance with the Code (number 10).
- **Accountability:** Accountability is held to be so important in Canada that it ranks first on the list of 10 principles. This puts the burden of protecting privacy substantially onto collectors and users of data.

### Core Principles for a Networked Environment

Below, we present nine specific recommendations to ensure privacy. While some of these recommendations reflect and are derived from the Fair Information Practice Principles, they have been updated and designed specifically to protect privacy in a...
networked environment, keeping in mind the unique and new risks described in the previous section.

1. Openness and Transparency
Perhaps the most important mechanism for privacy protection in the information age, this first principle stipulates that there should be a broad and universal practice of transparency in the way data is handled. Individuals should be able to establish what information exists about them in the data market and in government databases. They should be able to track how that information is used, and by whom, and they should be able to control how that information is disseminated. Individual choice is critical; control of information rests with persons, not with data aggregators or data users.

It is also essential that individuals be aware of how they can exert such control. Having strict laws to ensure transparency and openness serves little purpose if people do not know how they can find out where information about them exists, and how they can control who has access to that information. Ideally, patients should be able to give their informed consent to any use of their information.30 Outreach and education regarding privacy are critical, as is the role of civil society and consumer groups in facilitating such efforts.31 One possible policy option is to require all data collectors and aggregators to register with a government agency, probably the Federal Trade Commission (FTC), and for that agency to maintain a secure32 “one-stop” web site where people can view their data shadow.

2. Purpose Specification and Minimization
Data should never be collected without people knowing that it is being collected. Furthermore, they should always be aware of why that information is being collected, and how it will be used. This will allow them to give their informed consent to any act of data collection.

In addition, an important extension exists to this principle of purpose specification: data must be used only for the originally stated reason, or, in rare cases, for other purposes with specific legal sanction: see discussion below regarding “Use Limitation” (Principle 4). Currently, a number of privacy violations occur when data is collected for one legitimate purpose, with individual consent, and then resold and reused in another context, for a very different purpose. For example, clinical data may be collected to treat a patient, but later find its way to the hands of insurers or credit agencies that could use the information to deny coverage. A strict minimization requirement can prevent such unauthorized reuses of data.

3. Collection Limitation
The collection of personal information should be obtained by lawful and fair means and with the knowledge and consent of persons. There should be well-drafted and explicit permissions to ensure that data collectors state their purpose in ways that are clear and easily understood by the population for whom they are intended, without misleading language.

Collection limitation can be seen as an extension of “Purpose Specification and Minimization” (Principle 2). However, it goes beyond the requirement that data collectors specify why they are collecting information and suggests a blanket application of Principle 1 (“Openness”) to all aspects and forms of data collection. For example, the principle of collection limitation requires that information only be gathered in a legal manner, and in a manner that is apparent to patients. This last requirement is particularly important in a networked environment, because technology is often opaque and unclear to average users. Many users, for example, have little idea of the wealth of information that exists on their computers in the form of cookies. They may similarly not be aware of the potential abuses

---

30 Any provisions for informed consent need to be drafted in such a way that ensures the sharing of information is not unduly cumbersome on data users. It is probably unrealistic to assume that patients can or should give their assent to each and every use of their medical data.

31 At the same time, outreach and awareness-building must be conducted with consideration for the potentially harmful effects on a public that is overly-concerned about privacy violations. See, for instance, the following article, which highlights concerns that patients might avoid care due to recent privacy fears: http://www.ihealthbeat.org/index.cfm?Action=dsplItem&ItemID=110098.

32 Valid concerns have been raised that such a centralization may create additional security vulnerabilities.
that occur when they submit personal information to a medical or other web site. Thus, in addition to declaring their purpose clearly (Principle 2), data collectors should also be required to declare the very fact that they are collecting information.

4. Use Limitation
As stated, a minimization requirement would strictly limit whether data collected for one purpose could be reused in another context. Generally, we believe that such reuse should not be permissible without explicit consent of individuals.

However, certain legal exceptions may apply, particularly in the case of national security or law enforcement. Such cases should be the exception instead of the norm, and should be controlled by strict laws and sanctions. In addition, when information is reused, it is far preferable that the data in question be non-identifiable (i.e., it may consist of aggregated or demographic data), but to the greatest extent possible should not include information that could identify an individual. This allows data to be reused without representing a gross violation of an individual’s privacy.

5. Individual Participation and Control
An important principle of privacy protection is that an individual has a vital stake in, and thus needs to be a participant in, determining how his or her information is used. Privacy protections should be designed with this principle in mind: individuals should be seen as key participants in processes of information collection and dissemination, and not as mere subjects or passive spectators. At all stages in the information chain, they should be able to inspect and query their information, and to determine who uses that information. In addition, as we shall explore further, they should have clear avenues to correct information.

Such control can be facilitated through the principles of transparency and the various limitations we have outlined above. In addition, whenever possible, personal information should be collected directly from the individual rather than from a third-party. This enhances patient control over personal information. Finally, control means that people should have meaningful opt-out clauses when they do not want their information to be reused, or when they want to “reclaim” their information. Currently, many opt-out procedures administered by web sites and others are complicated and cumbersome, making it near-impossible for people to exert real control. In addition, opt-out provisions can be diluted when they represent all-or-nothing choices, forcing people to choose, for example, between privacy and inefficient service. For such reasons, “opt-in” is often regarded as providing more control to the patient: it allows patients explicitly to determine when, by whom, and for what purpose information is used. In the event patients do not understand the conditions under which their information is being used, they can choose to request more information, or refuse permission.

It is also important to note that greater individual control may confuse existing methods of determining and allocating liability for privacy violations and medical errors. For example, practitioners may be blamed for errors stemming from an individual’s refusal to release medical information. Similarly, an individual could accidentally “leak” his or her own data through a “phishing” attack or other online breach. Overall, there will certainly be new and unforeseeable liability issues raised by greater use of EMRs and greater patient control. To the extent possible, these need to be addressed beforehand, in a systematic manner, as part of any Fair Information Practice Principles.

6. Data Integrity and Quality
We have seen that data corruption is a key—and new—source of privacy violation in the information age. It follows that mechanisms need to be developed to address this violation, and for establishing accountability among those who maintain records. Such mechanisms can include technical tools for quality control, as well as regular backups and redundancy in systems.
and databases. In addition, individuals should have clear avenues to view all information that has been collected on them, and to ensure that the information is accurate, complete, and timely. The tools could include laws drafted along the lines of the Fair Credit Reporting Act, which permits people to correct mistakes in their credit report.

Individuals should also be able to ensure that information is being used for the originally stated purpose—they should be able to correct errors in context as well as content. This requires that people be able to view not only what information exists on them, but how it is being used. A discrepancy in either can be viewed as a form of data corruption, requiring clearly-articulated and publicized avenues for redress.

7. Security Safeguards and Controls
Security breaches, discussed above, represent another potential source of privacy violation, and so security safeguards represent another important principle for privacy protections. Given the increasing frequency of hacking and other forms of cyber-crime, it is imperative that reasonable security safeguards be built against loss, unauthorized access, destruction, use, modification, or disclosure of personal information. In addition, all data collectors and disseminators should be mandated to immediately disclose any security breach through a direct communication to those consumers affected (i.e., not just by releasing the news to the media). Such laws, similar to California’s information security breach law (Civil Code § 1798.29), will allow individuals to protect themselves through post-fact remedies.

Security represents an important example of how protections can be built into the design of technology. By implementing the right technologies, and by consulting security experts at the outset, key precautions can be taken at the design stage to increase the robustness of network security. For example, networks can be designed and built with enhanced identity management tools to ensure that access to information is limited to those with a specific need and authorization to see it. In addition, data scrubbing, hashing techniques, real-time auditing mechanisms, and a range of other technical tools can be deployed to ensure security. The key is to supplement legal protections with technical protections. That is the only way to ensure true data privacy.

8. Accountability and Oversight
It is essential that mechanisms be built to ensure that the responsibility for privacy violations is identifiable, and that remedial action can be taken. Boards of directors and senior management must be held accountable for any violations. It is their responsibility to ensure steps are taken to instigate, review, or modify their organization’s risk management strategy as it relates to handling patients’ information.

Several specific steps can be taken to enhance accountability and oversight. Organizations could be mandated to create a post for chief privacy officers (CPOs), who would fulfill the same duties with regard to privacy as CFOs and CTOs do with regard to finance and technology, respectively. In addition, organizations should hold regular employee training programs as well as privacy audits to monitor organizational compliance. These audits can be facilitated by technical tools that ensure clear audit trails and reveal patterns of use and potential abuse.

9. Remedies
This principle is closely related to Principle 8, with the exception that it probably entails greater participation by the state in the form of legal sanctions. One of the key challenges with enforcement of privacy rights is the difficulty (often impossibility) of clearly pinning blame, or even of tracing the source of a privacy violation. Solove and Hoofnagle (2005, 13) point out that approximately 50 percent of identity theft victims do not know how their information was accessed. Similarly, it is likely to be extremely difficult for a patient to monitor and identify violations of information contained in their EMRs. Without such information, it obviously becomes very difficult to seek remedies.

Some of the strategies described above (e.g., audit trails) can help pin the blame more accurately. In addition, internal controls such as those described in Principle 8 are also important to monitor uses and abuses of information.
While such remedies are not foolproof, they do help identify a data trail.

When it is possible to identify the source or perpetrator of a privacy violation, the next step is to ensure that clear legal remedies exist to address the situation. Minimum statutory punishments must be clearly articulated, as must damages for any violations. Solove and Hoofnagle have also suggested that ways must be developed to avoid extensive class action litigation, e.g., by allowing state authorities to fine companies and disburse remedies to victims of privacy violations from a state-administered fund. Whatever the specific steps adopted, the important point is that enforcing sanctions and remedies is as important as establishing the protections themselves.

V. Current Laws and Guidelines and How They Integrate an Architectural Approach

The above describes a template for privacy protections. We have seen nine key steps required to protect medical data in the information age. In this section, we provide an overview of existing policies, both at the state and federal levels. In addition, we discuss the emergence of community-based or other health sub-networks and describe the challenges and opportunities they pose to the integration of federal and state provisions.

The overview provided in this section is somewhat limited. The variety and patchwork of laws that exist, particularly in the states, makes it near-impossible to present a comprehensive overview in this backgrounder. We have therefore chosen to focus on the most important and relevant laws and statutes and, within those laws, to focus on key themes. Throughout the text, we have provided links where more detailed information can be found.

A. Federal: HIPAA Privacy Regulation

In 1996, the United States Congress passed the Health Insurance Portability and Accountability Act (HIPAA), which governed how medical information could be collected and shared. HIPAA's privacy protections, contained in the HIPAA Privacy Rule, became effective for most organizations in 2003. These marked the first (and, thus far, only) federal-level protections for privacy of medical data.

Among the more significant measures introduced by the Privacy Rule were a guarantee of patient access to medical records; provisions to protect personal health information from misuse; provisions to ensure notice of use to patients; the right to file a complaint; and a requirement for health providers to provide patients with information on their privacy practices. Below we provide an overview of these and other key privacy protections. It also includes a discussion of HIPAA's related Security Rule, which governs how electronic information can be used, stored, and shared.

Protected Health Information (PHI):

One of the initial functions performed by HIPAA's Privacy Rule is to define the notion of protected health information (PHI). PHI covers a variety of information and data that could be used to identify a patient, including names, addresses, Social Security numbers, license numbers, medical record numbers, and so on. Under HIPAA, all PHI is subject to the limits on use and disclosure described below.

Limits on Use and Disclosure: Generally, PHI can only be used or disclosed for a person's medical treatment, payment-related activities, or routine operations of a health care provider. Other than for these three purposes, known as TPO, information can be disclosed only when it is considered in the public interest, or when it forms part of a de-identified data set (see discussion below). Under HIPAA, all other uses or disclosures of information must receive written authorization from the patient. In addition, patients have the right to access and view how their information has been used and disclosed.

Reasonable Safeguards: HIPAA also requires health care providers and businesses to ensure "reasonable safeguards" to protect PHI. Such safeguards could include shredding.

34 It is also worth noting that some observers have suggested that penalties for abuses should be strengthened in order to act as a deterrent against future abuses.
documents, ensuring that medical records are safely locked, using curtains or other dividers in treatment rooms, and a variety of measures to protect electronic health information (or ePHI; see the discussion below). While the range of possible safeguards is broad, the law clearly puts the burden of protection on providers, in the process establishing clear lines of responsibility and liability.

Providing Notice of Privacy Practices: As mentioned above, HIPAA requires providers to ensure that patients are aware of their privacy rights and of providers’ privacy practices. Under the law, a “Notice of Privacy Practices” must be provided to patients in written form. In addition, the law also requires providers either to obtain written acknowledgement from the patient that he or she has received such notice; or at a minimum, providers must document that reasonable efforts have been made to obtain such acknowledgement.

Limited Data Set: One exception to the strict disclosure restrictions mentioned above is in the case of de-identified information and what the HIPAA law calls “limited data sets.” In the case of such information, no explicit written authorization is required for sharing. Information is considered de-identified when it does not contain PHI identifiers, and when it is stored using standard statistical and scientific methods (e.g., for research purposes). Even when PHI identifiers are removed, a Data Use Agreement must exist between the provider and user of the information.

Minimum Necessary Information: Although HIPAA permits providers to share information without patient authorization for TPO purposes, it nonetheless requires them to share the minimum amount of information. This concept of “minimum necessary” information is central to HIPAA’s privacy protections. In practice, it means that providers need to have standards and codes in place that define the extent of information necessary for certain practices. It also generally means that providers or other entities can request a patient’s full medical record only in exceptional circumstances.

Compliance and Enforcement: In addition to these central provisions, HIPAA includes a variety of provisions to ensure compliance and enforcement. These include stronger civil and criminal penalties for improper disclosures of PHI, as well as measures to train and provide information for health care providers to ensure that they are in compliance with HIPAA’s privacy standards. The law also gives patients the right to monitor how their information is accessed and used, and to seek redress in cases where violations have occurred.

Security Rule: Although technically separate from the law’s privacy provisions, HIPAA’s Security Rule is closely related. While the Privacy Rule covers all forms of data (including paper-based information), the Security Rule applies specifically to electronic protected health information (ePHI). Under the Security Rule, entities are required to protect ePHI from reasonably anticipated threats, institute appropriate technical protections to defend networks, ensure the integrity of data and physical infrastructure, and limit access to authorized individuals. The Security Rule is technology-neutral, meaning that it does not prescribe particular technologies or standards for protecting ePHI, but it is nonetheless, quite specific in its requirements.

B. State Laws
In addition to the above designed federal laws, a patchwork of state laws exists to provide privacy protections. Indeed, in the absence of a national set of privacy standards, individual states have historically taken the lead in protecting medical privacy in the United States. This has offered certain benefits, particularly in those states where protections are strong, but many also feel that it represents a weakness in the US system, which lacks an over-arching approach to privacy.

A comprehensive overview of state laws is not possible here. In an extensive report on state statutes, the Health Privacy Project noted the difficulty of the task, pointing out that the terrain was uneven (Pritts et al 2003). That report, The State of Health Privacy, Second Edition, A Survey of State Health Privacy Statutes, remains the best resource for state protections. In addition, Pritts presents a

36 It can be accessed at: http://medicalrecordrights.georgetown.edu/publications.html. The 2003 version of the report updated an earlier version - The State of Health Privacy: An Uneven Terrain (A Comprehensive Survey of
conceptual discussion of many of the most important issues raised by state laws, including their relationship to federal laws like the HIPAA Privacy Act. Other key issues include the federal pre-emption and the floor v. ceiling debate, and the way in which state laws are condition specific/circumstance specific and may be more stringent than HIPAA (Pritts 2002, 343, 335-36).

Pritts (2002, 330) notes that states can protect privacy through three legal avenues: constitutions, common law, and statute. The following summary of each of these avenues owes significantly to her discussion.

Constitutional Protections
State constitutional protections have recently been in the news due to alleged violations of Rush Limbaugh’s medical privacy in Florida. In fact, state constitutions generally offer only limited protection. Most states contain an implied right to privacy similar to that in the US Constitution, and some explicitly protect medical privacy. Yet, as Pritts notes, those protections are generally designed to limit only state action, and are easily outweighed by disclosure requirements.

Only two states, California and Hawaii, stand out for their strong, constitutional protections of medical privacy. These protections apply both to violations by the state, and by the private sector. In addition, they are explicitly written to cover medical information, providing a strong bulwark against the lack of adequate federal protections.

Common Law Protections
State common law is somewhat more robust in its protections than state constitutions. Here, too, state law is fragmented and varied, but a growing number of courts have found grounds for two privacy rights in particular: the right to maintain confidentiality of information and a patient’s right to access his or her medical information. These rights are important because many states do not grant a statutory right to access (Pritts 2002, 333, 349-50).

Despite the steady expansion of these rights, Pritts (2002, 332) notes at least two shortcomings in existing common law protections:

1. In cases involving disclosure of information, courts are increasingly finding legal grounds to accept cases, but patients have had trouble proving the guilt of those who have allegedly “leaked” their information. There exists, in short, a high burden of proof for many patients, and court decisions in general have led to the conclusion that “the underlying duty of confidentiality is not absolute” (Pritts 2002, 332).

2. In cases allowing patients access to their information, courts have found numerous legal grounds on which to consider patients’ complaints (e.g., adopting property principles). At the same time, there exists some disagreement on what “reasonable access” requirements would imply, and to what extent health care providers have discretion in deciding what information to make available to patients.

Statutory Protections
For some decades now, the main protections for patient medical privacy have come not through constitutional or common law, but rather through specially enacted statutory protections. Statutory protections have become so important that the previously mentioned Health Privacy Project reports focus almost entirely on this category of legal protection.

The scope of privacy laws is particularly diverse and uneven in this category of protections. Each state has its own principles and standards, and sometimes these principles clash. In addition, state laws are often highly specific, applying differently to various conditions, contexts, and participants.

In an attempt to enforce some cohesion on the patchwork of laws, Pritts (2002, 332)


For a discussion, see Goldman (2001) and Pritts (2002).

38 Colorado and Minnesota, for example, have recognized torts on the basis of “unreasonable disclosure of public facts.” Others, including New York and Nebraska, have explicitly denied this right.
identifies the following six principles that are upheld to a greater or lesser degree across states:

1. Access to Information
2. Right to Amend Health Records
3. Restrictions on Use and Disclosure of Information
4. Notice of Information Practices
5. Security Safeguards
6. Accountability

As noted, these principles are upheld unevenly, and in different ways, across states. In addition, the situation is fragmented within individual states, where a patchwork of laws often means that privacy is protected in a somewhat piecemeal fashion. However, Pritts (2002, 339) notes a recent trend towards “uniformity” in at least some states. She cites California, Maine, and Hawaii as notable examples. Hawaii, in particular, has a “truly comprehensive health privacy law,” which was adopted in 1999, and California has similarly inched towards such a comprehensive approach with a series of consumer- and patient-protective statutes.

A General Observation
Finally, while the above has highlighted the diversity of state laws, it is worth emphasizing one key and crosscutting finding of the original 1999 version of the Health Privacy Project overview of state laws. In one of the three main conclusions presented in its executive summary, the 1999 report indicates that, in general, “state laws have not kept pace with changes in health care delivery and technology” (Pritts 1999, 9). The report points out, for instance, that individual and institutional access to medical data will increase substantially as new technologies are adopted, and that state laws often fail to acknowledge this fact.

In addition, the patchwork and unevenness of state laws poses evident challenges to any attempt to adopt national EMRs or to protect privacy at the national level. This landscape of often robust but uneven protections is a critical factor that needs to be taken into account when designing privacy protection principles.

Ultimately, both the technologies and the policies deployed will need to be flexible and forward-looking enough to adapt to this unevenness.

C. Health Information Sub-Networks: Emerging Rules
In addition to the above discussion of federal- and state-level protections, it is important to briefly consider the tremendous and exciting growth of community based or non-geographic sub-network health information organizations. Such organizations, which provide care at a community-level, are increasingly seen as an effective grassroots way to facilitate information sharing.39

As envisioned, these sub-networks would act as “nodes” on an eventual information-sharing platform. The urgency and importance of information sharing to transform health care is widely understood. Unacceptable rates of avoidable medical errors, as much as $300 billion in unnecessary expenses, and continuing disparities in health care quality constitute a call to action to the health care system and to policymakers. An information-sharing environment has the potential to enable decision support anywhere at any time, improving public and individual health and reducing cost.40

However, the US health care system is highly fragmented. Many types of organizations exist as part of the current health care network, from giant hospital systems and insurance agencies to individual practices, with all manner of specialists, clinics, and agencies in between. In addition, and perhaps more importantly,

---

39 For a discussion of these sub-networks, often called “regional health information organizations” or RHIOs, see the following links: http://ccbh.ehealthinitiative.org/communities/community.aspx?section=102&category=14&document=590 and http://www.healthcareitnews.com/NewsArticleView.aspx?ContentID=1751&ContentTypeld=3]&IssueID=12. In addition, sub-network organizations operate as health information data exchange organizations (whether regionally or affinity-based) that operate as a part of the National Health Information Network (NHIN), a nationwide environment for the electronic exchange of health information made up of a “network of networks."

40 For a full analysis of the benefits of an information sharing environment, see Achieving Electronic Connectivity in Healthcare: A Preliminary Roadmap from the Nation’s Public and Private Healthcare Leaders. Available at: http://www.connectingforhealth.org.
sharing patient’s information will only succeed and be beneficial when it happens within a strong radius of trust.

Towards those ends, we must assume that any information sharing improvement will have to happen through a decentralized approach, where decisions about sharing are made by participating institutions and providers at the edges of the network. The system proposed, for instance, by the Connecting for Health Working Group on Accurately Linking Information for Health Care Quality and Safety, would leave it to the providers to determine locally with their patients what to link, share, and disclose, building upon their existing foundation of trust.

By leaving these decisions at the edges or local sub-networks, it is assumed that the information-sharing environment can grow incrementally, if based upon interoperable standards, and provide for the necessary security and trust. However, multiple challenges remain to be solved for those local and regional entities from the outset. In particular, as they grow beyond their regional origins, they will require coordination between existing state, federal, and local protections.

In addition, networking health information poses certain practical challenges to the sharing of patient information. For example, when data is shared between a larger provider and a small, regional provider, assurances will need to be built into the system to ensure that both adhere to the same privacy safeguards. Without such assurances, both the smaller and the larger provider might be reluctant to share information due to liability concerns. Similarly, concerns have been raised that the proliferation of these community-based networks could overload existing organizations that need to comply with HIPAA and other statutes. The paperwork required to ensure privacy requirements have been met at every step could simply prove overwhelming.

These and other obstacles do not suggest that health information networks at the community level do not provide immense potential to realize a national health information environment; nor are they meant to imply that they should be exempt from existing and emerging privacy protections. Rather, the above discussion is intended to suggest the range of issues raised by the creation of a health information network, and that need to be addressed by technology and policy. Both avenues—technology and law—offer potential solutions, but it is important that we acknowledge the problems from the outset.

VI. Conclusion
The preceding discussion has made clear the complexity of the topic at hand. Protecting medical privacy and confidentiality in a networked era involves a wide range of issues, and requires the cooperation and involvement of a similar range of actors. Practitioners and patients are, of course, critical to the effective deployment of EMRs, or indeed any other successful use of technology in health care. But the involvement of public health authorities, insurance companies, data marketers, civil society organizations, and a variety of other entities is also essential. In addition, governments and others at different jurisdictions—municipal, county, state, national, and international—will have to be considered.

Each of these actors brings different perspectives to the table. These differences can be productive, representing a wealth of knowledge and experience. But they can also be problematic. The range of experiences is accompanied by a variety of agendas, and—put more charitably—a variety of priorities. Harmonizing and doing justice to all these priorities is one of the key tasks confronting advocates of medical privacy.

Success, essentially a balancing act, will require more than the somewhat piecemeal approach to privacy that currently exists and that has been reviewed in this backgrounder. This underscores the need for a systematic and architectural solution. The foundations of this solution are the nine principles described in Section IV. Considered and applied together, these principles add up to an integrated and comprehensive approach to privacy that can help overcome the current fragmentation. It is critical that the nine principles be considered as part of one package. Elevating certain principles

41 Their report is available at: http://www.connectingforhealth.org.
over others will simply weaken the overall architectural solution this backgrounder has proposed.

Of course, the principles remain just that—principles—and their precise manifestation will vary from state to state, and from country to country. Yet while they are broad enough to apply across organizations, stakeholders, and jurisdictions, they are also specific and tangible enough to have real significance and practical effect. The key is to apply them in a thorough and comprehensive manner before creating any new information network, not as an afterthought, and not as an after-the-fact band-aid solution.
Works Cited


"Medical Files or Fishbowls?" Washington Post, 23 September 1997, A16.


<table>
<thead>
<tr>
<th>Privacy Architectural Principles(^1)</th>
<th>Policies and Procedures in a Networked Health Information Environment</th>
<th>Use of Technology for Privacy Protection(^2)</th>
<th>HIPAA Baseline Provisions(^3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Openness and Transparency</td>
<td>Transparency and tracking policies;</td>
<td>Standards and technologies for expressing policies;</td>
<td>Notice of Privacy Practices.</td>
</tr>
<tr>
<td></td>
<td>Collection and uses of personal data;</td>
<td>Standards and technologies for discovering policies once an institution’s HIPAA provider number is known;</td>
<td>Under HIPAA, patient information</td>
</tr>
<tr>
<td></td>
<td>Adequate proper notice of privacy practices;</td>
<td>- Defenses against people using transparency as an opportunity for phishing.(^4)</td>
<td>can be used or disclosed for treatment, payment, and health care operations without specific patient consent or authorization.</td>
</tr>
<tr>
<td></td>
<td>Disclosure procedures to individuals of security breaches;</td>
<td></td>
<td>The term health care operation includes quality assessment, outcomes evaluation, underwriting, legal services, auditing, business planning, customer service, and numerous other functions. The rules give each patient the right to request that a covered entity modify the standard terms. However, the covered entity has no duty to agree to a patient’s request.</td>
</tr>
<tr>
<td></td>
<td>Outreach and public education efforts to enhance awareness of privacy issues and privacy rights, as well as the risks and benefits of a networked environment.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Purpose Specification and Minimization</td>
<td>Define acceptable uses of the system;</td>
<td>Audit and logging technologies (including versioning);</td>
<td>Authorization for use of protected health information for marketing and fundraising and minimum</td>
</tr>
<tr>
<td>The purposes for which personal data is collected</td>
<td>Define purposes of</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

\(^1\) Considered and applied together, these principles add up to an integrated and comprehensive approach to privacy necessary for a connected health information exchange environment. **It is critical that the nine principles are considered as part of one package—elevating certain principles over others will simply weaken the overall architectural solution to privacy protection in a networked health information environment.**

\(^2\) The use of technology for privacy protection depends to a large extent on the level of automatization of the envisaged process.

\(^3\) HIPAA applies directly only to covered entities, which are health care providers, health plans (e.g., insurers, health maintenance organizations), and health care clearinghouses (organizations that facilitate the processing of health care claims and information). No other health care record keepers are covered directly. However, an organization that is not a covered entity may still become subject to the HIPAA rules if it functions as a business associate for a covered entity. A business associate is someone who carries out a function involving the use or disclosure of individually identifiable health information on behalf of a covered entity. The limited scope of the HIPAA rules and the narrow onward transfer provision mean that some health data covered by the rules can be transferred to others and escape the privacy protections of HIPAA.

\(^4\) Phishing is a tool used to gain personal information for purposes of identity theft. It involves using (fraudulent) e-mail messages that appear to come from legitimate businesses.
| data are collected should be specified at the time of collection, and the subsequent use should be limited to those purposes or others that are specified on each occasion of change of purpose. | collection and of access for separate users such as: health care provider; health plan; public health authority; other government agency (law enforcement); researchers; individuals accessing their own health information; contractors and vendors (these might have a separate agreement); − Develop policies requiring that data collected for one purpose should not be used for another; − Implement a minimization requirement. | Standards for expressing uses. | necessary rule. Treatment cannot be conditioned on an individual giving authorization to disclose to other parties. |
### Collection Limitation

*Personal health information should only be collected for specified purposes, should be obtained by lawful and fair means and, where possible, with the knowledge or consent of the data subject.*

- Define purposes of collection and of access for separate users such as: health care provider; health plan; public health authority; other government agency (law enforcement); researchers; individuals accessing their own health information; contractors and vendors (these might have a separate agreement).

- Separation of clinical and demographic information.

Authorization for use of protected health information for marketing and fundraising and minimum necessary rule.

### Use Limitation

*Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified.*

- Define acceptable uses of the system;
- Decisions about linking and sharing are to be made by the participating institutions and providers at the edges of the network;
- “User” limitation: different categories of users to be governed by different rules based upon separate use agreements;
- Some data may not be shared because of special sensitivity (e.g., alcohol/drug abuse history, psychiatric treatment);
- Patient authorization procedures need to be clarified and streamlined;
- Permitted disclosures need

- Technologies for de-identification;
- Technologies for data aggregation;
- Security to prevent unintended disclosures;
- Limiting queries.

Use and disclosure controls and business associate provisions, including minimum necessary rule.

*Note:*
The rule creates specific standards for uses and disclosures for purposes such as public health, research, law enforcement, health oversight, abuse reporting, judicial proceedings, emergencies, organ donations, and other purposes.
<table>
<thead>
<tr>
<th>Individual Participation and Control</th>
<th>Patient authorization procedures;</th>
<th>Differing degrees of control should be built into technology;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individuals should control access to their personal information;</td>
<td>Patient access to information procedures when information is:</td>
<td>Users should be able to choose the level of control and necessary tradeoffs that are acceptable to them;</td>
</tr>
<tr>
<td>Individuals should be able to obtain from each entity that controls personal health data, information about whether or not the entity has data relating to them.</td>
<td>• Maintained by provider</td>
<td>- Defenses against phishing and data theft (through user authentication).</td>
</tr>
<tr>
<td>Individuals should have the right to:</td>
<td>• Maintained by third party vendor;</td>
<td></td>
</tr>
<tr>
<td>- Have personal data relating to them communicated within a reasonable time (at an affordable charge, if any), and in a form that is readily understandable;</td>
<td>• User’s responsibility w/r/t consent prior to sharing data;</td>
<td></td>
</tr>
<tr>
<td>- Be given reasons if a request</td>
<td>• Need for meaningful and clear patient control clauses that do not present “all or nothing” choices;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Consider ways to enhance patient control;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Clarify new liability issues arising from greater individual control;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Policies by which data may be withheld at direction of</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Right to access.</td>
<td></td>
</tr>
</tbody>
</table>

Note: Authorization is required before disclosure to third parties other than for treatment, payment, operations, and other specified purposes.
(as described above) is denied, and be able to challenge such denial; and
- Challenge data relating to them and have it rectified, completed, or amended.

<table>
<thead>
<tr>
<th>Patient;</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Requirement to draft consent and authorization forms in clear language, easily understandable to users.</td>
</tr>
</tbody>
</table>

### Data Integrity and Quality

All personal data collected should be relevant to the purposes for which they are to be used and should be accurate, complete, and current.

<table>
<thead>
<tr>
<th>Policies to ensure accuracy, consistency, and completeness of data;</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Check their information and correct any errors (possibly model on Fair Credit Reporting Act);</td>
</tr>
<tr>
<td>- Patient should be able to correct context of data use as well as content of data (i.e., they should be able to correct any misuse of data);</td>
</tr>
<tr>
<td>- Clarify the SNO’s liability in the case of:</td>
</tr>
<tr>
<td>• Failure of the system to operate as expected or at all;</td>
</tr>
<tr>
<td>• Loss or corruption of data within the system;</td>
</tr>
<tr>
<td>• Incomplete or inaccurate data;</td>
</tr>
<tr>
<td>• Misuse of the system by others, including other users;</td>
</tr>
<tr>
<td>• Breach of security of the system.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Practices to ensure quality, accuracy, and availability, including backups, integrity checks, and periodic sampling;</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Technical methods for allowing an individual to access and review his/her health record.</td>
</tr>
</tbody>
</table>

| HIPAA Security Regulation and Privacy Regulation each require physical, technical, and administrative safeguards. |

**Security Safeguards and Controls**

*Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure.*

| - Authorizing, managing, and policing access to information in the system by all categories of users; |
| - Clear security policies (User's responsibility to implement reasonable and appropriate measures to maintain the security of the system and to notify the SNO of breaches in security, including any specific measures required by the SNO's policies and procedures); |
| - Policies to handle intra- and extra-community matching issues. |
| - Matching algorithm and thresholds; |
| - Authentication of users; |
| - Encryption technologies; |
| - Auditing, service management, and logging. |

HIPAA Security and Privacy Rules each require physical, technical, and administrative safeguards.

*Note:*
The general Security Rule requires covered entities to:

- Ensure the confidentiality, integrity, and availability of all electronic protected health information (EPHI) the covered entity creates, receives, maintains, or transmits;
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required by the Privacy Rule; and
- Ensure compliance by its workforce.
## Accountability and Oversight

Entities in control of personal health data must be held accountable for implementing these information practices.

- Contract administration;
- Policies by which the user has clear and sole responsibility for use of the system and actions taken in reliance on data in the system;
- Consider mandating a position of Chief Privacy Officer (CPO) in organizations;
- Clear user enrollment and termination procedures;
- Designate someone responsible for ensuring patients’ rights, such as access and amendment.

- Logging tools;
- Auditing tools (including versioning);
- Tracking systems;
- Standards and technologies for allowing remote institutions to identify those accessing data at the individual level.

Enforcement by United States Department of Health & Human Services (HHS) of Security and Privacy rules.

Note: HIPAA imposes on each covered entity a series of administrative requirements. These include: 1) designating a privacy official responsible for development and implementation of privacy policies and procedures; 2) training staff in privacy; 3) establishing appropriate administrative, technical, and physical safeguards to protect the privacy of information; 4) establishing a compliance process for individuals; and 5) developing and maintaining written policies and procedures for implementing the privacy rules.

## Remedies

Legal and financial remedies must exist to address any security breaches or privacy violations.

- Policy and remedies for unauthorized disclosures.

- Web site with information about how patients can identify and pursue possible remedies.

HIPAA provides no private right of action, although state law may permit such suits. The Secretary of HHS accepts complaints and can investigate and seek civil penalties against covered entities that violate the privacy rules. Criminal enforcement may be available.
Acknowledgements
The members of the Connecting for Health Policy Subcommittee have accomplished an extraordinary task in less than a year's time—the development of an evolving piece of work that can serve as the core of nationwide health information exchange—the policy components of The Common Framework. During this time, we have been fortunate to work with respected experts in the fields of health, information technology, and privacy law, all of whom have contributed their time, energy, and expertise to a daunting enterprise. Our consultants and volunteers have worked long hours in meetings and conference calls to negotiate the intricacies of such issues as privacy, security, authentication, notification, and consent in health information exchange. We offer them our heartfelt thanks for taking on this journey with us, and look forward to the remaining work ahead.

In addition, we would like to offer special thanks to the volunteers and consultants who authored the initial drafts of this body of work—their hard work created a strong foundation upon which to focus the Subcommittee's deliberations: Stefaan Verhulst, Clay Shirky, Peter Swire, Gerry Hinkley, Allen Briskin, Marcy Wilder, William Braithwaite, and Janlori Goldman.

Finally, we must note that none of this work would have been possible without the leadership and inspiration of our co-chairs, William Braithwaite and Mark Frisse. They have led us with steady hands and determination of spirit.

Connecting for Health Policy Subcommittee

William Braithwaite, MD, eHealth Initiative, (Co-Chair)

Mark Frisse, MD, MBA, MSc, Vanderbilt Center for Better Health, (Co-Chair)

Laura Adams, Rhode Island Quality Institute

Phyllis Borzi, JD, George Washington University Medical Center

Susan Christensen*, JD, Agency for Healthcare Research and Quality, United States Department of Health and Human Services

Art Davidson, MD, MSHP, Denver Public Health

Mary Jo Deering*, PhD, National Cancer Institute/National Institutes of Health, United States Department of Health and Human Services

Jim Dempsey, JD, Center for Democracy and Technology

Hank Fanberg, Christus Health

Linda Fischetti*, RN, MS, Veterans Health Administration

Seth Foldy, MD, City of Milwaukee Health Department

Janlori Goldman, JD, Columbia College of Physicians and Surgeons

Ken Goodman, PhD, University of Miami

John Halamka, MD, CareGroup Healthcare System

Joseph Heyman, MD, American Medical Association

Gerry Hinkley, JD, Davis, Wright, Tremaine LLP

Charles Jaffe, MD, PhD, Intel Corporation

Jim Keese, Eastman Kodak Company

Linda Kloss, RHIA, CAE, American Health Information Management Association

Gil Kuperman, MD, PhD, New York-Presbyterian Hospital

Ned McCulloch, JD, IBM Corporation

Patrick McMahon, Microsoft Corporation

Omid Moghadam, Intel Corporation
Joyce Niland, PhD, City of Hope National Medical Center

Louise Novotny, Communication Workers of America

Michele O’Connor, MPA, RHIA, MPI Services Initiate

Victoria Prescott, JD, Regenstrief Institute for Healthcare

Marc A. Rodwin, JD, PhD, Suffolk University Law School

Kristen B. Rosati, JD, Coppersmith Gordon Schermer Owens & Nelson PLC

Sara Rosenbaum, JD, George Washington University Medical Center

David A. Ross, ScD, Public Health Informatics Institute

Clay Shirky, New York University (Chair, Technical Subcommittee)

Don Simborg, MD, American Medical Informatics Association

Michael Skinner, Santa Barbara Care Data Exchange

Joel Slackman, BlueCross/BlueShield Association

Peter P. Swire, JD, Moritz College of Law, Ohio State University

Paul Tang, MD, Palo Alto Medical Foundation

Micky Tripathi, Massachusetts eHealth Collaborative

Cynthia Wark*, CAPT, United States Public Health Service Commissioned Corps, Centers for Medicare and Medicaid Services, United States Department of Health and Human Services

John C. Wiesendanger, MHS, West Virginia Medical Institute/Quality Insights of Delaware/Quality Insights of Pennsylvania

Marcy Wilder, JD, Hogan & Hartson LLP

Scott Williams, MD, MPH, HealthInsight

Robert B. Williams, MD, MIS, Deloitte

Joy Wilson, National Conference of State Legislatures

Rochelle Woolley, RxHub

Amy Zimmerman-Levitan, MPH, Rhode Island State Department of Health

*Note: Federal employees participate in the Subcommittee but make no endorsement
Model Privacy Policies and Procedures for Health Information Exchange
Model Privacy Policies and Procedures for Health Information Exchange
The document you are reading is part of The Connecting for Health Common Framework, which is available in full and in its most current version at: http://www.connectingforhealth.org/. The Common Framework will be revised and expanded over time. As of October 2006, the Common Framework included the following published components:
Model Privacy Policies and Procedures for Health Information Exchange*

The model policies contained in this paper are recommended by the Connecting for Health Policy Subcommittee to be used in conjunction with the Connecting for Health “Model Contract for Health Information Exchange” for those working to establish sub-network organizations (SNOs) that will use a Record Locator Service (RLS) and operate as part of the National Health Information Network (NHIN). The policies establish baseline privacy protections designed to apply to all individuals receiving care from a SNO Participant (Participant). The goal of these policies is to provide a framework for protecting health information while simultaneously permitting use of the information that is both productive and meaningful. The policies are intended to be useful for SNOs whether or not they are using an RLS.

The federal HIPAA Privacy and Security Rules provide the baseline for the model policies, although in some cases greater privacy protections and individual rights are recommended by the Connecting for Health Policy Subcommittee. Where provisions are derived from the HIPAA Privacy or Security Rules, citations are provided. In no instance do these policies permit less protection of personal health information than those required by federal law; however, participation in a SNO is not a surrogate for determining whether a Participant is a HIPAA “Covered Entity” or is in compliance with the HIPAA regulations. Importantly, the model policies permit Participants to establish and follow their own more protective data management, privacy and security policies, and procedures. In addition, some customization may be necessary at the SNO and Participant level to ensure consistency and compliance with applicable state laws. Many of these policies can and should already be in place at the Participant level. Some are aspirational and should be considered in the future as a networked environment for health information emerges and technology enables greater consumer access to their health records. The policies will need to be customized to reflect the Participants’ unique circumstances and modified to take account of applicable state laws.

The model policies are deeply rooted in nine privacy principles that together form a comprehensive privacy protective architecture, as discussed in the Connecting for Health “Architecture for Privacy in a Networked Health Information Environment.” These principles and the policies that flow from them promote balance between consumer control of and access to health information and the operational need to ensure that information uses and disclosures are not overly restricted such that consumers would be denied many of the benefits and improvements that information technology can bring to the health care system. The policies reflect a carefully balanced view of all of the principles and avoid emphasizing some over others in any way that would weaken the overall approach. The nine privacy principles are as follows:

Openness and Transparency.

Openness about developments, procedures, policies, technology, and practices with respect to the treatment of personal health data is essential to
Protecting privacy. Individuals should be able to understand what information exists about them, how that information is used, and how they can exercise reasonable control over that information. This transparency helps promote privacy practices and instills confidence in individuals with regard to data privacy, which in turn can help increase participation in health data networks.

**Purpose Specification and Minimization.** Data use must be limited to the amount necessary to accomplish specified purposes. Minimization of use will help reduce privacy violations, which can easily occur when data is collected for one legitimate reason and then reused for different or unauthorized purposes.

**Collection Limitation.** Personal health data should be obtained only by fair and lawful means, and, if applicable, with the knowledge or consent of the pertinent individual. In an electronic networked environment, it is particularly important for individuals to understand how information concerning them is being collected because electronic collection methods may be confusing to average users. Similarly, individuals may not be aware of the potential abuses that can arise if they submit personal health information via an electronic method.

**Use Limitation.** The use and disclosure of health information should be limited to those purposes specified by the data recipient. Certain exceptions such as law enforcement or security may warrant reuse of data for other purposes. However, when data is used for purposes other than those originally specified, prior de-identification of the data can help protect individual privacy while enabling important benefits to be derived from the information.

**Individual Participation and Control.** Every individual should retain the right to request and receive in a timely and intelligible manner information regarding who has that individual’s health data and what specific data the party has, to know any reason for a denial of such request, and to challenge or amend any personal information. Because individuals have a vital stake in their own personal health information, such rights enable them to be participants in the collection and use of their data. Individual participation promotes data quality, privacy, and confidence in privacy practices.

**Data Integrity and Quality.** Health data should be accurate, complete, relevant, and up-to-date to ensure its usefulness. The quality of health care depends on the existence of accurate health information. Moreover, individuals can be adversely affected by inaccurate health information in other arenas like insurance and employment. Thus, the integrity of health data must be maintained and individuals must be permitted to view information about them and amend such health information so that it is accurate and complete.

**Security Safeguards and Controls.** Security safeguards are essential to privacy protection because they help prevent data loss, corruption, unauthorized use, modification, and disclosure. With increasing levels of cyber-crime, networked environments may be particularly susceptible without adequate security controls. Design and implementation of various technical security precautions such as identity management tools, data scrubbing, hashing, auditing, authenticating, and other tools can strengthen information privacy.

**Accountability and Oversight.** Privacy protections have little weight if privacy violators are not held accountable for compliance failures. Employee training, privacy audits, and other oversight tools can help to identify and address privacy violations and security breaches by holding accountable those who violate
privacy requirements and identifying and correcting weaknesses in their security systems.

**Remedies.** The maintenance of privacy protection depends upon legal and financial means to remedy any privacy or security breaches. Such remedies should hold violators accountable for compliance failures, reassure individuals about the organization’s commitment to information privacy, and mitigate any harm that privacy violations may cause individuals.

These nine principles underlie the recommended model privacy policies presented below. While certain principles are emphasized by each individual policy, the policies as a whole balance all of the principles equally so that certain principles are not emphasized over others—which would undermine the effectiveness of the overall approach. Moreover, the policies are individual elements of an integrated and comprehensive Connecting for Health policy framework—The Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange—that is intended to be considered in its entirety. In that regard, please refer to the following additional materials developed by the Connecting for Health Policy Subcommittee: “A Model Contract for Health Information Exchange,” “Background Issues on Data Quality,” “Auditing Access to and Use of a Health Information Exchange,” “Breaches of Confidential Health Information,” “Authentication of System Users,” “Notification and Consent When Using a Record Locator Service,” “Patients’ Access to Their Own Health Information,” and “Correctly Matching Patients with Their Records.”

Although most of the recommended model policies can and should be implemented in the current technological environment, there are a few for which organizational and technical barriers may currently be prohibitive. For example, although patients would benefit from access to the RLS and the ability to obtain audit trails of those who have requested information about them from the index, technical and administrative barriers currently do not allow for such access. Health care participants, system vendors, and others should work toward implementing these functionalities as they will enhance privacy protections and help implement the privacy principles of openness and transparency, security safeguards and controls, purpose specification and minimization, use limitation, collection limitation, and accountability. Similarly, in the future, Participants and vendors should seek to realize the other policies that cannot be implemented at this time due to organizational and technical constraints.

The emergence of a networked electronic health information environment will transform patient care and improve the efficiency and effectiveness of the health system. At the same time, the emerging electronic health information infrastructure and the massive increase in the volume of health data that is easily collected, linked, and disseminated create unprecedented privacy and security risks that need to be adequately and appropriately addressed. By incorporating the principles outlined above and the basic requirements set forth in HIPAA, these recommended model policies seek to achieve a balance between maintaining the confidentiality of health information and maximizing the benefits of using such information. Integration of these privacy measures into the emerging networked health care environment can ensure that the benefits of electronic health information are realized while the confidentiality of health information is preserved.

Each of the recommended privacy policies outlined below contains an introductory section that provides background and explains the basis for the policy in law, the privacy principles described above, and other sources. The introductory sections are followed by recommended language for use by SNOs in drafting their own Policies and Procedures to use in conjunction with the Connecting for Health “Model Contract for Health Information Exchange.”

**SNO Policy 100: Compliance with Law and Policy**

**Purpose and Principles:** In the spirit of the privacy principles of openness and transparency, data integrity and quality, accountability and
oversight, and remedies, a requirement that Participants comply with applicable law and SNO policies and promulgate the internal policies required for such compliance is indispensable to the successful realization of essential privacy protections. In addition, the recommended model provision below governing conflicts between SNO policies and Participant policies, which states that the policy that is most protective of individual privacy should govern decision making, is designed to make clear that the policies provide a floor and Participants may choose to enhance privacy protections where appropriate. This deference to more protective policies echoes the HIPAA federal pre-emption requirements which do not preempt more protective state privacy laws.3

The recommended policy's requirement that Participants develop internal policies will help implement the principles of sound data management practices and accountability as well as ensure that decisions affecting individuals' privacy interests are made thoughtfully, rather than on an ad hoc basis. Written documentation of such policies facilitates the training of personnel who will handle health information and enhances the accountability of both Participants and members of their workforce. Finally, the existence of internal policies for compliance with applicable law and SNO policies creates transparency surrounding Participants' handling and safeguarding of data. Policies to establish privacy protection compliance, enforcement procedures and remedies following violations are crucial to maintaining health information privacy.

Recommended Language
Scope and Applicability: This Policy applies to all Participants that have registered with and are participating in the SNO and the RLS and that may provide, make available, or request health information through the SNO and the RLS.

Policy:
1. Laws. Each Participant shall, at all times, comply with all applicable federal, state, and local laws and regulations, including, but not limited to, those protecting the confidentiality and security of individually identifiable health information and establishing certain individual privacy rights. Each Participant shall use reasonable efforts to stay abreast of any changes or updates to and interpretations of such laws and regulations to ensure compliance.

2. SNO Policies. Each Participant shall, at all times, comply with all applicable SNO policies and procedures (“SNO Policies”). These SNO Policies may be revised and updated from time to time upon reasonable written notice to Participant. Each Participant is responsible for ensuring it has, and is in compliance with, the most recent version of these SNO Policies.

3. Participant Policies. Each Participant is responsible for ensuring that it has the requisite, appropriate, and necessary internal policies for compliance with applicable laws and these SNO Policies. In the event of a conflict between these SNO Policies and an institution's own policies and procedures, the Participant shall comply with the policy that is more protective of individual privacy and security.

SNO Policy 200:
Notice of Privacy Practices
Purpose and Principles: This recommended policy incorporates the HIPAA requirements obligating entities to provide individuals a notice of the entities' privacy practices.4 The policy exceeds HIPAA's requirements by also requiring disclosures to individuals of certain information related to the SNO and RLS.5 For example, under the model policy, the Privacy Notice should inform individuals about what information the Participant may make available

4 45 C.F.R. § 164.520.
5 HIPAA requires the Notice of Privacy Practices to include a description, with “at least one example, of the types of uses and disclosures that the covered entity is permitted ... to make for ... treatment, payment and health care operations” and a description of those other purposes for which the entity “is permitted or required ... to use or disclose protected health information without” individual authorization. 45 C.F.R. § 164.520(b)(1)(ii)(A). Unlike this recommended model policy, HIPAA does not require the Privacy Notice to set forth what specific information may be disclosed and who may access the information.
through the SNO and RLS, who is able to access
the information, and how they can have
information concerning them removed from the
RLS. These are not HIPAA requirements, but
rather build and expand upon the privacy law to
help incorporate information related to the NHIN
and the RLS. This recommended model policy
also exceeds HIPAA's requirements by providing
suggestions for additional, voluntary protections
that could be implemented on the Participant
level to enhance consumer protections, such as
excluding individuals from the RLS index unless
prior consent is obtained or loading information
into the RLS only after a notification and
opportunity to decline participation has been
provided to individual patients.

This recommended model policy promotes
the privacy principles of openness and
transparency, purpose specification and
minimization, use limitation, collection limitation,
and individual participation and control. In
addition, the model policy helps ensure that
information is collected and shared electronically
in a fair manner with the knowledge of relevant
individuals, which is particularly important in a
networked environment where the technology
may be unfamiliar to average users.

**Recommended Language**

**Scope and Applicability:** This Policy applies to
all Participants that have registered with and are
participating in the SNO and the RLS and that
may provide or make available health
information through the SNO and the RLS.

**Policy:**
Each Participant shall develop and maintain a
notice of privacy practices (the “Notice”) that
complies with applicable law and this Policy.

1. **Content.** The Notice shall meet the content
requirements set forth under the HIPAA
Privacy Rule and comply with all applicable
laws and regulations. The Notice also shall
include a description of the SNO and the
RLS and inform individuals regarding: (1)
what information the institution may include
in and make available through the SNO and
the RLS; (2) who is able to access the
information in the SNO and the RLS; (3) for
what purposes such information can be
accessed; and (4) how the individual can
have his or her information removed from the
RLS.

2. **Provision to Individuals.** Each Participant
shall have its own policies and procedures
governing distribution of the Notice to
individuals, which policies and procedures
shall be consistent with this Policy and
comply with applicable laws and regulations.

- For Participants that are health care
  providers, the Notice shall be: (1)
available to the public upon request; (2)
posted on all web sites of the Participant
and available electronically through such
sites; (3) provided to a patient at the date
of first service delivery; (4) available at
the institution; and (5) posted in a clear
and prominent location where it is
reasonable to expect individuals seeking
service to be able to read the Notice.

- For Participants that are health plans, the
  Notice shall be: (1) available to the public
upon request; (2) provided to new
enrollees at the time of plan enrollment;
(3) provided to current plan enrollees
within 60 days of a material revision; and
(4) posted on the plan's web sites and
available electronically through such sites.
Participating health plan institutions also
shall notify individuals covered by the plan
of the availability of the Notice and how to
obtain a copy at least once every three
years.

3. **Individual Acknowledgement.** Each
Participant that is a health care provider
shall make a good faith effort to obtain the
individual's written acknowledgement of
receipt of the Notice or to document their
efforts and/or failure to do so. The
acknowledgement of the Notice shall comply
with all applicable laws and regulations.
Each Participant shall have its own policies
and procedures governing obtaining an

---

6 45 C.F.R. § 164.520(b).

7 See 45 C.F.R. § 164.520(c)(2), (3).

8 See 45 C.F.R. § 164.520(c)(1), (3).

9 See 45 C.F.R. § 164.520(c)(2)(ii).
acknowledgement, which policies and procedures shall be consistent with this Policy and comply with applicable laws and regulations.

4. **Participant Choice.** Participants may choose a more proactive notice distribution process than provided herein and may include more detail in their notice of privacy practices. Possible additional protections for individuals whose information may be made available through the RLS (not all of which pertain to notice policies alone) could include: mailing the revised notice or a notification letter allowing for removal or exclusion of the information about that individual from the RLS to every individual prior to loading the information into the RLS or shortly thereafter; excluding individuals from the RLS index unless individual consent is obtained; loading individual information into the RLS on a going-forward, new individual encounter basis only; developing a method for time-stamping an RLS record to indicate when the record was loaded into the index; developing a method for allowing individuals to limit access to their RLS records; and obtaining individual consent prior to each inquiry made to the RLS index by a Participant, or on a periodic basis.

**SNO Policy 300: Individual Participation and Control of Information Posted to the RLS**

**Purpose and Principles:** This recommended model policy provides greater privacy protection over personal health information than the HIPAA Privacy Rule by allowing individuals to elect whether or not to have information about them included in the RLS. Importantly, individuals are treated as participants in the process of health information collection and dissemination, rather than as spectators. Providing such consumer protections allows individuals to better understand the conditions under which information concerning them might be used, to restrict such use, and to develop confidence in the protections surrounding the use of their data.

This model policy promotes the privacy principles of individual participation and control, purpose specification and minimization, use limitation, and collection limitation. By enhancing reasonable individual control over the collection and use of health information the policy will promote consumer confidence that health information is being used and collected in accordance with individual preferences.

**Recommended Language**

**Scope and Applicability:** This Policy applies to all institutions that have registered with and are participating in the SNO and the RLS and that may provide or make available health information through the SNO and the RLS.

**Policy:**

1. **Choice Not to Have Information Included in the RLS.** All individuals may choose not to have information about them included in or made available through the RLS.

2. **Effect of Choice.** An individual’s choice not to have information about him or her included in or made available through the RLS shall be exercised through the Participant, as described in the institution’s Notice, after which time the institution shall no longer include the individual in the RLS. Participants shall develop and implement appropriate mechanisms to remove information about an individual from the RLS if the individual chooses to have such information excluded from the RLS.

3. **Revocation.** An individual who has chosen not to make information concerning him or her available through the RLS subsequently may be included in the RLS only if the individual revokes his or her decision or subsequently chooses to renew participation in the RLS.

4. **Documentation.** Each Participant shall document and maintain documentation of all patients’ decisions not to have information about them included in the RLS.

5. **Participant Choice.** Participants shall establish reasonable and appropriate processes to enable the exercise of a patient’s choice not to have information...
about him or her included in the RLS. Each Participant retains the authority to decide whether and when to obtain patient consent prior to making information available through the RLS.

6. **Provision of Coverage or Care.** A Participant shall not withhold coverage or care from an individual on the basis of that individual’s choice not to have information about him or her included in the RLS.

**SNO Policy 400: Uses and Disclosures of Health Information**

**Purpose and Principles:** Through a variety of mechanisms, this model policy reflects the privacy principles of purpose specification and minimization, security safeguards and controls, use limitation, collection limitation, accountability and oversight, and data integrity and quality. The recommended policy integrates HIPAA’s general premise that health information may be used only for permissible purposes and its more specific requirement that entities may disclose only the amount of information reasonably necessary to achieve a particular purpose. In general, requests for disclosure of and/or use of health information for treatment, payment, and the health care operations of a covered entity, as each is defined by HIPAA, will be permitted. Furthermore, subject to certain limitations and under certain circumstances, requesting disclosure of and using health information for law enforcement, disaster relief, research, and public health purposes also may be permissible. Accessing health information through either the RLS or the SNO for marketing or marketing-related purposes is prohibited without specific patient authorization. Under no circumstances may health information be accessed or used for discriminatory purposes. For example, a health plan would not be permitted to use the RLS to determine if a member has visited a health care provider for whom the health plan has not been billed. Such activity would be an impermissible and discriminatory purpose and is prohibited by applicable law and under this Policy. SNOs may provide guidance to Participants detailing the permissibility or impermissibility of requesting or using health information for certain specified purposes under applicable law.

Requiring consideration of the purpose of a use and minimization of the use of information reduces the likelihood of inadvertent or intentional misuses of information. The model policy helps enhance the fair and legal collection and use of data, the oversight of data use and accountability for privacy violations by ensuring that Participants have legally required documentation prior to the use or disclosure of information. In addition, the integration of HIPAA’s accounting of disclosures and individual access to information requirements allows individuals to understand how health information about them is shared and to exercise certain rights regarding information about them with greater precision and ease.

The recommended provision also requires security measures essential to identify and remedy loss, unauthorized access, destruction, use, modification, or disclosure of personal health information. The audit requirement reflects the HIPAA Security Rule’s general
requirement that entities implement policies to prevent security violations, assess security risks, and examine data storage and access technology but, in a manner more protective than HIPAA, would establish monitoring requirements as to when information is accessed and by whom. To prevent unauthorized access of information and maintain data integrity and quality the authentication provision of the model policy requires that both the identity and authority of an entity requesting health information be verified and authenticated, integrating requirements from the HIPAA Privacy Rule and Security Rule.

The combination of this recommended policy’s use and security provisions helps guarantee that health information is used and accessed only as authorized and that Participants have proper measures in place to identify and address privacy violations. Consequently, individuals can remain confident that information about them is being used with care and in the manner promised by Participants.

**Recommended Language**

**Scope and Applicability:** This Policy applies to all institutions that have registered with and are participating in the SNO and that may provide, make available, or request health information through the SNO.

**Policy:**

1. **Compliance with Law.** All disclosures of health information through the SNO and the use of information obtained from the SNO shall be consistent with all applicable federal, state, and local laws and regulations and shall not be used for any unlawful discriminatory purpose. If applicable law requires that certain documentation exist or that other conditions be met prior to using or disclosing health information for a particular purpose, the requesting institution shall ensure that it has obtained the required documentation or met the requisite conditions and shall provide evidence of such at the request of the disclosing institution.

2. **Purposes.** A Participant may request health information through the RLS or SNO only for purposes permitted by applicable law. Each Participant shall provide or request health information through the RLS or SNO only to the extent necessary and only for those purposes that are permitted by applicable federal, state, and local laws and regulations and these Policies. Information may not be requested for marketing or marketing related purposes without specific patient authorization. Under no circumstances may information be requested for a discriminatory purpose. In the absence of a permissible purpose, a Participant may not request information through the RLS or from the SNO.

3. **SNO Policies.** Uses and disclosures of and requests for health information via the SNO shall comply with all SNO Policies, including, but not limited to, the SNO Policy on Minimum Necessary and the SNO Policy on Information Subject to Special Protection.

4. **Participant Policies.** Each Participant shall refer to and comply with its own internal policies and procedures regarding disclosures of health information and the conditions that shall be met and documentation that shall be obtained, if any, prior to making such disclosures.

5. **Accounting of Disclosures.** Each Participant disclosing health information through the SNO shall work towards implementing a system to document the purposes for which such disclosures are made, as provided by the requesting institution, and any other information that may be necessary for compliance with the HIPAA Privacy Rule’s accounting of disclosures requirement. Each Participant is responsible for ensuring its compliance with such requirement and may choose to

---

19 45 C.F.R. §§ 164.316, 164.308(a)(1)(i).
20 45 C.F.R. §§ 164.514(h), 164.312(d).
21 See 45 C.F.R. § 164.530(j).
22 45 C.F.R. § 164.502(a), (b).
23 45 C.F.R. § 164.502(b).
24 45 C.F.R. § 164.528. For HIPAA Covered Entities, this is currently required by law.
provide individuals with more information in the accounting than is required. Each requesting institution shall provide information required for the disclosing institution to meet its obligations under the HIPAA Privacy Rule’s accounting of disclosures requirement.

6. Audit Logs. Participants and SNOs shall consider and work towards maintaining an audit log documenting which Participants posted and accessed the information about an individual through the RLS and when such information was posted and accessed. Participants and SNOs shall consider and work towards implementing a system wherein, upon request, patients have a means of seeing who has posted and who has accessed information about them through the RLS and when such information was accessed.

7. Authentication. Each Participant shall follow uniform minimum authentication requirements for verifying and authenticating those within their institutions who shall have access to, as well as other Participants who request access to, information through the SNO and/or the RLS.

8. Access. Each SNO should have a formal process through which information in the RLS can be requested by a patient or on a patient’s behalf. Participants and SNOs shall consider and work towards providing patients direct access to the information contained in the RLS that is about them.

SNO Policy 500: Information Subject to Special Protection

Purpose and Principles: This model policy promotes the privacy principles of purpose specification and minimization, security safeguards and controls, use limitation, data integrity and quality, collection limitation, and individual participation and control. This recommended provision facilitates individualized privacy protections by requiring Participants to heed any special protections of certain information set forth under applicable law. In complying with these special protections, Participants’ collection, use and disclosure of health information is limited to legitimate purposes. Moreover, in guaranteeing deference to the law or policy most protective of privacy, the provision below echoes HIPAA’s federal preemption requirements which defer to state laws that are more protective than HIPAA’s own privacy provisions.

Recommended Language

Scope and Applicability: This Policy applies to all institutions that have registered with and are participating in the SNO and that may provide or make available health information through the SNO.

Policy:

Some health information may be subject to special protection under federal, state, and/or local laws and regulations (e.g., substance abuse, mental health, and HIV). Each Participant shall determine and identify what information is subject to special protection under applicable law prior to disclosing any information through the SNO. Each Participant is responsible for complying with such laws and regulations.

SNO Policy 600: Minimum Necessary

Purpose and Principles: To promote the privacy principles of collection limitation, use limitation, data integrity and quality, and security safeguards and controls, this recommended model policy incorporates HIPAA’s requirement that entities may disclose only the amount of information reasonably necessary to achieve a particular purpose. The policy exempts treatment disclosures from this minimum necessary requirement to balance the protection of privacy and the provision of quality

---

27 See 45 C.F.R. §§ 164.514(h), 164.312(d).
29 See 45 C.F.R. § 164.524.
30 See Connecting for Health, “Patients’ Access to Their Own Health Information.”
31 45 C.F.R. § 164.203.
32 45 C.F.R. § 164.502(b).
health care. In assessing the smallest amount of information that is necessary to accomplish a particular purpose, Participants are less likely to collect, use or disclose information for an unauthorized purpose. Minimal collection, access, use and disclosure increases public confidence in the privacy practices of Participants, enhances information privacy, and diminishes the potential for data corruption and security violations.

**Recommended Language**

**Scope and Applicability**: This Policy applies to all institutions that have registered with and are participating in the SNO and that may provide, make available, or request health information through the SNO.

**Policy**:  
1. **Uses.** Each Participant shall use only the minimum amount of health information obtained through the SNO as is necessary for the purpose of such use. Each Participant shall share health information obtained through the SNO with and allow access to such information by only those workforce members, agents, and contractors who need the information in connection with their job function or duties.

2. **Disclosures.** Each Participant shall disclose through the SNO only the minimum amount of health information as is necessary for the purpose of the disclosure. Disclosures to a health care provider for treatment purposes and disclosures required by law are not subject to this Minimum Necessary Policy.

3. **Requests.** Each Participant shall request only the minimum amount of health information through the SNO as is necessary for the intended purpose of the request. This Minimum Necessary Policy does not apply to requests by health care providers for treatment purposes.

4. **Entire Medical Record.** A Participant shall not use, disclose, or request an individual’s entire medical record except where specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request. This limit does not apply to disclosures to or requests by a health care provider for treatment purposes or disclosures required by law.

**SNO Policy 700: Workforce, Agents, and Contractors**

**Purpose and Principles**: By incorporating HIPAA’s administrative requirements for workforce training, sanctions for privacy violations, and the reporting of complaints, this recommended model policy advances the privacy principles of use limitation, security safeguards and controls, accountability and oversight, data integrity and quality, and remedies. Because a Participant’s workforce is responsible for implementation of privacy practices, proper training is vital to ensure the legitimate use of health information and the prompt identification, reporting, and correction of any security weaknesses. Individual accountability in the form of sanctions for those persons responsible for privacy violations is fundamental to encouraging compliance with privacy practices. Without such incentive for compliance, privacy violations and security risks may go unchecked and lead to larger privacy problems. Similarly, providing for the reporting of non-compliance enables Participants to discover and correct privacy violations and identify and sanction privacy violators. This model policy helps guarantee the legitimate use of health data, the proper implementation of Participants’ privacy practices, and the prompt identification of and undertaking of remedial action for privacy violations.

**Recommended Language**

**Scope and Applicability**: This Policy applies to all institutions that have registered with and are participating in the SNO and that may provide, make available, or request health information through the SNO.

**Policy**:  
1. **Access to System.** Each Participant shall allow access to the SNO only by those workforce members, agents, and contractors who have a legitimate and appropriate need to use the SNO and/or 

---

33 45 C.F.R. § 164.530.
release or obtain information through the SNO. No workforce member, agent, or contractor shall be provided with access to the SNO without first having been trained on these Policies, as set forth below.

2. Training. Each Participant shall develop and implement a training program for its workforce members, agents, and contractors who will have access to the SNO to ensure compliance with these Policies. The training shall include a detailed review of applicable Policies and each trained workforce member, agent, and contractor shall sign a representation that he or she received, read, and understands these Policies.

3. Discipline for Non-Compliance. Each Participant shall implement procedures to discipline and hold workforce members, agents, and contractors accountable for ensuring that they do not use, disclose, or request health information except as permitted by these Policies and that they comply with these Policies. Such discipline measures shall include, but not be limited to, verbal and written warnings, demotion, and termination and provide for retraining where appropriate.

4. Reporting of Non-Compliance. Each Participant shall have a mechanism for, and shall encourage, all workforce members, agents, and contractors to report any non-compliance with these Policies to the Participant. Each Participant also shall establish a process for individuals whose health information is included in the RLS to report any non-compliance with these Policies or concerns about improper disclosures of information about them.

**SNO Policy 800: Amendment of Data**

**Purpose and Principles:** This recommended model policy integrates the right granted by the HIPAA Privacy Rule of individuals to amend health information about them under certain circumstances. Accurate health information not only is indispensable to the delivery of health care, but is important to individuals’ applications for insurance and employment and in a variety of other arenas. Allowing individuals to verify the accuracy and completeness of information concerning them contributes to the transparency of Participants’ operations and fosters confidence in Participants’ privacy practices and commitment to data accuracy. This policy promotes the privacy principles of data integrity and quality, openness and transparency, individual participation and control, and accountability and oversight. Using such a model policy will enable Participants to more readily rely upon the integrity and quality of their data and more easily monitor, account for, and remedy systemic data inaccuracies, corruptions, and other data deficiencies or privacy lapses.

**Recommended Language**

**Scope and Applicability:** This Policy applies to all institutions that have registered with and are participating in the SNO and that may provide, make available, or request health information through the SNO.

Policy:

Each Participant shall comply with applicable federal, state and local laws and regulations regarding individual rights to request amendment of health information. If an individual requests, and the Participant accepts, an amendment to the health information about the individual, the Participant shall make reasonable efforts to inform other Participants that accessed or received such information through the SNO, within a reasonable time, if the recipient institution may have relied or could foreseeably rely on the information to the detriment of the individual.

**SNO Policy 900: Requests for Restrictions**

**Purpose and Principles:** To advance the privacy principles of individual participation and control, use limitation and accountability and oversight, this recommended model policy

---

34 See 45 C.F.R. § 164.530(b).
35 45 C.F.R. § 164.530(e).
36 See 45 C.F.R. § 164.530(a), (d).
37 45 C.F.R. § 164.526.
38 45 C.F.R. § 164.526.
requires Participants who agree to individuals’ request for restrictions in accordance with the HIPAA Privacy Rule to comply with such request with regard to the release of information in the SNO. Such compliance ensures permissible use of health information and accountability on the part of Participants who agree to individually requested use restrictions. Without the ability to request restrictions and without assurance that Participants will honor these agreed-upon restrictions, individuals may remain silent about important information that could affect their health. By creating confidence in Participants and their privacy protections and encouraging individual participation, this policy fosters dialog between individuals and Participants. Improved communications between a provider and patient improves the overall delivery of health care.

**Recommended Language**

**Scope and Applicability:** This Policy applies to all institutions that have registered with and are participating in the SNO and that may provide or make available health information through the SNO.

**Policy:**
If a Participant agrees to an individual’s request for restrictions, as permitted under the HIPAA Privacy Rule, such Participant shall ensure that it complies with the restrictions when releasing information through the SNO. If an agreed-upon restriction will or could affect the requesting institution’s uses and/or disclosures of health information, at the time of disclosure, the Participant disclosing such health information shall notify the requesting institution of the fact that certain information has been restricted, without disclosing the content of any such restriction.

---

39 45 C.F.R. § 164.522.

40 Under the HIPAA Privacy Rule, individuals have the right to request restrictions on the use and/or disclosure of health information about them. 45 C.F.R. § 164.522. For example, an individual could request that information not be used or disclosed for a particular purpose or that certain information not be disclosed to a particular individual. Covered entities are not required to agree to such requests under HIPAA.

---

**SNO Policy 1000: Mitigation**

**Purpose and Principles:** By incorporating HIPAA’s requirement that entities have procedures to and take steps to mitigate harm resulting from an impermissible use or disclosure of health information, this model policy reflects the privacy principles of remedies, accountability and oversight, security safeguards and controls, openness and transparency, and data integrity and quality. Without the duty to mitigate harm from privacy violations, Participants may not promptly address data security weaknesses or breaches which could lead to greater privacy lapses in the future, diminish the confidence that individuals have in Participants’ privacy practices, and compromise the accuracy, integrity, and quality of Participants’ data. Remedial action and mitigation are essential both to reassure individuals that Participants are vigilant in addressing privacy violations and ameliorating any harm from such violations and to help Participants ensure that their data oversight practices and security measures are functioning and effective.

**Recommended Language**

**Scope and Applicability:** This Policy applies to all institutions that have registered with and are participating in the SNO and that may provide, make available, or request health information through the SNO.

**Policy:**
Each Participant shall implement a process to mitigate, and shall mitigate and take appropriate remedial action, to the extent practicable, any harmful effect that is known to the institution of a use or disclosure of health information through the SNO in violation of applicable laws and/or regulations and/or these Policies by the institution, or its workforce members, agents, and contractors. Steps to mitigate could include, among other things, Participant notification to the individual of the disclosure of information about them or Participant request to the party who received such information to return and/or destroy the impermissibly disclosed information.

---

41 45 C.F.R. § 164.530(f).
Acknowledgements
The members of the Connecting for Health Policy Subcommittee have accomplished an extraordinary task in less than a year’s time—the development of an evolving piece of work that can serve as the core of nationwide health information exchange—the policy components of The Common Framework. During this time, we have been fortunate to work with respected experts in the fields of health, information technology, and privacy law, all of whom have contributed their time, energy, and expertise to a daunting enterprise. Our consultants and volunteers have worked long hours in meetings and conference calls to negotiate the intricacies of such issues as privacy, security, authentication, notification, and consent in health information exchange. We offer them our heartfelt thanks for taking on this journey with us, and look forward to the remaining work ahead.

In addition, we would like to offer special thanks to the volunteers and consultants who authored the initial drafts of this body of work—their hard work created a strong foundation upon which to focus the Subcommittee’s deliberations: Stefaan Verhulst, Clay Shirky, Peter Swire, Gerry Hinkley, Allen Briskin, Marcy Wilder, William Braithwaite, and Janlori Goldman.

Finally, we must note that none of this work would have been possible without the leadership and inspiration of our co-chairs, William Braithwaite and Mark Frisse. They have led us with steady hands and determination of spirit.

Connecting for Health Policy Subcommittee

**William Braithwaite**, MD, eHealth Initiative, (Co-Chair)

**Mark Frisse**, MD, MBA, MSc, Vanderbilt Center for Better Health, (Co-Chair)

**Laura Adams**, Rhode Island Quality Institute

**Phyllis Borzi**, JD, George Washington University Medical Center

**Susan Christensen***, JD, Agency for Healthcare Research and Quality, United States Department of Health and Human Services

**Art Davidson**, MD, MSHP, Denver Public Health

**Mary Jo Deering***, PhD, National Cancer Institute/National Institutes of Health, United States Department of Health and Human Services

**Jim Dempsey**, JD, Center for Democracy and Technology

**Hank Fanberg**, Christus Health

**Linda Fischetti***, RN, MS, Veterans Health Administration

**Seth Foldy**, MD, City of Milwaukee Health Department

**Janlori Goldman**, JD, Columbia College of Physicians and Surgeons

**Ken Goodman**, PhD, University of Miami

**John Halamka**, MD, CareGroup Healthcare System

**Joseph Heyman**, MD, American Medical Association

**Gerry Hinkley**, JD, Davis, Wright, Tremaine LLP

**Charles Jaffe**, MD, PhD, Intel Corporation

**Jim Keese**, Eastman Kodak Company

**Linda Kloss**, RHIA, CAE, American Health Information Management Association

**Gil Kuperman**, MD, PhD, New York-Presbyterian Hospital

**Ned McCulloch**, JD, IBM Corporation

**Patrick McMahon**, Microsoft Corporation

**Omid Moghadam**, Intel Corporation
Joyce Niland, PhD, City of Hope National Medical Center

Louise Novotny, Communication Workers of America

Michele O’Connor, MPA, RHIA, MPI Services Initiate

Victoria Prescott, JD, Regenstrief Institute for Healthcare

Marc A. Rodwin, JD, PhD, Suffolk University Law School

Kristen B. Rosati, JD, Coppersmith Gordon Schermer Owens & Nelson PLC

Sara Rosenbaum, JD, George Washington University Medical Center

David A. Ross, ScD, Public Health Informatics Institute

Clay Shirky, New York University (Chair, Technical Subcommittee)

Don Simborg, MD, American Medical Informatics Association

Michael Skinner, Santa Barbara Care Data Exchange

Joel Slackman, BlueCross/BlueShield Association

Peter P. Swire, JD, Moritz College of Law, Ohio State University

Paul Tang, MD, Palo Alto Medical Foundation

Micky Tripathi, Massachusetts eHealth Collaborative

Cynthia Wark*, CAPT, United States Public Health Service Commissioned Corps, Centers for Medicare and Medicaid Services, United States Department of Health and Human Services

John C. Wiesendanger, MHS, West Virginia Medical Institute/Quality Insights of Delaware/Quality Insights of Pennsylvania

Marcy Wilder, JD, Hogan & Hartson LLP

Scott Williams, MD, MPH, HealthInsight

Robert B. Williams, MD, MIS, Deloitte

Joy Wilson, National Conference of State Legislatures

Rochelle Woolley, RxHub

Amy Zimmerman-Levitan, MPH, Rhode Island State Department of Health

*Note: Federal employees participate in the Subcommittee but make no endorsement
Notification and Consent
When Using a Record Locator Service
Notification and Consent When Using a Record Locator Service
The document you are reading is part of The Connecting for Health Common Framework, which is available in full and in its most current version at: http://www.connectingforhealth.org/. The Common Framework will be revised and expanded over time. As of October 2006, the Common Framework included the following published components:

- **Policy Guides: How Information is Protected**
  - P1: The Architecture for Privacy in a Networked Health Information Environment
  - P2: Model Privacy Policies and Procedures for Health Information Exchange
  - P3: Notification and Consent When Using a Record Locator Service
  - P4: Correctly Matching Patients with Their Records
  - P5: Authentication of System Users
  - P6: Patients’ Access to Their Own Health Information
  - P7: Auditing Access to and Use of a Health Information Exchange
  - P8: Breaches of Confidential Health Information
  - P9: A Common Framework for Networked Personal Health Information

- **Technical Guides: How Information is Exchanged**
  - T1: The Common Framework: Technical Issues and Requirements for Implementation
  - T2: Health Information Exchange: Architecture Implementation Guide
  - T3: Medication History Standards
  - T4: Laboratory Results Standards
  - T5: Background Issues on Data Quality
  - T6: Record Locator Service: Technical Background from the Massachusetts Prototype Community

**Future Technical Guides**

**Future Policy Guides**

**Model Contractual Language**
- M1: Key Topics in a Model Contract for Health Information Exchange
- M2: A Model Contract for Health Information Exchange
Notification and Consent When Using a Record Locator Service*

Statement of Issue
Protecting medical privacy and confidentiality in the context of the Record Locator Service (RLS) involves a wide range of issues. Providing adequate confidence in the RLS will require more than a piecemeal approach to privacy. The Connecting for Health Policy Subcommittee therefore proposes and emphasizes the need for a systematic and architectural approach to these issues. The foundations of this approach depend on the balanced implementation of the following nine principles associated with fair information practices:

1. Openness and Transparency
2. Purpose Specification and Minimization
3. Collection Limitation
4. Use Limitation
5. Individual Participation and Control
6. Data Integrity and Quality
7. Security Safeguards and Controls
8. Accountability and Oversight
9. Remedies

Considered and applied together, these principles enable the development of an integrated and comprehensive approach to privacy that can be built into any information-sharing system or network at the outset in order to ensure confidentiality and privacy of patient data. It is critical that the nine principles be balanced together and considered as part of one package, as elevating certain principles over others will weaken the overall architectural solution, and no one principle can assure confidentiality and privacy of patient data on its own. It is not true, for instance, that just because patient consent (control) over the use or dissemination of information is obtained that it can alone take the place of an integrated approach to protecting the privacy of information addressed by the other eight principles. We therefore recommend that an institution or provider participating in the RLS develop an actionable policy regime that integrates all nine of the principles and communicates them actively to patients and others involved in sub-network organizations (SNOs).

The particular policy question at issue in this document is: What should an institution or provider participating in the RLS be required to do to inform patients and give them the ability to decide not to be listed in the index? In addressing this question, the Connecting for Health Policy Subcommittee has considered in particular the principles of openness and transparency, individual participation and control, purpose specification and minimization, collection limitation, and use limitation.

While this particular document does not address the remaining principles of data integrity and quality, security safeguards and controls, accountability and oversight, or remedies, the Connecting for Health Policy Subcommittee has developed additional materials that do so. Please refer to the Connecting for Health Common Framework resources, and in particular, “A Model Contract for Health Information Exchange,” “Background Issues on Data Quality,” “Auditing Access to and Use of a Health Information Exchange,” “Breaches of Confidential Health Information,” “Authentication of System Users,” and “Correctly Matching Patients with Their Records.” These papers are individual elements of an integrated

* Connecting for Health thanks Marcy Wilder of Hogan & Hartson LLP for drafting this paper.

©2006, Markle Foundation
This work was originally published as part of The Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange and is made available subject to the terms of a license (License) which may be viewed in its entirety at: http://www.connectingforhealth.org/license.html. You may make copies of this work; however, by copying or exercising any other rights to the work, you accept and agree to be bound by the terms of the License. All copies of this work must reproduce this copyright information and notice.

1 A sub-network organization (SNO) shall operate as a health information data exchange organization (whether regionally or affinity-based) that operates as a part of the National Health Information Network (NHIN), a nationwide environment for the electronic exchange of health information made up of a “network of networks.”
and comprehensive policy framework that is intended to be considered in its entirety.

**Background: Structure of the Record Locator Service**

Requests for protected health information will go through a two-stage process in the context of a Record Locator Service. In the first stage, a participating institution or provider ("Participant") will query the Record Locator Service ("RLS") to see if information about a particular patient exists at other participating institutions. The RLS index would include only the patient name, non-clinical details used to identify the patient (name, date of birth, etc.), and participating institutions where that patient has had care. If the RLS reports that patient information exists at a participating institution, the requester may then contact the listed institution or institutions to request the clinical records, and will need to satisfy the disclosure requirements of those institutions. The RLS itself, however, would only return a pointer to the institution(s) or provider(s) holding the records, and an indication that one or more records for the patient exists at those institutions.

A hallmark of the RLS system is that the RLS index, which will contain patient names and demographic information only, will be maintained separately from any clinical records. This separation of records is a technical specification that was developed specifically to protect patient privacy. Providing transparency and individual control with regard to the RLS helps ensure that the system is adequately and securely populated with patient information so as to be a useful and viable tool, while enabling only a minimal amount of information, given its stated purpose, to be available from the RLS itself—the location of records for a given patient. Its design relies on the participating institution or provider to decide in the first instance whether to load patient information into the RLS. Moreover, it leaves the decision as to whether or not to release clinical records with the individual institution or provider holding the records, acting in compliance with its own disclosure policies and the stated desires of patients, when relevant. The RLS two-step approach: (1) is a key piece of the Connecting for Health architecture that enables the sharing of clinical information to occur without requiring it to be stored in a central repository—it enables clinical information about patients to remain in the hands of the clinicians and institutions that have a direct relationship with the patient; (2) leaves judgments about who should have access to patient information to patients and their providers; and (3) assures that the system is robust and sufficiently useful from an early stage to be considered viable. The RLS two-step process was developed in part to assure that the system would not lead to any increased exposure of personal health information while at the same time providing some early value by establishing a way to readily and efficiently locate records in order to improve health care quality and patient safety. Though clinical records and other personal information will be kept private, and not in the RLS, knowing where a patient might have other health information is a first and important step to improving the health care he or she receives.

**Background: What HIPAA Requires**

The Policy Subcommittee agrees that the HIPAA Privacy Rule would permit participation in the RLS system without a provision requiring for notice to the patient or patient authorization. The Privacy Rule permits covered entities to “use or disclose protected health information for treatment, payment, or health care operations” without first obtaining an individual’s authorization for such use or disclosure. Treatment is defined as “the provision, coordination, or management of health care and related services by one or more health care providers.” Health care operations is broadly defined and includes, for example: “[c]onducting quality assessment and improvement activities, including outcomes evaluation...[and] population-based activities relating to improving health or reducing health care costs.” The

---

2 We note that the RLS index is not a facility directory. A facility directory maintains information about the location and general condition of patients presently at or being treated by an institution whereas the RLS index identifies patients that have received care at an institution and about which the institution maintains records.

3 45 C.F.R. § 164.506.

4 45 C.F.R. § 164.501.

5 Id. § 164.501.
information sharing that the RLS is designed to facilitate falls squarely within the HIPAA sanctioned uses and disclosures that do not require patient authorization. Therefore, the following proposed notice and patient choice policies go above and beyond what is required by the federal HIPAA privacy law and further than what a number of local and regional interoperable systems, such as the Indiana Network for Patient Care, currently require.

**Proposed Privacy Policy**

**Architecture Regarding Posting of Information to the Record Locator Service**

In accordance with the principles of openness and transparency, purpose specification and minimization, collection limitation, use limitation, and individual participation and control, discussed in detail in the *Connecting for Health* “Architecture for Privacy in a Networked Health Information Environment,” the *Connecting for Health* Policy Subcommittee first notes that it is firmly committed to a policy supporting notice to patients and patient choice as to whether to participate in the RLS. In this regard, the *Connecting for Health* Policy Subcommittee recommends that patients be given notice that their health care provider or health plan participates in a system that provides an electronic means for locating their medical records across the providers they are seeing (the RLS). Individuals should also be provided with an opportunity to choose not to have such information about them included in the system. Moreover, the Policy Subcommittee recommends that patients should retain the ability to choose not to participate in the RLS system at any time. It is noted again that these policy recommendations apply only to patient information contained in the RLS; the decision as to whether or not to release clinical records in a given circumstance remains with the individual institution or provider holding the records, acting in compliance with its own disclosure policies, the stated desires of patients, when relevant, and applicable federal and state laws.

The Policy Subcommittee also understands, however, that the operational burden created by requiring that notice be given to patients prior to an institution’s initial loading of patient information into the RLS index might not be practical in some settings and might threaten the robustness and viability of the two-step approach articulated in the *Connecting for Health* architecture. The two-step approach was designed to separate actual clinical data from information about the location of that data in order to limit risk of exposure while at the same time enabling early and significant value in health information exchange.

The Policy Subcommittee therefore proposes that information regarding patients of a participating institution generally be included in the RLS index on day one and going forward. The index would include only patient names, non-clinical details used to identify the patient (name, date of birth, etc.), and participating institutions where that patient has had care. The index would not include patient clinical records. The question of whether information regarding patients previously seen at the participating institution should be posted to the index, and the details of that information (age of information, etc.), would be left to the participating institution.

Further, the Policy Subcommittee encourages participating institutions and providers to exercise additional means of providing for notice and patient choice with regard to participation in the RLS as they deem feasible and appropriate. For example, institutions could choose to provide for written notice and the opportunity to choose not to participate in the RLS to patients prior to an institution’s initial loading of patient information into the RLS index, either en masse, or on an individual basis during patient encounters. An institution or provider might also choose to contact patients via electronic means for those patients for whom it has such information.

Finally, as noted above, the design of the RLS relies in the first instance on the participating institution or provider to decide whether to load patient information into the RLS at all. Additional privacy practices that participating institutions and providers might choose to implement are listed in Section B below.

**Notice of Privacy Practices.** In accordance with these recommendations, Participants must revise their HIPAA Notice of Privacy Practices to include provisions describing the RLS and to offer an opportunity for
individuals to choose not to be included in the RLS. The description must include: (1) what information is included in and made available through the RLS; (2) who is able to access information in the RLS; (3) for what purposes such information can be accessed; and (4) how the patient can choose not to have his or her information from that institution included in the RLS. All patients must be given the HIPAA Privacy Notice during their initial encounter with a provider. Many institutions provide notice at every service delivery date. In addition, the notice must be available at the institution and on request, posted “in a clear and prominent location where it is reasonable to expect individuals seeking service...to be able to read the notice,” and posted on the institution’s website.

**Initial Inquiry Audit.** In a further effort to implement the principles of openness and transparency and individual participation and control, as articulated in “The Architecture for Privacy in a Networked Health Information Environment,” the Connecting for Health Policy Subcommittee recommends that individual participants and SNOs consider and work towards implementing a system that enables an “initial inquiry audit.”

In such a system, individual participants and SNOs would work towards developing a method so that the first time an inquiry is made to the RLS index regarding a particular patient, the patient would be given notice explaining that information about them is included in a system that provides an electronic means for locating their medical records across providers they are seeing (the RLS) and explaining how the patient may choose to have that information excluded from the RLS in the future.

**Patient Access to RLS Record.** In the spirit of the openness and transparency and individual participation and control principles articulated in “The Architecture for Privacy in a Networked Health Information Environment,” the Connecting for Health Policy Subcommittee recommends that Participants and SNOs consider and work towards implementing a system wherein, upon request, patients are provided direct access to the information contained in the RLS that is about them.

The Policy Subcommittee understands that current options for direct patient access and authentication to the RLS are not robust enough to be implemented without the possibility of introducing serious vulnerability to the security of the system.

For this reason, the Policy Subcommittee recommends that, at this point, each SNO should have a formal process through which information in the RLS can be requested by a patient or on a patient’s behalf.

**Analysis**

The Connecting for Health Policy Subcommittee’s Proposal Comports with the Principles of Openness and Transparency, Purpose Specification and Minimization, Collection Limitation, Use Limitation, and Individual Participation and Control.

A. The RLS policy enables openness, transparency, and individual participation while also addressing the Connecting for Health principles of purpose specification and minimization, collection limitation, and use limitation.

- Provides for patient notification by each participating institution, allowing the patient to control whether information is included in the RLS index on a participant-by-participant basis.

- Provides for the development by individual institutions and SNOs of initial inquiry audit mechanisms that would allow additional patient notification and control opportunities at time of first query.

- Provides immediate benefits, including economic benefits, on day one. Information will be more complete and system will be more robust.

- Provides the greatest likelihood of meeting the goals of saving lives and decreasing health care costs through the efficient and timely exchange of information.
• Allows participating institutions to retain complete control over when and whether clinical records are disclosed.

• Imposes less administrative burden on participating institutions.

• Enables future expansion of system.

B. The RLS policy allows institutions to implement additional privacy protections as they deem appropriate.

Posting information to the RLS using a notice and patient choice regime sets a minimum standard for privacy protections that exceeds the requirements of federal law. Moreover, as noted above, Participants retain the authority and ability to be more proactive in their patient notice and individual participation efforts. The Policy Subcommittee encourages participating institutions and providers to exercise additional means of providing for notice and patient choice with regard to participation in the RLS as they deem feasible and appropriate. While the Policy Subcommittee is not currently taking a position on the institution-based implementation of any of the following, such possible additional protections could include:

• Mailing a revised notice or a notification and individual choice letter to every patient prior to the loading of patient information into the RLS or shortly thereafter.

• Excluding individuals from the RLS index unless individual consent is first obtained.

• Loading patient information into the RLS on a going forward basis only (i.e., do not post information regarding treatment prior to the creation of the RLS).

• Providing a mechanism for a patient to receive, upon request, a list of:
  o All providers or institutions which have posted a patient’s demographic information to the RLS; and
  o All users who have requested record locations for that patient.

• Developing a method for time-stamping an RLS record to indicate when the record was loaded to the index, if technically feasible.

• Developing a method for allowing patients to limit access to their RLS records, if technically feasible.

• Developing a method for using a single indication of the existence of one or more patient records at a single location as opposed to reporting the presence of each patient record individually.

• Seeking individual patient participation prior to each inquiry to the RLS index by the participant or on a periodic basis.

C. The RLS policy recognizes that a requirement for prior individual consent to participate in the RLS would likely jeopardize the goals of the RLS framework.

The Connecting for Health Policy Subcommittee carefully considered the option of requiring individual consent prior to including a patient’s information in the RLS. Some parties have referred to this type of consent as “opt-in” consent. While the Policy Subcommittee is firmly committed to a policy supporting notice to patients and patient choice as to whether to participate in the RLS, it also understands that a policy requiring individual consent prior to including a patient’s information in the RLS might threaten the robustness and viability of the system at an early stage, in addition to placing large burdens on the institutions and providers involved. The Policy Subcommittee carefully considered the privacy protections enabled by the RLS architecture, which separates demographic from clinical data, thus minimizing risks associated with inclusion in it, in making its decision not to recommend a policy requiring prior individual consent. In addition, as discussed in Section B above, the Policy Subcommittee encourages participating institutions and providers to implement additional privacy protections and exercise
additional means of providing for notice and patient choice with regard to participation in the RLS as they deem feasible and appropriate.

Finally, the Policy Subcommittee considered the requirements of real-world implementation of the system in addition to the following issues in making its decision not to recommend a policy requiring individual consent prior to including patients’ information in the RLS:

- Requiring patients’ consent to be listed in the RLS prior to their inclusion in the index would create a significant barrier to establishing a functional system. The start-up time and cost associated with obtaining such consent and populating the index would likely be prohibitive. The RLS two-step process, which separates knowing where records are located from knowing what is in them, was developed in part to assure that the system would not lead to increased exposure of personal health information while at the same time providing a way that some information would be readily and efficiently available to locate records while clinical records and other personal information would be kept private. Providing some incremental and early value is of key importance to the success and utility of the system.

- Requiring consent prior to including a patient’s information in the RLS might provide an incentive to obtain a broader consent than necessary due to the time and cost associated with the process, including consent to share the entire contents of clinical records for a broad range of purposes. Such a result would over-emphasize only one of the privacy principles articulated in the Connecting for Health “Architecture for Privacy in a Networked Health Information Environment”—individual participation and control—and could undermine certain of the others, such as purpose specification and minimization. Such consents, in practice, might promote the consolidation of full clinical records in repositories as opposed to fostering a layered architecture that protects privacy by its very design. A requirement for prior consent before posting information to the RLS could ultimately result in reduced privacy protections because such a requirement would stimulate the use of large, consolidated databases and effectively eliminate the rationale for the RLS architecture at all.

- It is administratively and operationally burdensome for participants to obtain, maintain, and track this type of individual consent.

- An approach requiring individual consent to participate in the RLS would likely require stripping local participants of the authority and flexibility to make policies regarding when and how often consent will be obtained (e.g., each time information is queried or retrieved through the system; initially; every year, etc.) and what the policy ought to be regarding revocation of consent.

- An approach requiring individual consent prior to including a patient’s information in the RLS would not permit future expansion of the system without modifying such consent and, therefore, obtaining new consent from each patient.

- An approach requiring individual consent to participate in the RLS creates impediments to use of the system for any purpose, including treatment.

- If individual consent were provided only for certain purposes (e.g., treatment only), it would be difficult to ensure that participating institutions access information only for the permitted purposes.

- If details regarding use of a changing system are not described for a patient in the individual consent materials, the consent process could be considered misleading and raise consumer protection concerns.
Acknowledgements

The members of the Connecting for Health Policy Subcommittee have accomplished an extraordinary task in less than a year’s time—the development of an evolving piece of work that can serve as the core of nationwide health information exchange—the policy components of The Common Framework. During this time, we have been fortunate to work with respected experts in the fields of health, information technology, and privacy law, all of whom have contributed their time, energy, and expertise to a daunting enterprise. Our consultants and volunteers have worked long hours in meetings and conference calls to negotiate the intricacies of such issues as privacy, security, authentication, notification, and consent in health information exchange. We offer them our heartfelt thanks for taking on this journey with us, and look forward to the remaining work ahead.

In addition, we would like to offer special thanks to the volunteers and consultants who authored the initial drafts of this body of work—their hard work created a strong foundation upon which to focus the Subcommittee’s deliberations: Stefaan Verhulst, Clay Shirky, Peter Swire, Gerry Hinkley, Allen Briskin, Marcy Wilder, William Braithwaite, and Janlori Goldman.

Finally, we must note that none of this work would have been possible without the leadership and inspiration of our co-chairs, William Braithwaite and Mark Frisse. They have led us with steady hands and determination of spirit.

Connecting for Health Policy Subcommittee

William Braithwaite, MD, eHealth Initiative, (Co-Chair)

Mark Frisse, MD, MBA, MSc, Vanderbilt Center for Better Health, (Co-Chair)

Laura Adams, Rhode Island Quality Institute

Phyllis Borzi, JD, George Washington University Medical Center

Susan Christensen*, JD, Agency for Healthcare Research and Quality, United States Department of Health and Human Services

Art Davidson, MD, MSHP, Denver Public Health

Mary Jo Deering*, PhD, National Cancer Institute/National Institutes of Health, United States Department of Health and Human Services

Jim Dempsey, JD, Center for Democracy and Technology

Hank Fanberg, Christus Health

Linda Fischetti*, RN, MS, Veterans Health Administration

Seth Foldy, MD, City of Milwaukee Health Department

Janlori Goldman, JD, Columbia College of Physicians and Surgeons

Ken Goodman, PhD, University of Miami

John Halamka, MD, CareGroup Healthcare System

Joseph Heyman, MD, American Medical Association

Gerry Hinkley, JD, Davis, Wright, Tremaine LLP

Charles Jaffe, MD, PhD, Intel Corporation

Jim Keese, Eastman Kodak Company

Linda Kloss, RHIA, CAE, American Health Information Management Association

Gil Kuperman, MD, PhD, New York-Presbyterian Hospital

Ned McCulloch, JD, IBM Corporation

Patrick McMahon, Microsoft Corporation

Omid Moghadam, Intel Corporation
Joyce Niland, PhD, City of Hope National Medical Center

Louise Novotny, Communication Workers of America

Michele O’Connor, MPA, RHIA, MPI Services Initiate

Victoria Prescott, JD, Regenstrief Institute for Healthcare

Marc A. Rodwin, JD, PhD, Suffolk University Law School

Kristen B. Rosati, JD, Coppersmith Gordon Schermer Owens & Nelson PLC

Sara Rosenbaum, JD, George Washington University Medical Center

David A. Ross, ScD, Public Health Informatics Institute

Clay Shirky, New York University (Chair, Technical Subcommittee)

Don Simborg, MD, American Medical Informatics Association

Michael Skinner, Santa Barbara Care Data Exchange

Joel Slackman, BlueCross/BlueShield Association

Peter P. Swire, JD, Moritz College of Law, Ohio State University

Paul Tang, MD, Palo Alto Medical Foundation

Micky Tripathi, Massachusetts eHealth Collaborative

Cynthia Wark*, CAPT, United States Public Health Service Commissioned Corps, Centers for Medicare and Medicaid Services, United States Department of Health and Human Services

John C. Wiesendanger, MHS, West Virginia Medical Institute/Quality Insights of Delaware/Quality Insights of Pennsylvania

Marcy Wilder, JD, Hogan & Hartson LLP

Scott Williams, MD, MPH, HealthInsight

Robert B. Williams, MD, MIS, Deloitte

Joy Wilson, National Conference of State Legislatures

Rochelle Woolley, RxHub

Amy Zimmerman-Levitan, MPH, Rhode Island State Department of Health

*Note: Federal employees participate in the Subcommittee but make no endorsement
Correctly Matching Patients with Their Records
Correctly Matching Patients with Their Records
The document you are reading is part of The Connecting for Health Common Framework, which is available in full and in its most current version at: http://www.connectingforhealth.org/. The Common Framework will be revised and expanded over time. As of October 2006, the Common Framework included the following published components:
Correctly Matching Patients with Their Records*

Introduction

Health institutions with large numbers of records must rely on probability to declare that a given record or set of records matches a set of identifiers (name, gender, date of birth, etc.). The risk of this strategy, of course, is that the matches so recorded may not be accurate. There is some risk of “false negatives”—records that pertain to a patient but are not found. There is a much greater risk, however, from “false positives”—matches with records that do not pertain to the subject patient, but are wrongly returned in a search.

False positive matches carry two forms of risk—privacy risk and clinical risk. The privacy risk is that records pertaining to patients not under the care of a particular clinician will be delivered, exposing personal details to those who have no need for them. The clinical risk is that a clinician will make a decision based on information that is erroneous because it is actually information about a different person, not the subject patient. Although clinicians are trained to make allowances for the fact that there is a significant error rate in clinical information when they make important decisions, the technology for handling such matches still needs to be optimized for a high degree of certainty, and where incorrect matching does occur, the system should err on the side of returning false negatives rather than false positives.

In addition to the technology, however, there also need to be policies spelling out how...

---

*Connecting for Health* thanks William Braithwaite, Senior Vice President and Chief Medical Officer, eHealth Initiative, and Clay Shirky, Adjunct Professor, New York University Graduate Interactive Telecommunications Program, for drafting this paper.

©2006, Markle Foundation

This work was originally published as part of The Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange and is made available subject to the terms of a license (License) which may be viewed in its entirety at: http://www.connectingforhealth.org/license.html. You may make copies of this work; however, by copying or exercising any other rights to the work, you accept and agree to be bound by the terms of the License. All copies of this work must reproduce this copyright information and notice.

---

1 A sub-network organization (SNO) operates as a health information data exchange organization (whether regionally or affinity-based) that operates as a part of the National Health Information Network (NHIN), a nationwide environment for the electronic exchange of health information made up of a “network of networks.”
present a set of demographic details and receive in return zero or more matching record locations. Probability weighted matching can improve the quality of record matching by taking the specific characteristics of records in particular databases into account.

**Issue:** the “false positive match” and the RLS

- What should our recommendations or requirements be for optimizing matching probabilities so as to minimize incidental disclosures and clinical risk caused by false positive matches within the RLS?

**Example:**
Attempt to match: John Q Public, 1043 W. Easy St., Phoenix, AZ 85535, 5556060, 10-24-1950, 482891822.

Which of the potential matches should be returned in response to this query?

---

**Sample Data Listed in Order of Probability of Match**

*Comparison Scoring*
Part of Initiate's Identity Hub Software, [http://www.initiatesystems.com](http://www.initiatesystems.com)
This example from their literature

<table>
<thead>
<tr>
<th>Rec#</th>
<th>Name</th>
<th>Address</th>
<th>Phone</th>
<th>DOB</th>
<th>SSN</th>
<th>Example Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>101</td>
<td>John Q Public</td>
<td>&quot;1043 W. Easy St, Phoenix, AZ 85535&quot;</td>
<td>5556060</td>
<td>10-24-1950</td>
<td>482891822</td>
<td>20.0</td>
</tr>
<tr>
<td>102</td>
<td>Jon Public</td>
<td>&quot;1043 W. Easy St, Phoenix, AZ 85535&quot;</td>
<td>5556060</td>
<td>10-24-1950</td>
<td>482891822</td>
<td>18.0</td>
</tr>
<tr>
<td>103</td>
<td>J Public</td>
<td>&quot;1043 W. Easy St, Phoenix, AZ 85535&quot;</td>
<td>5553232</td>
<td>10-25-1950</td>
<td>482891822</td>
<td>11.0</td>
</tr>
<tr>
<td>104</td>
<td>John Q Long</td>
<td>&quot;552 Green Dr, Phoenix, AZ 85535&quot;</td>
<td>5552745</td>
<td>10-24-1950</td>
<td>48224857</td>
<td>4.0</td>
</tr>
<tr>
<td>105</td>
<td>Danny Smith</td>
<td>5553274</td>
<td>5554289</td>
<td>10-24-1950</td>
<td>482891822</td>
<td>5.0</td>
</tr>
</tbody>
</table>

*Note:* The example score on a scale of 1 to 20 is an arbitrary placeholder for different levels of matching for purposes of discussion, but does not represent an absolute scale of probability.
Questions
1. Does this false positive match scenario qualify as an “incidental disclosure” pursuant to HIPAA?
2. What should our recommendations be regarding prevention of such disclosures?
3. What should our recommendations be regarding what actions to take when such disclosures occur?
4. Is this a Common Framework issue?

HIPAA
Pursuant to HIPAA privacy regulations, a covered entity is permitted to use or disclose protected health information for treatment, payment, or health care operations. An entity is also permitted to use or disclose protected health information incident to an otherwise permitted use or disclosure, provided that it has complied with applicable requirements of the minimum necessary standard and required security safeguards.

In proposing the addition of the incidental disclosure provision to the Privacy Rule in its 2002 guidance, the United States Department of Health & Human Services (HHS) described an incidental use or disclosure as a secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and that occurs as a by-product of an otherwise permitted use or disclosure. As described in the preamble to the Privacy Rule, an incidental use or disclosure is permissible only to the extent that the covered entity has applied reasonable safeguards and implemented the minimum necessary standard. In addition, covered entities are not required to document permitted incidental disclosures in an accounting of disclosures.

HIPAA’s minimum necessary standard requires covered entities to limit how much protected health information is used, disclosed, and requested for certain purposes. These minimum necessary policies and procedures also reasonably must limit who within the entity has access to protected health information, and under what conditions, based on job responsibilities and the nature of the business.

Recommendation
The Connecting for Health Policy Subcommittee assumes that the RLS false positive match is an incidental disclosure pursuant to HIPAA, with the understanding that such a disclosure is permissible under the law only to the extent that the covered entity or entities involved have applied reasonable safeguards and implemented the minimum necessary standard. The parameters recommended in this document for such matches are believed to require such safeguards.

NB: It has been noted that, as a legal matter, it is unclear whether “false positive match” disclosures are “incidental” according to HIPAA. There may be a legal argument that they can be considered permissible treatment disclosures. In either case, the disclosure would

The minimum necessary standard does not apply to disclosures, including oral disclosures, among health care providers for treatment purposes. HIPAA security standards require that a covered entity must have in place appropriate administrative, technical, and physical safeguards that protect against uses and disclosures not permitted by the Privacy Rule and that limit incidental uses and disclosures. It is not expected that a covered entity’s safeguards guarantee the privacy of protected health information from any and all potential risks.

An incidental use or disclosure that occurs as a result of a failure to apply reasonable safeguards or the minimum necessary standard, where required, is a violation of the Privacy Rule. Failure to comply with HIPAA regulations can result in general fines of up to $25,000 per incident.

1. Does the false positive match scenario qualify as an “incidental disclosure” pursuant to HIPAA?

5 45 CFR 164.502(b), 164.514(d).
6 45 CFR 164.530(c).
7 HIPAA is a federal law. Individual states may place additional requirements/restrictions on the communication/transmission of protected health information.
be permissible under HIPAA, so the result would be the same. At the time of this writing, there has been no authoritative guidance on the issue from HHS, although it is possible that an FAQ on the topic could be sought in the future.

2. What should our recommendations be regarding prevention of such disclosures?

Recommendations
The Connecting for Health Policy Subcommittee assumes that the covered entities who could be involved in a request for information from the RLS, including the requester of information, the RLS (which could be defined as a “business associate” pursuant to HIPAA\(^8\)), and the entity holding information pointed to by the index are in compliance with HIPAA’s minimum necessary standard and required security safeguards. Indeed, if the entities are not in compliance with HIPAA’s requirements and disclosures of protected health information occur, they are in violation of federal law and subject to the penalties described above.\(^9\)

Beyond the strictures of HIPAA, the false positive match scenario may still produce incidental disclosures, albeit “permissible ones” according to the law. For example, in the sample data presented above, it is possible that J Public is not the person for whom information was requested. If J Public had, perhaps, visited a psychiatric hospital and that information was both recorded in the index, even without any additional clinical information, and returned to the requester, J Public might feel that his privacy had been violated, despite the entities’ compliance with the letter of the law.

Therefore, the Connecting for Health Policy Subcommittee recommends the setting of a minimum level of certainty before the RLS returns information to the requester; and that whenever that level of certainty is not reached, the RLS could request additional demographic fields until either the level of certainty is reached or no record can be returned. This recommendation is based on ethical and public policy reasons, as opposed to the merely legal requirements of the HIPAA “reasonable safeguards” standard. It is also based on the need to reduce errors in record linkage.

For example, if a requester submits information in five demographic fields for a patient to the RLS, but the RLS does not find a match with a certain level of certainty on any one record, the RLS will report back that there is no match.

In the case that the RLS can return no matches with the specified certainty level, the RLS could require additional demographic data in order to determine a match. For example, at this point, the requester could be asked to supply data for additional demographic fields.

These levels could be set in order to minimize the extent possible incidental disclosures of protected health information in an effort to respect the privacy of patients for ethical and public policy reasons.

Issues considered in formulating these recommendations include:

1. Should the Policy Subcommittee specify a level of accuracy for matching? Yes.
2. Should the level of accuracy be different for different use cases? No. The Policy Subcommittee made it clear that the RLS will not accept “wild-card” queries and can only respond to attempts to locate records on an individually identifiable patient. Other than that, the RLS has no mechanism to distinguish one use case from another, so the level of accuracy should not change.
3. Assuming the Policy Subcommittee specifies a level of accuracy for matching, how should it be determined? At least for external requests for matches, the level of certainty should be high enough that the probability of data being returned on the wrong patient would be very unlikely. One in 100,000 and one in a million were mentioned as potential levels, but the level could be different for different databases. The Policy Subcommittee recommends that the figure of one in 100,000 be set as the initial maximum probability of a false positive error when querying an RLS. It is expected that this set point may be adjusted as experience with operational RLSs gives us more real

\(^8\) 45 CFR 160.103.
\(^9\) All covered entities except small health plans were required to have compliant security standards in place before 4/21/05, while small health plans have until 4/21/06 to comply with the HIPAA Security Rule.
Correctly Matching Patients with Their Records

data with which to judge whether it continues to be appropriate. The Policy Subcommittee also recommends that a large test data set and standard set of queries be developed so that vendors of matching algorithms can test against this standard.\textsuperscript{10}

4. Under what circumstances, if any, would it be acceptable to lower a matching threshold—the “Break the Glass” scenario? For normal external requests, a Break the Glass scenario assumes that the requester can make better judgments about unreliable data than the probabilistic matching algorithm. The Policy Subcommittee concluded that this was a useful “escape” mechanism in the past but that the increasing sophistication of matching algorithms might make such a mechanism anachronistic in the future. Special circumstances such as internal research or audits were considered to be situations when the high probability level for the matching algorithm might be reduced. Breaking the Glass is fraught with technical, practical, and operational problems and may have greater potential for harm than benefit. The Policy Subcommittee concludes that such a mechanism has no place in the RLS. When such special circumstances arise, a requester should go directly to the source of the clinical data and work through local mechanisms for dealing with them.

3. What should our recommendations be regarding what actions to take when incidental disclosures occur?

Recommendations

The Connecting for Health Policy Subcommittee assumes that the covered entities who could be involved in a request for information from the RLS are in compliance with HIPAA’s minimum necessary standard and required security safeguards. The incidental disclosures in this scenario would be permissible according to the law.

However, as discussed above, the false positive match scenario may still produce incidental disclosures, even if the RLS requires a high level of certainty in order to return information from the index. Given the above recommendations of this Subcommittee, if a match meets the criteria for a positive match, they are permissible disclosures and cannot possibly be prevented without making the threshold for a positive match so high that it would create an unacceptable level of false negative matches.

The Connecting for Health Policy Subcommittee adopts the following position: In the case in which a requester of information recognizes that information received from the RLS does not apply to the patient about whom information was requested, the requester should take reasonable steps to immediately destroy that information, including, where applicable, deleting the electronic version of that portion of the RLS response and/or any paper copies thereof.

4. Is this a Common Framework issue?

Recommendations

Yes. If the false positive match scenario is not approached as a Common Framework issue, it is possible that various SNOs could set different standards for certainty and different numbers of required fields of demographic data in order for the RLS involved to return information to the requester.

This variability in what information will be returned from an RLS raises reliability of information questions: How will I, as a provider, be able to rely upon the information returned from the RLS in Idaho as well as the information from the RLS in Maine? Moreover, it is also unclear how sub-network RLS systems could grow and become increasingly interoperable when different threshold standards for information return are set across the systems.

For these reasons, the Connecting for Health Policy Subcommittee adopts the position that the false positive match/incidental disclosure scenario and the recommendations arrived at by this Policy Subcommittee should be

considered part of the Common Framework, to allow for increased reliability and scalability of a nationwide electronic health information exchange.
Acknowledgements
The members of the Connecting for Health Policy Subcommittee have accomplished an extraordinary task in less than a year’s time—the development of an evolving piece of work that can serve as the core of nationwide health information exchange—the policy components of The Common Framework. During this time, we have been fortunate to work with respected experts in the fields of health, information technology, and privacy law, all of whom have contributed their time, energy, and expertise to a daunting enterprise. Our consultants and volunteers have worked long hours in meetings and conference calls to negotiate the intricacies of such issues as privacy, security, authentication, notification, and consent in health information exchange. We offer them our heartfelt thanks for taking on this journey with us, and look forward to the remaining work ahead.

In addition, we would like to offer special thanks to the volunteers and consultants who authored the initial drafts of this body of work—their hard work created a strong foundation upon which to focus the Subcommittee’s deliberations: Stefaan Verhulst, Clay Shirky, Peter Swire, Gerry Hinkley, Allen Briskin, Marcy Wilder, William Braithwaite, and Janlori Goldman.

Finally, we must note that none of this work would have been possible without the leadership and inspiration of our co-chairs, William Braithwaite and Mark Frisse. They have led us with steady hands and determination of spirit.

Connecting for Health Policy Subcommittee

William Braithwaite, MD, eHealth Initiative, (Co-Chair)

Mark Frisse, MD, MBA, MSc, Vanderbilt Center for Better Health, (Co-Chair)

Laura Adams, Rhode Island Quality Institute

Phyllis Borzi, JD, George Washington University Medical Center

Susan Christensen*, JD, Agency for Healthcare Research and Quality, United States Department of Health and Human Services

Art Davidson, MD, MSHP, Denver Public Health

Mary Jo Deering*, PhD, National Cancer Institute/National Institutes of Health, United States Department of Health and Human Services

Jim Dempsey, JD, Center for Democracy and Technology

Hank Fanberg, Christus Health

Linda Fischetti*, RN, MS, Veterans Health Administration

Seth Foldy, MD, City of Milwaukee Health Department

Janlori Goldman, JD, Columbia College of Physicians and Surgeons

Ken Goodman, PhD, University of Miami

John Halamka, MD, CareGroup Healthcare System

Joseph Heyman, MD, American Medical Association

Gerry Hinkley, JD, Davis, Wright, Tremaine LLP

Charles Jaffe, MD, PhD, Intel Corporation

Jim Keese, Eastman Kodak Company

Linda Kloss, RHIA, CAE, American Health Information Management Association

Gil Kuperman, MD, PhD, New York-Presbyterian Hospital

Ned McCulloch, JD, IBM Corporation

Patrick McMahon, Microsoft Corporation

Omid Moghadam, Intel Corporation
Joyce Niland, PhD, City of Hope National Medical Center

Louise Novotny, Communication Workers of America

Michele O’Connor, MPA, RHIA, MPI Services Initiate

Victoria Prescott, JD, Regenstrief Institute for Healthcare

Marc A. Rodwin, JD, PhD, Suffolk University Law School

Kristen B. Rosati, JD, Coppersmith Gordon Schermer Owens & Nelson PLC

Sara Rosenbaum, JD, George Washington University Medical Center

David A. Ross, ScD, Public Health Informatics Institute

Clay Shirky, New York University (Chair, Technical Subcommittee)

Don Simborg, MD, American Medical Informatics Association

Michael Skinner, Santa Barbara Care Data Exchange

Joel Slackman, BlueCross/BlueShield Association

Peter P. Swire, JD, Moritz College of Law, Ohio State University

Paul Tang, MD, Palo Alto Medical Foundation

Micky Tripathi, Massachusetts eHealth Collaborative

Cynthia Wark*, CAPT, United States Public Health Service Commissioned Corps, Centers for Medicare and Medicaid Services, United States Department of Health and Human Services

John C. Wiesendanger, MHS, West Virginia Medical Institute/Quality Insights of Delaware/Quality Insights of Pennsylvania

Marcy Wilder, JD, Hogan & Hartson LLP

Scott Williams, MD, MPH, HealthInsight

Robert B. Williams, MD, MIS, Deloitte

Joy Wilson, National Conference of State Legislatures

Rochelle Woolley, RxHub

Amy Zimmerman-Levitan, MPH, Rhode Island State Department of Health

*Note: Federal employees participate in the Subcommittee but make no endorsement
Authentication of System Users
Authentication of System Users
The document you are reading is part of *The Connecting for Health Common Framework*, which is available in full and in its most current version at: [http://www.connectingforhealth.org/](http://www.connectingforhealth.org/). The Common Framework will be revised and expanded over time. As of October 2006, the Common Framework included the following published components:

![Diagram](image-url)
Authentication of System Users*

This document describes the policy considerations for handling identity, authentication, and authorization issues in the Connecting for Health Common Framework. Every sub-network organization (SNO) will need to define particular policies related to these issues which must take into account both the basic requirements laid out here, and the local conditions among the SNO’s members.

Identity, authentication, and authorization can be thought of as the answers to a quartet of questions:

- Who am I? (Identity)
- How is that identity represented? (Identifiers)
- How can I prove who I am? (Authentication)
- What can I do when I’ve proved who I am? (Authorization)

Though the differences among these questions are relatively simple, they are often confused in the literature. It is critical that any SNO implementing the Connecting for Health Common Framework make plans to address all four questions, and to handle them separately, with regard to their unique characteristics, described below under “Definitions.”

This document describes the requirements of governance, not implementation. It does not cover HIPAA requirements of either the participating members, or of the SNO itself. The variability of systems in place for securing data, and the differences in regulatory regimes for the kind of data to be secured (for example, use or non-use of Social Security Numbers (SSNs)) makes modeling the threats and possible security responses a local requirement. Other than the policy minimums specified here, security issues are subject to local control. Each SNO will need to decide how much or little to require uniformly of its members, always assuming HIPAA compliance. Procedures such as password recovery, log-in protections, or two-factor authentication can be set by each entity, or standardized across the SNO.

Because of the sensitivity of patient data, unauthorized users of any electronic system for discovering, transmitting, or viewing patient data must be prevented from unauthorized access, and the users of such a system who do have authorization must be accountable for how that information is used or misused. The issuance of identifiers that point uniquely and unambiguously to persons allowed to access patient data, and the handling of both authentication and authorization for those users, are challenging problems. For the purposes of this document, identity, identifiers, authorization, and authentication are defined in federal HIPAA Privacy and Security Rules provide the baseline for the Connecting for Health Common Framework, although in some cases greater privacy protections and individual rights are recommended by the Connecting for Health Policy Subcommittee. Importantly, the Connecting for Health Common Framework permits SNO participants to establish and follow their own more protective data management, privacy, and security policies and procedures. In addition, some customization may be necessary at the SNO and participant level to ensure consistency and compliance with applicable state and local laws.

Similarly, this document does not cover technical issues of security of either the participating members, or of the SNO itself. The variability of systems in place for securing data, and the differences in regulatory regimes for the kind of data to be secured (for example, use or non-use of Social Security Numbers (SSNs)) makes modeling the threats and possible security responses a local requirement. Other than the policy minimums specified here, security issues are subject to local control. Each SNO will need to decide how much or little to require uniformly of its members, always assuming HIPAA compliance. Procedures such as password recovery, log-in protections, or two-factor authentication can be set by each entity, or standardized across the SNO.

Because of the sensitivity of patient data, unauthorized users of any electronic system for discovering, transmitting, or viewing patient data must be prevented from unauthorized access, and the users of such a system who do have authorization must be accountable for how that information is used or misused. The issuance of identifiers that point uniquely and unambiguously to persons allowed to access patient data, and the handling of both authentication and authorization for those users, are challenging problems. For the purposes of this document, identity, identifiers, authorization, and authentication are defined in

* Connecting for Health thanks Clay Shirky, Adjunct Professor, New York University Graduate Interactive Telecommunications Program, for drafting this paper.

1 A sub-network organization (SNO) shall operate as a health information data exchange organization (whether regionally or affinity-based) that operates as a part of the National Health Information Network (NHIN), a nationwide environment for the electronic exchange of health information made up of a “network of networks.”

2 ISO 15408, Common Criteria for IT Security Evaluations, represents industry best practices for such modeling.
the next section.

There is no obvious parallel in the world today for an electronic health care information system in the US. Highly secure systems such as those used by defense agencies have control of both the users and the technology; systems with multiple participants and a high degree of end-user access such as the credit card clear system are tolerant of a degree of fraud that would be unacceptable in a medical context; and all such systems exclude large numbers of individuals.

The current health care system is large, heterogeneous, and fragmented. There is no one entity or small coordinated group responsible for it, yet it covers all consumers of health care services. Furthermore, it is governed by HIPAA, which sets strong national minimums for privacy and security protections of health care information, but allows local deviations to stronger protections, and in all cases has very high requirements for deterring misuse. As a result, any local solution is likely to be both contextual and temporary. The solutions adopted by any given SNO will be largely guided by the degree of technical investment already made in the region and by any local requirements that are more stringent than HIPAA, and are more likely to be adopted in response to available technologies that may change in the near future.

Given these characteristics, the policies around identity, authentication, and authorization are going to be aimed in the direction of assuring compliance with the spirit of the Connecting for Health Common Framework, and avoiding a small number of known errors. A more comprehensive and definitional framework will have to wait for more robust technology and more extensive real-world experience.

**Definitions**

**Identity**

Identity is, in this context, an individual person or institution that needs access to health care data, for any purpose. Crucially, an identity is not merely a role; if you want to know the identity of someone who authorized a particular prescription, you want to know that it was Dr. Smith, not just that it was a doctor.

**Identifier**

An identifier is an attribute that points unambiguously and uniquely to an identity. In practice, the person identifier will often be an employee ID number, or, possibly, a log-in name guaranteed unique within the scope of the institution. It is critical that such identifiers not be re-issued to other, later users. If "jsmith" is used as an identifier, all future John or Jane Smiths must be issued a different identifier. (Note that this policy will require a tightening of existing policy for those institutions that currently allow for re-use of identifiers.)

An identifier is an abstract attribute and generated attribute of a particular person or entity, in the case of institutional identifiers. Tokens that refer to roles such as "Primary Care Physician," or those referring to institutional relations such as "Admitting Privileges at General Hospital" are not considered identifiers in this context.

The problem is often expressed in terms of issuing identities, which means, in practice, issuing unique identifiers that correspond uniquely and unambiguously to an existing identity, in the manner of providing an employee ID or unique login.

**Authentication**

Authentication requires an identifier, and is required for authorization. Authentication is a way of allowing a user to prove that he is who he claims to be. The simplest form of authentication is in the providing of an identifying token, plus a secret of some sort, such as a bank card + PIN, or a username + password or phrase.

An example of how not to handle authentication is the SSN. One of the reasons the SSN has turned out to be a bad identifier is that one number is meant to provide the function of both the public and secret parts of authentication: you have an SSN that points uniquely to you, but you must reveal it as proof that you have it. Without being accompanied by a second, secret token such as a PIN, the SSN is damaged in regard to authentication by the very use that makes it otherwise worthwhile.

**Authorization**

After a user claiming a given identity has been authenticated, an authorization mechanism
needs to determine what data the user is allowed to access and what functions may be performed by the user on that data, e.g., to view, copy, or update data. Authorization is typically role-based; that is, the different operations available are tied to the role of the user, such as physician, administrative support, etc. One individual can have many roles within the system (for example, Primary Care Physician, Admitting Physician, Specialist, etc.).

In the event of a health care emergency, some method may be provided to allow access in the event of an authentication failure as a kind of "Break the Glass" function on an existing account. However, role-based authorization is not sufficient for use of the system; no access to the system should be allowed for any such role without a human identifier attached. It is not enough to ask that someone prove that they have admitting privileges at General Hospital; they must also provide their actual identity, so that should a later audit be required, a person can be associated with the audited actions, not just a role.

A Note on Auditing

Though the handling of identity, identifiers, authentication, and authorization is often lumped together with issues of auditing, these issues are best approached separately. Auditing is required simply to have the ability to determine who accessed the system after the fact. Auditing as a technology is largely orthogonal to the technologies required for identity, identifiers, authentication, and authorization, and auditing is also used for unrelated requirements, such as statistical sampling of use patterns, and needs and trends analysis. The Connecting for Health Policy Subcommittee is publishing a separate piece on auditing requirements.3

Requirements

Every transaction involving patient data between institutions in a SNO will operate by transitive trust, often based in the legal requirements of a contract. The institutional members of a SNO trust one another, and therefore they trust requests from the authenticated and authorized employees of those institutions. The backbone of the transitive trust model is the ability to identify anyone violating that trust, and to link them unambiguously to the entity that gave them access.

Transitive trust is a practical rather than ideal system. Though there has been work on more elaborate federated identity systems, none are yet at a level of practicality necessary for this work, nor are they simple enough to be implemented broadly. The advantages of transitive trust are thus largely practical: it allows systems to scale upwards in the number of employees covered without forcing each institution to know about every other employee in every remote institution. The design and implementation of even a simple system of transitive trust is complex, and will be highly dependent on existing technological tools and frameworks, but all such systems should have the following basic policy restrictions:

• A SNO must have identifiers for all its participating institutions. These identifiers can be issued by the SNO, or they can be adopted from an external source (e.g. HIPAA-mandated identifiers4), as long as that source guarantees the uniqueness and persistence of any given identifier.

• All users must be authenticated before they are given access to any SNO-wide resource containing patient data. This may take a number of different forms: the local institutions can ask users to log in, and communicate the authenticated identifiers to other participants in the SNO, or the SNO can run authentication services itself, getting lists of users and roles from the participating institutions. This latter strategy may suffer from scaling problems, but may be useful for getting a SNO off the ground.

• Any request for data from a remote institution, an institution other than the one the user is logged in to, must be accompanied by at least two pieces of identifying information: which

---

3 See Connecting for Health, “Auditing Access to and Use of a Health Information Exchange.”

4 45 CFR § 162.404(a). HIPAA requires that covered health care providers comply with the specifications in § 162.410 regarding implementation of the standard unique health identifiers no later than May 23, 2007.
institution authenticated the requesting user and an identifier for that user. There are a number of ways such a system could be implemented technically, but the basic policy prescription is that, for any given request from a remote institution, the local institution should know where the request came from, and who authorized it.

- A method may be provided to allow access to patient data in the event of an authorization failure—a so-called “Break the Glass” function. Access failure for someone who should be authorized can happen for a number of reasons: he or she does not remember or have the required information or tokens for authentication; or he or she does not have permission from the system to look at or interact with the data they are requesting. Any request that allows a known user to request data they believe they need, e.g., a physician attempting to access the medication history of a patient, when the system would not otherwise give that person access, should be accompanied by a brief description of the rationale for the request.

- No matter what the cause of the authorization failure in the Break the Glass scenario, any system access must be accompanied by an identifier for that user. In no case is an otherwise unidentified “Emergency” account to be used, on the grounds that it amounts to the provisioning of a role without an accompanying person identifier.

- Any request that allows a known user to request data they believe they need, when the system would not otherwise give them access, must be accompanied by enhanced auditing and timely human review.

- The Record Locator Service itself may not offer a Break the Glass function; all such requests must go to the institutions hosting the clinical data.

- In the case of a SNO providing a method for a patient or patient representative to access his or her own records, some “bootstrapping” will be required. The initial issuing of the patient access capability must be done by a participating institution, or by a third-party recognized by the SNO. The patient can then be given a SNO-specific identifier, accompanied by an authentication method, with authorization limited to looking at his or her own material. Depending on implementation within the SNO, the patient could then access his or her records directly after having been issued such credentials, subject to local terms and conditions, and to periodic review. SNO-wide patient access requests, however handled otherwise, must carry the name of the institution that initially created the patient’s identifier.

Authentication methods can be as simple or complex as the SNO requires; however, the SNO should publish minimum standards for authentication adhered to by all participating institutions, or be ready to add an additional layer of SNO-hosted authentication. The issue here, to be handled SNO by SNO, is that the less secure an authentication system is, the likelier it is to suffer from misuse, but the more secure it is, the likelier it is to suffer from non-use.

Authorization presents similar issues to authentication. The more granular such a role-based authorization system is, the better a fit can be imagined between a set of roles and any given situation, e.g., a patient’s primary care physician accessing data from a hospital where they refer patients, but where they do not have admitting privileges. However, with each added element come both management complexity and the possibility of subtle and unpredictable errors. Authorization can also be as simple as the SNO desires, with two caveats: there must be restrictions on who, if anyone, can add to or alter a record (as opposed to simply viewing it), and there must be restrictions on who can trigger any available Break the Glass functions.

When implementing identity, authentication, and authorization policies, SNOs will need to balance defensiveness, flexibility, and practicality. Defensiveness is the quality that leads a SNO to actively model and protect against threats of accidental or malicious access to or misuse of data. Flexibility is necessary because medicine is not banking—when there is a judgment call, it should be in favor of getting patient data to a clinician who needs it to provide care, even when such provisioning
requires Break the Glass functionality. Such uses of the system must be accompanied by enhanced auditing and timely human review. Finally, practicality is that set of choices which balances heightened security with adoptability. It is possible to design a system so well defended against misuse that it is defended against legitimate uses as well. As this cannot be allowed to happen, each SNO will have considerable discretion in designing its identification, authentication, and authorization policies, as long as those policies conform to the minimum standards listed here, and are subjected to annual review to ensure that they are continually improved where such improvement is practical. Such annual review is probably best done in conjunction with the mandated HIPAA security audit.
Acknowledgements
The members of the Connecting for Health Policy Subcommittee have accomplished an extraordinary task in less than a year’s time—the development of an evolving piece of work that can serve as the core of nationwide health information exchange—the policy components of The Common Framework. During this time, we have been fortunate to work with respected experts in the fields of health, information technology, and privacy law, all of whom have contributed their time, energy, and expertise to a daunting enterprise. Our consultants and volunteers have worked long hours in meetings and conference calls to negotiate the intricacies of such issues as privacy, security, authentication, notification, and consent in health information exchange. We offer them our heartfelt thanks for taking on this journey with us, and look forward to the remaining work ahead.

In addition, we would like to offer special thanks to the volunteers and consultants who authored the initial drafts of this body of work—their hard work created a strong foundation upon which to focus the Subcommittee’s deliberations: Stefaan Verhulst, Clay Shirky, Peter Swire, Gerry Hinkley, Allen Briskin, Marcy Wilder, William Braithwaite, and Janlori Goldman. Finally, we must note that none of this work would have been possible without the leadership and inspiration of our co-chairs, William Braithwaite and Mark Frisse. They have led us with steady hands and determination of spirit.

Connecting for Health Policy Subcommittee

William Braithwaite, MD, eHealth Initiative, (Co-Chair)
Seth Foldy, MD, City of Milwaukee Health Department

Mark Frisse, MD, MBA, MSc, Vanderbilt Center for Better Health, (Co-Chair)
Janlori Goldman, JD, Columbia College of Physicians and Surgeons

Laura Adams, Rhode Island Quality Institute
Ken Goodman, PhD, University of Miami

Phyllis Borzi, JD, George Washington University Medical Center
John Halamka, MD, CareGroup Healthcare System

Susan Christensen*, JD, Agency for Healthcare Research and Quality, United States Department of Health and Human Services
Joseph Heyman, MD, American Medical Association

Art Davidson, MD, MSHP, Denver Public Health
Gerry Hinkley, JD, Davis, Wright, Tremaine LLP

Mary Jo Deering*, PhD, National Cancer Institute/National Institutes of Health, United States Department of Health and Human Services
Charles Jaffe, MD, PhD, Intel Corporation

Jim Dempsey, JD, Center for Democracy and Technology
Jim Keese, Eastman Kodak Company

Hank Fanberg, Christus Health
Linda Kloss, RHIA, CAE, American Health Information Management Association

Linda Fischetti*, RN, MS, Veterans Health Administration
Gil Kuperman, MD, PhD, New York-Presbyterian Hospital

Omid Moghadam, Intel Corporation
Ned McCulloch, JD, IBM Corporation

Patrick McMahon, Microsoft Corporation

Connecting for Health Common Framework | www.connectingforhealth.org | April 2006
Joyce Niland, PhD, City of Hope National Medical Center

Louise Novotny, Communication Workers of America

Michele O’Connor, MPA, RHIA, MPI Services Initiate

Victoria Prescott, JD, Regenstrief Institute for Healthcare

Marc A. Rodwin, JD, PhD, Suffolk University Law School

Kristen B. Rosati, JD, Coppersmith Gordon Schermer Owens & Nelson PLC

Sara Rosenbaum, JD, George Washington University Medical Center

David A. Ross, ScD, Public Health Informatics Institute

Clay Shirky, New York University (Chair, Technical Subcommittee)

Don Simborg, MD, American Medical Informatics Association

Michael Skinner, Santa Barbara Care Data Exchange

Joel Slackman, BlueCross/BlueShield Association

Peter P. Swire, JD, Moritz College of Law, Ohio State University

Paul Tang, MD, Palo Alto Medical Foundation

Micky Tripathi, Massachusetts eHealth Collaborative

Cynthia Wark*, CAPT, United States Public Health Service Commissioned Corps, Centers for Medicare and Medicaid Services, United States Department of Health and Human Services

John C. Wiesendanger, MHS, West Virginia Medical Institute/Quality Insights of Delaware/Quality Insights of Pennsylvania

Marcy Wilder, JD, Hogan & Hartson LLP

Scott Williams, MD, MPH, HealthInsight

Robert B. Williams, MD, MIS, Deloitte

Joy Wilson, National Conference of State Legislatures

Rochelle Woolley, RxHub

Amy Zimmerman-Levitan, MPH, Rhode Island State Department of Health

*Note: Federal employees participate in the Subcommittee but make no endorsement
Patients’ Access to Their Own Health Information
Patients’ Access to Their Own Health Information
The document you are reading is part of *The Connecting for Health Common Framework*, which is available in full and in its most current version at: http://www.connectingforhealth.org/. The Common Framework will be revised and expanded over time. As of October 2006, the Common Framework included the following published components:
Patients’ Access to Their Own Health Information*

Collecting, storing, and sharing personal health information about patients is a fundamental component of health care. In addition to serving as the information hub to health care providers in treating patients, medical records are frequently used by a host of other health care professionals, such as quality improvement organizations, researchers, and public health officials.

Patients have a vital interest in accessing sensitive information about their own health care. A central principle of privacy policy is to provide people with access to their own information, so that they may make informed choices about who should get their information, under what circumstances, and be made aware of errors that the records may contain. Access to their own medical records can also empower consumers to become more engaged participants in their own health care.

Most consumers want access to their medical records. A national survey documents that 68 percent of Americans believe that “giving people the right to see and make corrections to their own medical records” would be an effective way of promoting privacy and health care.¹ In fact, Americans’ interest in accessing their personal medical information has increased over the years. In 2005, 51 percent of Americans tried to access their medical records, up from 45 percent in 1999.² However, until recently, many people did not have the legal right to see, copy, and amend their health information held by their providers. As of April 2003, the HIPAA Privacy Rule mandates that people have such rights, whether their records are in paper or electronic format.³

Patients’ ability to effectively access their own personal health information could be significantly enhanced with the use of new technologies. Although there are significant concerns about privacy that must be addressed, accessing personal health information electronically could have a positive impact on how patients participate in their own care. Some providers and companies have taken the lead by offering patients electronic access to their medical information. The growing movement towards the development of electronic health record (EHR) systems should include patients as authorized users of their health information for both practical and legal purposes, enabling compliance with the privacy regulation and enhancing a person’s ability to make informed choices about his or her health and the use of his or her information.

While the Privacy Rule allows patient access to both paper and electronic records, the increasing use of technology in health care fosters the potential for streamlining the process of granting patients access to their records. The Privacy Rule provides a floor of protection, whereby individual states can—and have—enforced laws that both provide stronger protections for personal health information and allow patients easier access to their medical records.

* Connecting for Health thanks Janlori Goldman, Research Scholar, Center on Medicine as a Profession, Columbia College of Physicians and Surgeons; Health Privacy Project, and Emily Stewart, formerly of the Health Privacy Project, for drafting this paper.


³ The Privacy Rule went into effect on 4/14/01, and most providers and health plans were required to be in compliance with the law by 4/14/03.
The HIPAA Privacy Rule—Accessing Protected Health Information

In promulgating the HIPAA regulations, the United States Department of Health and Human Services (HHS) recognized that allowing consumers access to their health information is a necessary component of a well-functioning health care system. Based on the principle of informed consent, the Privacy Rule acknowledges that in order to have meaningful control over personal health care decisions—including limitations on who can access information—individuals need to have access to their own health information. The Privacy Rule gives consumers rights with regard to certain health care organizations, or “covered entities,” defined as health plans, health care clearinghouses, and health care providers who transmit health information in electronic form in connection with specified financial and administrative transactions.4

In general, protected health information under the Privacy Rule correlates with what most consumers would consider their medical record. Whether or not their health information is paper-based or stored electronically, the Privacy Rule affords patients the right to access their medical record within 30 days of a request. The Privacy Rule explicitly gives patients the right to inspect and obtain a copy of protected health information held in a “designated record set” by the covered entity.5 Protected health information (PHI) is defined as “individually identifiable health information,” with the exception of some education and other records.6 Consumers only have a right to access PHI if, and for as long as, it is maintained in a designated record set, which the Privacy Rule defines as a “group of records maintained by or for a covered entity that is:

(i) the medical records and billing records about individuals maintained by, or for a covered health care provider;

(ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by, or for a health plan; or

(iii) used, in whole or in part, by or for the covered entity to make decisions about individuals.”7

Although the Privacy Rule grants consumers the right of access in most situations, there are several specific situations in which covered entities are neither required to give consumers access to their own protected health information held in a designated record set nor required to allow the individual a review of the denial. For instance, individuals do not have the right to access psychotherapy notes or information compiled in reasonable anticipation of, or for use in a civil, criminal, or administrative action or proceeding.8

On the other hand, there are some circumstances when covered entities have the right to deny access, but individuals also have the right to request a review of that denial. For example, if in the exercise of professional judgment, a licensed health care professional believes that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person, the covered entity can then deny access.9 Also, if the PHI makes reference to another person, unless the other person is a health care provider, and a licensed health care professional believes that the access requested is reasonably likely to cause substantial harm to such other person, a covered entity can deny access to the health information.10 Again, in these types of situations,

---

4 45 C.F.R. § 160.103.
5 45 C.F.R. § 164.524(a)(1).
6 45 C.F.R. § 164.501. The Privacy Rule defines individually identifiable health information as “a subset of health information, including demographic information collected from an individual” that (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) that identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual. See 45 C.F.R. § 160.103.
7 45 C.F.R. § 164.501.
8 45 C.F.R. § 164.524(a)(1-2). See citation for more circumstances whereby a covered entity can deny access and refuse to allow the individual an opportunity for review of the denial.
9 Note that only “life or physical safety” is specified; possible harm to mental or emotional health is not a reason to deny access.
10 45 C.F.R. § 164.524(a)(3). See citation for more circumstances whereby a covered entity can deny access but individuals also have a right to request a review of the denial.
an individual has a right to request a review of the denial.\textsuperscript{11}

The Privacy Rule outlines a basic process for individuals seeking access to their medical information and establishes guidelines to ensure covered entities provide access in a timely manner. As a basic principle, the Privacy Rule establishes that covered entities must allow individuals to request access to their own records; the law allows covered entities to require that requests be written provided that patients are informed of this requirement.\textsuperscript{12} Otherwise, patients may request access orally.

Within 30 days of the receipt of the request, the covered entity must act on the request by providing the patient access, providing a written denial of access, or informing the individual of the reason for which the covered entity needs additional time (but no more than 30 days) to complete the request.\textsuperscript{13} The one exception is for information not maintained or accessible to the covered entity on-site; in this instance, the covered entity may take up to 60 days to take one of the above actions.\textsuperscript{14}

If the covered entity grants access, it must provide the individual with the information in the format requested if possible and otherwise in a readable hard copy or another format agreed upon by both the covered entity and the individual.\textsuperscript{15} However, the covered entity may provide a summary of the health information if the individual agrees in advance to the summary and to any additional fees it would produce. The covered entity must arrange with the individual for “a convenient time and place to inspect or obtain a copy of the protected health information, or mail the copy of the protected health information at the individual’s request” and may charge a “reasonable, cost-based fee” if the individual requests a copy of the record, but the fee can only include costs for copying, postage, and the development of a summary if the individual agreed to one.\textsuperscript{16}

If the covered entity denies access to a patient, it must deny access only to the specific information for which it has grounds to deny access. In addition, and within 30 days, the covered entity must provide the individual with a denial written in plain language. The statement must contain the basis for the denial, information about the individual’s review rights if applicable and how to exercise those rights, as well as a description detailing pertinent names, titles, and contact information of how the individual may file a complaint. Furthermore, if the covered entity does not maintain the protected health information about the individual requested, but has knowledge about where it is stored, the law requires the covered entity to inform the individual about where to submit a request for access.\textsuperscript{17}

If the individual requests a review of the covered entity’s denial, the covered entity must ensure that the review is conducted by a licensed health care professional who was not directly involved in the denial. The covered entity must forward the request in a timely manner to the reviewer, and the designated reviewing professional must determine “within a reasonable period of time” whether or not to deny access. Once a decision is made, the covered entity must immediately provide notice

\textsuperscript{11} 45 C.F.R. § 164.524(a)(3).
\textsuperscript{12} 45 C.F.R. § 164.524(b)(1). Often, covered entities may contract with “business associates” to perform some of the covered entity’s functions. In the business associate contract, the business associates must agree to make protected health information available for access, amendment, and accounting of disclosures. See 164.504(e)(2)(ii)(E-G).
\textsuperscript{13} If a covered entity needs more time to take action related to the individual’s request for access, it must, within 30 days, notify the individual with a written statement establishing the reasons for the delay and the date by which the covered entity will complete its action. The covered entity may only have one extension of time. See 45 C.F.R. § 164.524(b)(2)(ii).
\textsuperscript{14} 45 C.F.R. § 164.524(b).
\textsuperscript{15} 45 C.F.R. § 164.524(c)(2)(i).
\textsuperscript{16} 45 C.F.R. § 164.524(c). According to the Preamble to the Privacy Rule, 65 F.R. 82557, “If the individual requests a copy of protected health information, a covered entity may charge a reasonable, cost-based fee for the copying, including the labor and supply costs of copying. If hard copies are made, this would include the cost of paper. If electronic copies are made to a computer disk, this would include the cost of the computer disk. Covered entities may not charge any fees for retrieving or handling the information or for processing the request. If the individual requests the information to be mailed, the fee may include the cost of postage. Fees for copying and postage provided under state law, but not for other costs excluded under this rule, are presumed reasonable. If such per page costs include the cost of retrieving or handling the information, such costs are not acceptable under this rule.” Available at: http://aspe.hhs.gov/admnsimp/final/PvcPre02.htm.
\textsuperscript{17} 45 C.F.R. § 164.524(d).
to the individual and take any necessary action.\textsuperscript{18}

**The HI PAA Privacy Rule—Amending Protected Health Information**

The Privacy Rule recognizes the importance of allowing patients the right to amend inaccurate or incomplete medical records. Under the law, after an individual has reviewed his or her medical records, he or she may request that the covered entity amend the protected health information in the designated record set.\textsuperscript{19} However, in order to protect both the integrity of the record and the patient, the individual does not have the right to request that the covered entity delete any information from the record.\textsuperscript{20} Instead, information is added to the record, identifying and amending the pertinent information.

The Privacy Rule allows covered entities to require that individuals make amendment requests in writing and also provide a reason for the request, as long as individuals are notified in advance of any requirements. Within 60 days of receiving the request, the covered entity must either make the requested amendment or deny it.\textsuperscript{21} However, just as with the other access provisions, the law does allow the covered entity one extension (of no more than 30 days), provided that it sends the individual a written statement explaining the delay and listing the expected completion date.\textsuperscript{22}

If the covered entity decides to accept the amendment request, the Privacy Rule requires that at a minimum, it must identify the records that are affected by the amendment and either attach the amendment or provide a link to the location of the amendment. The law also requires the covered entity to notify the individual that the record has been amended in a timely manner and to secure the individual’s agreement allowing the covered entity to inform other relevant persons. Also in a timely manner, the covered entity must make reasonable efforts to notify and provide the amendment to anyone that the individual designates as having received PHI needing amendment. The covered entity must also notify others, including business associates, which have the information and may have relied or could rely on the un-amended information to the detriment of the individual.\textsuperscript{23}

If a covered entity decides to deny the amendment request, it must still abide by several related requirements, such as using plain language and within 60 days, the covered entity must provide the individual with a written denial that details both the basis for the denial and the individual’s right, as well as how to exercise this right, to submit a written statement disagreeing with the denial. If the individual submits a statement of disagreement, the statement, the original request, the covered entity’s denial, and any rebuttal must be appended to the designated record set and included in any future disclosures.\textsuperscript{24} Even if the individual does not submit a statement of disagreement, he or she may request—and the covered entity must comply—that the covered entity include the request for amendment and the denial with any future disclosures of pertinent sections of the designated record set.\textsuperscript{25} In addition, the covered entity is required to append or link to the appropriate section of the designated record set, as a recordkeeping function, the individual’s amendment request, the denial of request, the statement of disagreement, and any rebuttal statement.\textsuperscript{26}

\textsuperscript{18} 45 C.F.R. § 164.524(d)(4).
\textsuperscript{19} 45 C.F.R. § 164.526(a)(1).
\textsuperscript{20} It is important to note that any amendment made to an individual medical record is technically a supplement to that record. In other words, no information is discarded in the amendment process. Instead, information is added, identifying and amending the medical record. This process was designed primarily to ensure the integrity of the record and to protect the patient. See 45 C.F.R. § 164.526(c)(1).
\textsuperscript{21} 45 C.F.R. § 164.526(a-b).
\textsuperscript{22} 45 C.F.R. § 164.526(b)(2)(ii).
\textsuperscript{23} 45 C.F.R. § 164.526(c).
\textsuperscript{24} 45 C.F.R. § 164.526(d). The Privacy Rule also allows covered entities to include in future disclosures—"in lieu of including the actual request, denials, disagreement statements, and rebuttals—"an accurate summary of any such information." See 45 C.F.R. § 164.526(d)(4)-(5).
\textsuperscript{25} 45 C.F.R. § 164.526(d). The Privacy Rule requires covered entities to inform individuals that if a disagreement statement is not submitted, the individual may request that the covered entity attach the request and denial to any future disclosures. See 45 C.F.R. § 164.526(d)(1)(iii). The Privacy Rule also allows covered entities to include in future disclosures—"in lieu of including the actual request, denials, disagreement statements, and rebuttals—"an accurate summary of any such information." See 45 C.F.R. § 164.526(d)(4)-(5).
\textsuperscript{26} 45 C.F.R. § 164.526(d)(4).
The HIPAA Privacy Rule—Accounting for Disclosures

Knowing who has had access to one’s personal health information is related to having access oneself. Accordingly, the Privacy Rule acknowledges the importance of allowing patients the ability to see who accessed their personal health information. With exceptions, the Privacy Rule gives patients the right to see to whom covered entities have disclosed their personal health information for the six years prior to the date of the request.27

Upon request, covered entities must provide consumers with an accounting of disclosures during the previous six years, including the date of the disclosure, the name of the person who received the information, a brief description of the protected health information disclosed, and a brief statement of the purpose of the disclosure. If a covered entity has made multiple disclosures to the same person for the same purpose, it may provide the above information only for the first disclosure as long as it also provides the frequency of the disclosures and the date of the last disclosure.28

Within 60 days of the request, a covered entity must provide the accounting or a written statement detailing a reason for why it needs an extension of time (no more than 30 days).29 The covered entity must provide an accounting of disclosures once a year without charge. However, if an individual requests an accounting more than once a year, a reasonable, cost-based fee may be imposed, provided that the individual was informed in advance of the fee and the covered entity also provides the individual with an opportunity to withdraw or modify the request in order to avoid the fee.30

Individuals do not have the right to accountings of certain disclosures, most notably disclosures to carry out treatment, payment, and health care operations and disclosures to the individual actually requesting the accounting of disclosures of their own PHI.31 Furthermore, a covered entity must temporarily suspend an individual’s right to receive an accounting of disclosures made to a health oversight agency or law enforcement official, if the agency or official provides the covered entity with a written statement illustrating that such an accounting would be reasonably likely to impede the agency’s activities. The written statement must also specify the time period for which such a suspension is required.32

The HIPAA Privacy Rule and State Laws

In general, covered entities are required to follow both the Privacy Rule and related state laws. However, if a Privacy Rule provision contradicts state law, the Privacy Rule automatically preempts that law.33 Still, there are exceptions, for example, a state law prevails when that law “provides for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance,”

---

27 45 C.F.R. § 164.528(a).
28 Additionally, if a covered entity has made PHI disclosures for research purposes for 50 or more people, the accounting of disclosures may (with respect to such disclosures for which the PHI of the individual may have been included) provide: the name of the protocol or research activity; a description in plain language about the activity, including purpose and criteria for selecting records; a description of the type of PHI that was disclosed; when the disclosure occurred (date or period of time and the date of the last disclosure); contact information (name, address, and telephone number) of the entity that sponsored the research and of the researcher to whom the PHI was disclosed; and a statement that the PHI of the individual may or may not have been disclosed. If it is reasonably likely that the PHI of the individual was disclosed, and at the request of the individual, a covered entity must assist in contacting the entity or the researcher. See 45 C.F.R. § 164.528(b).
29 45 C.F.R. § 164.528(c)(1)(ii). The covered entity is allowed only one 30-day extension.
30 45 C.F.R. § 164.528(c).
31 Other exceptions include (i) for the facility’s directory or to persons involved in the individual’s care or other notification purposes; (ii) for national security or intelligence purposes; (iii) to correctional institutions or law enforcement officials for certain purposes; (iv) as part of a limited data set; or (v) that occurred prior to the compliance date for the covered entity. See 45 CFR 164.512(k)(2), 45 CFR 164.512(k)(5), and 45 C.F.R. § 164.514(e)(2).
32 45 C.F.R. § 164.528.
33 According to 45 C.F.R. § 160.202, “contrary” means, when used to compare a provision of state law to a standard, requirement, or implementation specification adopted under this subchapter: (1) a covered entity would find it impossible to comply with both the state and federal requirements; or (2) the provision of state law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of part C of title XI of the Act or section 264 of Pub.L.104-191, as applicable.
investigation, or intervention.” State law remains in effect in other circumstances as well, such as when the Secretary of HHS determines that the state law is necessary to prevent fraud and abuse related to health care services, to meet state reporting on health care delivery or costs, or for the purposes of serving a need related to public health, safety, or welfare.

The Privacy Rule also establishes that patients may be afforded stronger privacy safeguards at the state level. The Privacy Rule expressly stipulates that when state laws are more stringent than the Privacy Rule, they remain in force. Therefore, in some states, patients are granted easier access to their personal health information. For example, some state laws actually cap copying and postage fees for medical records, institute shorter time frames for granting access, or require additional accountings of disclosures.

State laws vary widely in terms of how they address health privacy, including the right to access personal health information. Whereas in some states, patients will be afforded only

---

34 45 C.F.R. § 160.203(c), (d).
35 See 45 C.F.R. § 160.203(a) for more instances whereby the Secretary can make a determination where state law prevails. Section 45 C.F.R. § 160.204 outlines a process by which a request can be filed with the Secretary for such a determination. Any exception determination made by the Secretary applies to all persons subject to the state provision in question. When a determination is made, HHS will publish a notice in the Federal Register and on related HHS web sites. See HHS’s Office of Civil Rights, Frequently Asked Questions, Answer ID 407.
36 According to 45 C.F.R. § 160.202, “more stringent” means, in the context of a comparison of a provision of state law and a standard, requirement, or implementation specification, a state law that meets one or more of the following criteria: (1) With respect to the rights of an individual who is the subject of the individually identifiable health information of access to or amendment of individually identifiable health information, permits greater rights of access or amendment, as applicable; (2) With respect to information to be provided to an individual who is the subject of the individually identifiable health information about a use, a disclosure, rights, and remedies, provides the greater amount of information; (3) With respect to recordkeeping or requirements relating to accounting of disclosures, provides for the retention or reporting of more detailed information or for a longer duration; (4) With respect to any other matter, provides greater privacy protection for the individual who is the subject of the individually identifiable health information. 45 C.F.R. § 160.203(b) establishes that state laws that are more stringent are exempted from being preempted by the Privacy Rule.

access rights guaranteed under the Privacy Rule, other states offer stronger rights of access. For instance, in New York, patients have a right to see their protected health information within 10 days, as opposed to the 30 days allowed by the Privacy Rule. New York caps copying charges at 75 cents per page, while California establishes a fee of 25 cents per page for a regular photocopy. In fact, many states, including Illinois, Missouri, Georgia, Arkansas, New Hampshire, and Nevada, cap copying fees to varying degrees. Meanwhile, states such as New York and Florida stipulate that access cannot be denied because of inability to pay.

The HIPAA Privacy Rule and Electronic Access to Medical Records

The Administrative Simplification section of HIPAA, under which the Privacy Rule is mandated, was aimed at fostering the electronic exchange of health information. In that section, Congress called for the development of a “health information system through the establishment of standards and requirements for the electronic transmission of certain health information.”

The Privacy Rule and the related Security Rule were devised to establish a baseline of policies and practices to safeguard health information to

---

42 The HIPAA Security Rule (with an April 2005 compliance date) provides detailed provisions related to how covered entities must protect electronic health information.
ensure that technology would improve care without jeopardizing confidentiality.

As the health care industry adopts more technologically sophisticated methods of record maintenance and patient communication, patients’ access to their own personal health information could potentially become easier and more cost-efficient. By guaranteeing patients access to their own health information, the Privacy Rule set in place an important incentive for consumers to actively engage in health information technologies, such as electronic medical record (EMR) systems and personal health records (PHRs). In fact, the Privacy Rule requires that covered entities provide information in the requested format if it is “readily producible.” At the same time, covered entities can exercise their ability to impose reasonable fees associated with providing access to personal health information. As such, the preamble of the Privacy Rule points out that if, in the course of providing access to a patient, electronic copies are made to a computer disk, any fees could include, for instance, the cost of the computer disk. It is important to note that where covered entities receive the services of vendors, or “business associates,” in the course of developing an EMR system, for instance, the contract must stipulate that the business associate will make protected health information available for access, amendment, and accounting of disclosures.

However, since the Privacy Rule only applies to “covered entities,” some entities that have access to protected health information are not covered by the federal law. For instance, some private companies offering consumers PHR services are not covered by the law and therefore the federal right to an accounting of disclosures would not apply. This is problematic and serves as a critical reminder that strong laws and standards must be implemented to protect and extend established rights of patients.

As long as covered entities are collecting, using, and storing protected health information, the Privacy Rule and its access requirements apply to that entity—whether the information is stored electronically or not. The opportunity exists to build in patient access to records, even if not directly required by HIPAA. State laws related to patient access may also surpass HIPAA’s requirements in this area.

**Patient Access and the Record Locator Service**

Connecting for Health’s Record Locator Service (RLS) is intended as a critical line of communication within and among sub-network organizations (SNOs), and, as a matter of principle, patients should be able to access the RLS. At this stage, however, there are serious privacy and policy issues that must be addressed regarding such access.

Both the HIPAA Privacy Rule and the Connecting for Health “Architecture for Privacy in a Networked Health Environment” are instructive here. As discussed above, patients have a federal right to see and copy their medical records held by a provider. However, since the RLS may not be covered under the HIPAA Privacy Rule as a provider, plan, or clearinghouse, there may be no legal obligation to provide patients access to the information in the index. But, as a matter of principle, the RLS should be designed to provide such access in a secure, authenticated manner.

The nine principles articulated in the Connecting for Health “Architecture for Privacy in a Networked Health Information Environment” support this philosophy. The most pertinent principles are “openness and transparency,” “individual participation and control,” and “data integrity and quality.” The principle of openness and transparency asserts that patients should be able to establish what information exists about them in the data

---

43 Like electronic health records (EHRs), personal health records (PHRs) can be Internet-based and are designed to provide easy access to important health-related information about patients. Unlike EMRs, however, PHRs would be controlled entirely by the patient and would include information provided by the patient.

44 45 C.F.R. § 164.524(c)(2).

45 Available at: http://aspe.hhs.gov/admnsimp/final/PvcPre02.htm.

46 See 164.504(e)(2)(ii)(E-G).

47 A sub-network organization (SNO) is to operate as a health information data exchange organization (whether regionally or affinity-based) that operates as a part of the National Health Information Network (NHIN), a nationwide environment for the electronic exchange of health information made up of a “network of networks.”
market and in government databases, should be able to track how that information is used, and by whom. The principle of individual participation and control clearly stipulates that patients should be able to see and amend their information: “at all stages in the information chain, they should be able to inspect and query their information...they should have clear avenues to correct information.” The data integrity and quality principle further emphasizes this point, establishing that patients “should have clear avenues to view all information that has been collected on them, and to ensure that that information is accurate, complete, and timely.”

Based on the access provisions of the Privacy Rule and the principles articulated in the Connecting for Health Architecture for Privacy in a Networked Health Information Environment, it becomes clear that, ideally, patients should have access to the information in the RLS. Allowing patients the opportunity to independently access information held in the RLS will empower patients to be more informed and active in their care.

However, providing access to the RLS is not a simple task. Significant privacy and security concerns come into play when considering giving patients direct access to the service. Authentication poses a significant challenge for allowing such access. Ensuring that information is not accessed by unauthorized individuals is central to establishing privacy and security, but developing a reliable and convenient method of authentication even beyond the issue of patient access remains a significant obstacle in the field of health information exchange. The problem with authentication is both fundamental and widespread. Indeed, one of the longest functioning SNOs—the Indianapolis Network for Patient Care (INPC)—cites authentication as a challenge. Outside of the health care industry, experts in banking and government continue to struggle with devising policies and technologies that would allow individuals access to data while ensuring security. Many proposals have come forth. For instance, the Liberty Alliance Project—an open standards organization representing over 160 companies—emphasizes decentralized authentication, allowing individuals to link “elements of their identity...without centrally storing all their personal information.”

A few current health information exchange networks have taken steps to address patient access in a secure environment. Caregroup, a Massachusetts-based hospital consortium using electronic information exchange, is often noted for its strong privacy and security practices, including those for authentication. Caregroup implements a three-tiered authentication process for providers, requiring users to prove identity with a user name, password, and a SecurID Token system. Caregroup’s PHR service for patients follows this model—requiring users to authenticate themselves twice—passing through both a front and interior “door.”

The RLS poses unique challenges related to patient access and authentication; yet given the imperative of allowing patients the ability to see, copy, and amend their personal health information, it is important to work towards realizing goals supported by the Connecting for Health Architecture for Privacy in a Networked Health Information Environment principles.

Recommendations:
• Each SNO should have a formal process through which information in the RLS can be requested by a patient or on a patient’s behalf.
• Participating entities and SNOs shall consider and work towards providing patients direct, secure access to the information about them contained in the RLS.

Conclusion
The access provisions of the Privacy Rule serve as an important baseline for ensuring that patients have adequate control over their personal health information. Meanwhile the
principles articulated in the Connecting for Health “Architecture for Privacy in a Networked Health Information Environment” recommend taking these rights further, establishing that patients should have access to all their information, including information held outside of a covered entity. With this in mind, a discussion about how to give patients access to the information held in the RLS is appropriate.

The RLS could ultimately empower patients. Patients’ ability to access a reliable list of where their personal health information is stored could significantly enhance their ability to access and potentially amend information. It is, therefore, important to adopt policies and procedures that adhere to the notion that patients should have the same access to their own information that health care providers do.

EHRs, PHRs, and similar information systems could significantly enhance patient participation, with untold benefits to both individuals and the general public. Using the RLS and asserting their rights to access under the Privacy Rule could go a long way to ensuring that patients play an active and informed role in their own health care.
Acknowledgements
The members of the Connecting for Health Policy Subcommittee have accomplished an extraordinary task in less than a year’s time—the development of an evolving piece of work that can serve as the core of nationwide health information exchange—the policy components of The Common Framework. During this time, we have been fortunate to work with respected experts in the fields of health, information technology, and privacy law, all of whom have contributed their time, energy, and expertise to a daunting enterprise. Our consultants and volunteers have worked long hours in meetings and conference calls to negotiate the intricacies of such issues as privacy, security, authentication, notification, and consent in health information exchange. We offer them our heartfelt thanks for taking on this journey with us, and look forward to the remaining work ahead.

In addition, we would like to offer special thanks to the volunteers and consultants who authored the initial drafts of this body of work—their hard work created a strong foundation upon which to focus the Subcommittee’s deliberations: Stefaan Verhulst, Clay Shirky, Peter Swire, Gerry Hinkley, Allen Briskin, Marcy Wilder, William Braithwaite, and Janlori Goldman.

Finally, we must note that none of this work would have been possible without the leadership and inspiration of our co-chairs, William Braithwaite and Mark Frisse. They have led us with steady hands and determination of spirit.

Connecting for Health Policy Subcommittee

William Braithwaite, MD, eHealth Initiative, (Co-Chair)

Mark Frisse, MD, MBA, MSc, Vanderbilt Center for Better Health, (Co-Chair)

Laura Adams, Rhode Island Quality Institute

Phyllis Borzi, JD, George Washington University Medical Center

Susan Christensen*, JD, Agency for Healthcare Research and Quality, United States Department of Health and Human Services

Art Davidson, MD, MSHP, Denver Public Health

Mary J Deering*, PhD, National Cancer Institute/National Institutes of Health, United States Department of Health and Human Services

Jim Dempsey, JD, Center for Democracy and Technology

Hank Fanberg, Christus Health

Linda Fischetti*, RN, MS, Veterans Health Administration

Seth Foldy, MD, City of Milwaukee Health Department

Janlori Goldman, JD, Columbia College of Physicians and Surgeons

Ken Goodman, PhD, University of Miami

John Halamka, MD, CareGroup Healthcare System

Joseph Heyman, MD, American Medical Association

Gerry Hinkley, JD, Davis, Wright, Tremaine LLP

Charles Jaffe, MD, PhD, Intel Corporation

Jim Keese, Eastman Kodak Company

Linda Kloss, RHIA, CAE, American Health Information Management Association

Gil Kuperman, MD, PhD, New York-Presbyterian Hospital

Ned McCulloch, JD, IBM Corporation

Patrick McMahon, Microsoft Corporation

Omid Moghadam, Intel Corporation
Joyce Niland, PhD, City of Hope National Medical Center

Louise Novotny, Communication Workers of America

Michele O’Connor, MPA, RHIA, MPI Services Initiate

Victoria Prescott, JD, Regenstrief Institute for Healthcare

Marc A. Rodwin, JD, PhD, Suffolk University Law School

Kristen B. Rosati, JD, Coppersmith Gordon Schermer Owens & Nelson PLC

Sara Rosenbaum, JD, George Washington University Medical Center

David A. Ross, ScD, Public Health Informatics Institute

Clay Shirky, New York University (Chair, Technical Subcommittee)

Don Simborg, MD, American Medical Informatics Association

Michael Skinner, Santa Barbara Care Data Exchange

Joel Slackman, BlueCross/BlueShield Association

Peter P. Swire, JD, Moritz College of Law, Ohio State University

Paul Tang, MD, Palo Alto Medical Foundation

Micky Tripathi, Massachusetts eHealth Collaborative

Cynthia Wark*, CAPT, United States Public Health Service Commissioned Corps, Centers for Medicare and Medicaid Services, United States Department of Health and Human Services

John C. Wiesendanger, MHS, West Virginia Medical Institute/Quality Insights of Delaware/Quality Insights of Pennsylvania

Marcy Wilder, JD, Hogan & Hartson LLP

Scott Williams, MD, MPH, HealthInsight

Robert B. Williams, MD, MIS, Deloitte

Joy Wilson, National Conference of State Legislatures

Rochelle Woolley, RxHub

Amy Zimmerman-Levitan, MPH, Rhode Island State Department of Health

*Note: Federal employees participate in the Subcommittee but make no endorsement
Auditing Access to and Use of a Health Information Exchange
Auditing Access to and Use of a Health Information Exchange
The document you are reading is part of *The Connecting for Health Common Framework*, which is available in full and in its most current version at: [http://www.connectingforhealth.org/](http://www.connectingforhealth.org/).

The Common Framework will be revised and expanded over time. As of October 2006, the Common Framework included the following published components:

**The Common Framework: Overview and Principles**

**Policy Guides: How Information is Protected**

- **P1** The Architecture for Privacy in a Networked Health Information Environment
- **P2** Model Privacy Policies and Procedures for Health Information Exchange
- **P3** Notification and Consent When Using a Record Locator Service
- **P4** Correctly Matching Patients with Their Records
- **P5** Authentication of System Users
- **P6** Patients’ Access to Their Own Health Information
- **P7** Auditing Access to and Use of a Health Information Exchange
- **P8** Breaches of Confidential Health Information
- **P9** A Common Framework for Networked Personal Health Information

**Technical Guides: How Information is Exchanged**

- **T1** The Common Framework: Technical Issues and Requirements for Implementation
- **T2** Health Information Exchange: Architecture Implementation Guide
- **T3** Medication History Standards
- **T4** Laboratory Results Standards
- **T5** Background Issues on Data Quality
- **T6** Record Locator Service: Technical Background from the Massachusetts Prototype Community

**Future Technical Guides**

**Future Policy Guides**

**Model Contractual Language**

- **M1** Key Topics in a Model Contract for Health Information Exchange
- **M2** A Model Contract for Health Information Exchange
Auditing Access to and Use of a Health Information Exchange*

This document recommends an initial set of logging and audit practices for a National Health Information Network (NHIN). Effective logging and audit practices are essential safeguards as electronic protected health information (ePHI) is shared at the regional and national levels, and can assure participating institutions that there is compliance with legal requirements for technical, physical, and administrative safeguards. At least as importantly, publicly announced audit and logging practices can foster trust among individual patients and the general public that their data is being used only in appropriate ways.

Part I explains the logging and other audit requirements under HIPAA. These legal requirements form the baseline for auditing in any eventual system for sharing ePHI.

Part II sets forth the general conclusions concerning logging and auditing at the level of covered entities, of each sub-network organization (SNO)¹ and for the Record Locator Service (RLS). The principle conclusion is that HIPAA should form the baseline for individual covered entities, but that logging and auditing practices, which may go beyond HIPAA requirements, should be in place for SNOs and the RLS.

Part III implements those general conclusions by setting forth a checklist for auditing and accountability for each SNO and the RLS. It supplements the checklist with a list of recommended additional measures, including independent third-party auditing for the RLS.

I. Logging and Audit Controls under HIPAA

It is useful to understand current law before deciding what new logging and audit control requirements, if any, should be used when handling ePHI. The HIPAA Privacy Rule does not specifically mention logging or audits. It does provide that “a covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.” 45 CFR § 164.530 (c)(1). An effective audit and logging system will often be part of the overall set of safeguards expected under the Privacy Rule.

The HIPAA Security Rule is more specific. Section 164.312(b) requires audit controls as a standard: “[Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.]” The United States Department of Health & Human Services explained that the nature of the audit controls will depend on the context: “We believe that it is appropriate to specify audit controls as a type of technical safeguard. Entities have flexibility to implement the standard in a manner appropriate to their needs as deemed necessary by their own risk analyses.” 68 Fed. Reg. at 8355 (Feb. 20, 2003).

The HIPAA Security Rule also mandates “information system activity review” as an element of administrative safeguards:

©2006, Markle Foundation
This work was originally published as part of The Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange and is made available subject to the terms of a license (License) which may be viewed in its entirety at: http://www.connectingforhealth.org/license.html. You may make copies of this work; however, by copying or exercising any other rights to the work, you accept and agree to be bound by the terms of the License. All copies of this work must reproduce this copyright information and notice.
“Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.” 45 CFR § 164.308(a)(1)(ii)(D). Once again, the sophistication of the required safeguard depends on the setting: “Our intent for this requirement was to promote the periodic review of an entity’s internal security controls, for example, logs, access reports, and incident tracking. The extent, frequency, and nature of the reviews would be determined by the covered entity’s security environment.” 68 Fed. Reg. at 8347.

One additional relevant provision in the HIPAA Security Rule is Section 164.308(a)(5)(ii)(C), which concerns log-in monitoring. The Rule sets forth an addressable implementation specification (i.e., good practice but not necessarily required), which covers “[p]rocedures for monitoring log-in attempts and reporting discrepancies.”

Beyond these federal requirements, there may be state and local laws that create requirements in the areas of logging and audit controls that will need to be assessed by individual SNOs and their participants.

II. Logging and Audit Controls in a National Health Information Network

With these HIPAA requirements as a baseline, audit and logging practices will differ in important respects among the various actors in a National Health Information Network. This section will provide a general analysis of the level of logging and audit controls to be expected among covered entities within each SNO, at each SNO itself, and for inter-SNO sharing. The next section will recommend specific logging and audit practices to apply at the SNO and inter-SNO levels.

For covered entities within each SNO, the baseline will be the requirements of the HIPAA Security Rule, discussed briefly in the prior section. The Security Rule contemplates that the level of audit controls required varies with the security environment. Throughout HIPAA, requirements are “scalable,” which means that large and sophisticated entities are expected to establish more rigorous safeguards than small entities. For audit, scalability means that small entities often have less thorough safeguards than large entities.

In setting policy for logging and audit control practices for covered entities within each SNO, it is important to recognize the small scale of many covered entities. Even for many large covered entities, current logging and audit control systems likely do not match the rigor and complexity of the best practices of large institutions. Given these current practices, it would likely be difficult to insist on heightened logging and audit control standards for each covered entity within SNOs. Any attempt to require such standards would quite possibly discourage participation in the overall system and further delay participation. Our recommendation at this time is thus not to require heightened logging and audit control standards for each covered entity or other participant within a SNO.

The analysis shifts, however, for logging and audit control practices at the level of each SNO in order to best safeguard ePHI. Each SNO is expected to be a sophisticated entity, operating at a scale that is consistent with rigorous audit and other security practices. Compared with individual providers, who often depend largely on paper records, SNOs are likely to rely more heavily on electronic health records, which are typically more suitable than paper records for enhanced and automated logging and audit control approaches. In order to promote trust among patients and participating institutions, we therefore recommend excellent logging and audit control practices at the SNO level, as described in the next section.

The case for strong logging and audit control standards is even stronger for inter-SNO sharing through the RLS. As discussed in previous documents of Connecting for Health, the RLS will provide a means for locating records of an individual patient that...
are held by different data providers, including in different SNOs. It will be crucial to build public confidence in the good data handling practices of the RLS. A transparent and effective method for logging and audit controls is one important component of the case that the public deserves to trust the RLS. The next section recommends specific practices, notably including an independent, third-party audit on a regular basis.

In establishing these strict logging and audit practices at the SNO and inter-SNO levels, it is important to clarify what types of records are likely to move through such information systems. As contemplated in the Connecting for Health Common Framework, the RLS itself will not contain clinical data. Instead, the RLS will contain demographic data, in order to identify and provide contact information for the actual holders of clinical records. Transfer of clinical records will be “point to point.” That is, an entity seeking the records of a particular patient may learn about other record holders through the RLS. That entity then will directly contact the other record holders in order to receive the clinical records. For purposes of logging and audit controls, this structure means that the flows of demographic information will be carefully tracked at the RLS level.

Transfers of clinical records, however, will not take place through the RLS itself, and will thus be subject to the logging and audit practices at the level of each entity. As a related point, SNOs may operate in a similar way. Whatever demographic (or other) information moves through the SNO would be subject to audit under the strict logging and audit standards contemplated here for SNOs. Transfers of clinical records, however, may take place through paths that do not include a SNO.

III. Specific Logging and Audit Recommendations

In preparing this paper on logging and audit practices, it has been helpful to review the actual audit documents of some large, cutting-edge health care organizations. The discussion here draws on those documents, as well as some publicly available materials.2

A. Audit and Accountability Checklist

We first put forward a recommended audit and accountability checklist. This checklist is intended to apply at least to SNOs and the RLS, and it represents good practice for a broader range of covered entities.

2 One helpful, published source of information on audits is “Security and Privacy Auditing in Health Care Information Technology.” This paper was published in 2001 by the Joint Security and Privacy Committee of three organizations, the National Electrical Manufacturers Association, the European Coordination Committee of the Radiological and Electromedical Industry, and the Japan Industries Association of Radiological Systems, available at: http://www.nema.org/medical. The paper provides a useful synopsis, in six pages, of the elements of an audit for health care information technology.

For additional background, there is a recent paper on “Immutable Audit Logs” by Jeff Jonas and Peter Swire for the Markle Task Force on National Security in the Information Age. See http://www.markle.org. The paper analyzes the heightened auditing procedures that can be used to increase public confidence about systems that are not transparent to the public.

For more information on industry best practices in healthcare security auditing, see RFC 3881 (http://www.faqs.org/rfcs/rfc3881.html), Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications.
Audit & Accountability Checklist

Audit and Accountability. Audit is the practice of recording the occurrence of selected system events; management uses reports/alerts generated from audit records to monitor the appropriateness of activities. Accountability results when activities are attributable to individuals.

<table>
<thead>
<tr>
<th></th>
<th>Yes</th>
<th>NO</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>The system is required to log users' system login and logoff with date and time, or, if the system does not have the capability to record login/logoff activity, it may rely on an external security system's access control logging function to record access.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>The system must have the ability to log read, create, update, delete, forward, and print access initiated by individuals and processes for systems containing confidential and restricted data. For data warehouses, data marts, and operational data stores, the system must have the ability to log queries, or alternatively the tables read must be logged. Row-level logging must be available on demand.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 3. | All audit records must be identified by a unique record key or number, and include:  
   - User identifier/name of user  
   - Time/date  
   - Device identifier (when used to access)  
   - Source (i.e. subsystem or system of origin of the event [access request])  
   - Content (type of data being accessed or activity being performed)  
   - Type of action (e.g. read, write, update, delete, or copy) or access for diagnostic purposes. |   | |
| 4. | Unsuccessful login attempts and access violations within the system must be logged. |   | |
| 5. | Security administrative functions must be logged. |   | |
| 6. | System administrative functions must be logged. |   | |
| 7. | Audit records must be protected against unauthorized access, modifications, and deletion. |   | |
| 8. | Audit records must be readily available for 90 days and archived for a minimum of two years, or up to the six years used for the archiving of HIPAA disclosures. |   | |
| 9. | Security administrators and auditors can request or generate reports which may consist of any or all of the audit record elements for any or all types of actions. |   | |
B. Categories of Logging and Audit Controls

In addition to the checklist, there are additional logging and audit control functions that are generally recommended at the SNO and RLS level. Some of these functions are included in other papers of the Connecting for Health Policy Subcommittee, such as tracking of authentication or responses to security breaches, but the list here errs on the side of inclusion:

1. Audit of VIP records.
2. Procedures for follow-up on suspicious activity, such as indications of possible privacy or security breaches.
4. Review of system administrator authorizations and activity.
5. Review of physical access to data centers.
6. Other review of technical, physical, and administrative safeguards as established by the policies of the organization.

Under the HIPAA Privacy and Security Rules, a legal argument can be made that the high-quality practices set forth in Section III of this paper are approximately what is required by the scalable requirements of those rules. Whether or not this legal position is correct, the practices set forth in this paper provide significant detail to assist organizations in developing their own logging and audit practices. A transparent and effective logging and audit control approach can help assure trust in the expanded use of electronic health records by patients and the general public.

B. Categories of Logging and Audit Controls

1. Audit of VIP records.
2. Procedures for follow-up on suspicious activity, such as indications of possible privacy or security breaches.
4. Review of system administrator authorizations and activity.
5. Review of physical access to data centers.
6. Other review of technical, physical, and administrative safeguards as established by the policies of the organization.

Beyond these sorts of compliance efforts, it is recommended that SNOs and the RLS have random audits of demographic and clinical records, based on the level of risk for that portion of the system. SNOs may wish to provide for some level of random audits (sampling) of the participants in the SNOs. Random audits should be done for records held at the SNO level and within the RLS. For the RLS (and where appropriate for each SNO), an independent third-party should perform such random audits, with public reporting of at least the principal results.

Conclusion

This paper provides a general template for assessing where excellent logging and audit practices are especially essential, at the SNO and RLS levels. It then recommends a checklist for audits, as well as a supplementary list of measures to be taken at the SNO and RLS levels to ensure an overall high quality of audit and accountability.

3 See Connecting for Health, “Authentication of System Users,” and “Breaches of Confidential Health Information.”
Acknowledgements

The members of the Connecting for Health Policy Subcommittee have accomplished an extraordinary task in less than a year’s time—the development of an evolving piece of work that can serve as the core of nationwide health information exchange—the policy components of The Common Framework. During this time, we have been fortunate to work with respected experts in the fields of health, information technology, and privacy law, all of whom have contributed their time, energy, and expertise to a daunting enterprise. Our consultants and volunteers have worked long hours in meetings and conference calls to negotiate the intricacies of such issues as privacy, security, authentication, notification, and consent in health information exchange. We offer them our heartfelt thanks for taking on this journey with us, and look forward to the remaining work ahead.

In addition, we would like to offer special thanks to the volunteers and consultants who authored the initial drafts of this body of work—their hard work created a strong foundation upon which to focus the Subcommittee’s deliberations: Stefaan Verhulst, Clay Shirky, Peter Swire, Gerry Hinkley, Allen Briskin, Marcy Wilder, William Braithwaite, and Janlori Goldman.

Finally, we must note that none of this work would have been possible without the leadership and inspiration of our co-chairs, William Braithwaite and Mark Frisse. They have led us with steady hands and determination of spirit.

Connecting for Health Policy Subcommittee

William Braithwaite, MD, eHealth Initiative, (Co-Chair)

Mark Frisse, MD, MBA, MSc, Vanderbilt Center for Better Health, (Co-Chair)

Laura Adams, Rhode Island Quality Institute

Phyllis Borzi, JD, George Washington University Medical Center

Susan Christensen*, JD, Agency for Healthcare Research and Quality, United States Department of Health and Human Services

Art Davidson, MD, MSHP, Denver Public Health

Mary Jo Deering*, PhD, National Cancer Institute/National Institutes of Health, United States Department of Health and Human Services

Jim Dempsey, JD, Center for Democracy and Technology

Hank Fanberg, Christus Health

Linda Fischetti*, RN, MS, Veterans Health Administration

Seth Foldy, MD, City of Milwaukee Health Department

Janlori Goldman, JD, Columbia College of Physicians and Surgeons

Ken Goodman, PhD, University of Miami

John Halamka, MD, CareGroup Healthcare System

Joseph Heyman, MD, American Medical Association

Gerry Hinkley, JD, Davis, Wright, Tremaine LLP

Charles Jaffe, MD, PhD, Intel Corporation

Jim Keese, Eastman Kodak Company

Linda Kloss, RHIA, CAE, American Health Information Management Association

Gil Kuperman, MD, PhD, New York-Presbyterian Hospital

Ned McCulloch, JD, IBM Corporation

Patrick McMahon, Microsoft Corporation

Omid Moghadam, Intel Corporation
Joyce Niland, PhD, City of Hope National Medical Center

Louise Novotny, Communication Workers of America

Michele O’Connor, MPA, RHIA, MPI Services Initiate

Victoria Prescott, JD, Regenstrief Institute for Healthcare

Marc A. Rodwin, JD, PhD, Suffolk University Law School

Kristen B. Rosati, JD, Coppersmith Gordon Schermer Owens & Nelson PLC

Sara Rosenbaum, JD, George Washington University Medical Center

David A. Ross, ScD, Public Health Informatics Institute

Clay Shirky, New York University (Chair, Technical Subcommittee)

Don Simborg, MD, American Medical Informatics Association

Michael Skinner, Santa Barbara Care Data Exchange

Joel Slackman, BlueCross/BlueShield Association

Peter P. Swire, JD, Moritz College of Law, Ohio State University

Paul Tang, MD, Palo Alto Medical Foundation

Micky Tripathi, Massachusetts eHealth Collaborative

Cynthia Wark*, CAPT, United States Public Health Service Commissioned Corps, Centers for Medicare and Medicaid Services, United States Department of Health and Human Services

John C. Wiesendanger, MHS, West Virginia Medical Institute/Quality Insights of Delaware/Quality Insights of Pennsylvania

Marcy Wilder, JD, Hogan & Hartson LLP

Scott Williams, MD, MPH, HealthInsight

Robert B. Williams, MD, MIS, Deloitte

Joy Wilson, National Conference of State Legislatures

Rochelle Woolley, RxHub

Amy Zimmerman-Levitan, MPH, Rhode Island State Department of Health

*Note: Federal employees participate in the Subcommittee but make no endorsement
Breaches of Confidential Health Information
Breaches of Confidential Health Information
The document you are reading is part of *The Connecting for Health Common Framework*, which is available in full and in its most current version at: [http://www.connectingforhealth.org/](http://www.connectingforhealth.org/). The Common Framework will be revised and expanded over time. As of October 2006, the Common Framework included the following published components:
Breaches of Confidential Health Information*

This document outlines a proposed policy for sub-network organizations (SNOs) regarding breaches of confidentiality of patient data.

Definitions
When used in this policy, the following words shall have the definitions indicated:

- **A Sub-Network Organization (SNO)** shall operate as a health information data exchange organization (whether regionally or affinity-based) that operates as a part of the National Health Information Network (NHIN), a nationwide environment for the electronic exchange of health information made up of a “network of networks.”

- **Confidentiality** shall have the same meaning as in the HIPAA Security Rule, which is “the property that data or information is not made available or disclosed to unauthorized persons or processes.”

- **Breach of Confidentiality** shall mean that confidential data or information has been made available or disclosed to unauthorized persons or processes.

- **Participant** shall have the same meaning as in the **Connecting for Health** “Model Contract for Health Information Exchange,” which is a party that is registered with the SNO to act as a Data Provider and/or as a Data Recipient.

* **Connecting for Health** thanks Victoria M. Prescott, General Counsel and Business Development Specialist, Regenstrief Institute for Health Care, for drafting this paper.

1 45 C.F.R. § 164.304.

2 See **Connecting for Health**, “A Model Contract for Health Information Exchange,” Section 2 (Definitions).

3 45 C.F.R. § 164.304.

4 45 C.F.R. § 164.501.

Executive Summary
This proposed SNO policy includes the following:

A. **Compliance with HIPAA Security Rule**: The SNO will comply with the HIPAA Security Rule. The SNO Participants will be required to comply with all applicable federal, state, and local laws.

B. **Responsibility of Participants to Train Personnel and Enforce Policy**: A SNO Participant that may have access to patient data via the SNO network, must appropriately train its personnel and inform them that any breach of confidentiality is actionable. Each Participant should follow and enforce its own institution’s confidentiality policies and disciplinary procedures.

C. **Notification of Breach**: The SNO itself must report any breaches and/or security incidents to the particular data provider whose data was improperly used, as in most
cases the SNO is a business associate of some or all of its Participants. Each SNO Participant must agree to inform the SNO of any serious breach of confidentiality, but is not required to notify the SNO of minor breaches. [Note: As mentioned earlier, any SNO policy should require that the Participants comply with all applicable federal, state, and local laws, which may include laws relating to notification of patients. Participants and SNOs should also work towards implementing a system that ensures affected patients are notified in the event of a breach.]

D. Withdrawal from the SNO: Provisions could be included in SNO agreements relating to withdrawal from the SNO. The Connecting for Health “Model Contract for Health Information Exchange” provides a variety of model provisions that could allow Participants to terminate their participation freely at any time, require that termination be preceded by a substantial period of advance notice, or require that Participants maintain their participation for a certain period of time. The Connecting for Health “Model Contract for Health Information Exchange” also provides a model provision allowing for a Participant to withdraw from a SNO if a serious breach of its patient data has occurred.5 SNOs and Participants are encouraged to consider the particular circumstances of small provider practices in developing relevant terms for withdrawal from SNO provisions in their SNO agreements.

E. Indemnification for Breaches of Confidentiality: The Connecting for Health “Model Contract for Health Information Exchange” provides a variety of model provisions concerning indemnification. A SNO may also choose to adopt special rules governing indemnification for particular situations, such as a breach of confidentiality of protected health information. For example, the SNO’s agreement could provide for mutual indemnification between all Participants for breaches of confidentiality of patient data, with the scope of the indemnification to be determined by the SNO.

Detailed Discussion and Sample Contract Language

Compliance with HIPAA Security Rule

The SNO should comply with the HIPAA Security Rule and thus do the following: (1) ensure the confidentiality, integrity, and availability of all electronic protected health information the SNO creates, receives, maintains, or transmits; (2) protect against any reasonably anticipated threats or hazards to the security and integrity of such information; (3) protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under HIPAA; and (4) ensure compliance with this regulation by its workforce. Of course, the SNO must also comply with other applicable federal, state, and local laws.

Any SNO participation or vendor agreement should also require that the other parties comply with all applicable federal, state, and local laws.

Responsibility of Participants to Train Personnel and Enforce Policy

The SNO policy should mandate that the SNO Participant appropriately train its personnel9 and inform its personnel that any breach of

---

confidentiality is actionable. See relevant sample contract excerpt below:

Section 4.04 Access to Information By Participants' Personnel. Each Participant shall determine the personnel under its control (including any personnel of physician practice groups allowed to access Information pursuant to Section 4.01(b)) who may [have] access [to patient data via] the Network ... For Participants who are technically able to do so, each Participant shall provide daily electronic files to [the SNO] of the individuals it designates under this Section. If such electronic notice is not feasible, each Participant shall provide lists of such individuals through e-mail, hard copy, or facsimile to [the SNO] no less frequently than biweekly. Each Participant shall certify:

(a) That such designated personnel have received training regarding the confidentiality of PHI under the Privacy Rule and all other applicable State and local laws and agree to protect the Information in compliance with the Privacy Rule, such laws and this Agreement;
(b) That such designated personnel shall only access the Network for [allowable] purposes;
(c) That such designated personnel have agreed to hold any passwords, or other means for accessing the Network, in a confidential manner and to release them to no other individual;
(d) ...; and
(e) That such designated personnel agree and understand that their failure to comply with the terms of this Agreement may result in their exclusion from the Network and may constitute cause for disciplinary action by the Participant.

Further, the SNO may also want to require that the SNO Participant enforce these confidentiality provisions by appropriately disciplining its personnel. No specific policy is set at the SNO level for Participants, because each Participant should already have its own confidentiality policies and disciplinary procedures within its organization. See relevant sample contract excerpt below:

Section 5.02 Enforcement of Confidentiality by Participants. Each Participant agrees to enforce the confidentiality provisions of this Agreement by appropriately disciplining individuals within each Participant's organization who violate the confidentiality of the Information pursuant to each Participant's respective confidentiality and disciplinary policies. Such discipline may include, but not be limited to: warnings; suspensions; termination; or modification, suspension, or revocation of medical staff privileges.

Notification of Breach
Notification of breach of confidentiality of patient data is impacted not only by HIPAA laws, but also by state breach notification laws that are becoming more common. Thus, any SNO policy should require that the Participants (and the SNO itself) comply with all applicable federal, state, and local laws.

In addition, the SNO must report any breaches to the particular data provider whose data was improperly used. This would not be limited to serious breaches, but would include all breaches. Most SNOs will be a business associate of the Participants who provide patient data to the SNO, in which case the SNO is required under HIPAA to report all Security

10 "The Indiana Network for Patient Care: A Case Study of a Successful Healthcare Data Sharing Agreement," ABA Health eSource, Volume 2 Number 1 (Sept 2005), re-printed in Healthcare Informatics Online (Sept. 28, 2005). All references in this document to “sample contract excerpt” refer to this document and are intended for illustrative purposes only.

11 Of course, the SNO needs to establish its own internal policy for its own employees.

12 Data here means patient data provided by the data provider to or through the SNO.
Breaches of Confidential Health Information

Incidents to the covered entity. See relevant sample contract excerpts below:

Section 8.03 Report of Improper Use or Disclosure. [The SNO] agrees promptly to report to a [Participant] any use or disclosure of the [Participant’s] PHI not provided for by this Agreement of which [the SNO] becomes aware.

and


(a) ...
(b) [The SNO] agrees promptly to report to a [Participant] any Security Incident related to the [Participant’s] ePHI of which [the SNO] becomes aware.

Similarly, each Participant must agree to inform the SNO of any serious breach of confidentiality. It is not necessary for a Participant to inform the SNO of minor breaches of confidentiality (unless there is otherwise a legal duty to disclose such breaches to the SNO). While it is difficult to define what would rise to the level of a “serious” breach, SNOs and Participants might decide that the breaches of concern would be ones that impact: (1) the viability of the network, (2) the trust that other Participants have in each other, or (3) the legal liability of the SNO. In addition, SNOs and Participants might decide that repeated minor breaches that demonstrate a pattern of lax internal operations or enforcement may also rise to the level of a “serious” breach. See relevant sample contract excerpt below:

Section 5.01 Confidentiality. The Participants agree that any Information obtained from the Network will be kept confidential pursuant to the Privacy Rule and all other applicable federal, state, and local laws, statutes and regulations, as well as each Participant’s own rules and regulations governing the confidentiality of patient records and information. Participants agree to report promptly to the Management Committee any serious breach of the confidentiality of the Information of which it becomes aware. ...

As mentioned above, some states have enacted laws that require the notification of individuals whose personal data is compromised. Several federal bills have also been introduced that include breach notification (which could pre-empt state law if and when enacted). SNOs must analyze any relevant state laws in this regard and what impact such laws may have on the SNO’s operations. For example, a state law may require that a SNO notify a covered entity/Participant of a breach, but the burden to notify patients may fall on the covered entity/Participant rather than the SNO. In any event, procedures need to be in place that will address this scenario in advance of an event. Communities should be prepared to comply with evolving national norms regarding breach notification, and Participants and SNOs should work towards implementing a system that ensures affected patients are notified in the event of a breach.

Withdrawal from the SNO

SNOs may wish to consider including a provision in their Participant agreements allowing for withdrawal from the SNO. As noted above, the Connecting for Health “Model Contract for Health Information Exchange” provides a variety of model provisions that could allow Participants to terminate their participation freely at any

14 Section 8.14 is a new amendment to Regenstrief’s INPC Agreement that has not been published yet.
15 In 2005, security breach notification legislation (also referred to as victim’s rights laws) was introduced in at least 35 states. Nineteen states passed some form of legislation in this regard (including AK, CA, CT, DE, FL, GA (data brokers only), IL, IN (state agencies only), LA, ME, MN, MT, NV, NJ, NY, NC, ND, RI, TN, TX, WA). Several more state bills are under consideration. Web sites that summarize state laws include: http://www.ncsl.org/programs/lis/CIP/priv/breach.htm; http://www.sia.com/state_affairs/pdf/BreachofSecurityChart.pdf; and http://www.consumersunion.org/campaigns/Breach_laws_May05.pdf.
time, require that termination be preceded by a substantial period of advance notice, or require that Participants maintain their participation for a certain period of time. In general, SNOs and Participants are encouraged to consider the particular circumstances of small provider practices in developing relevant terms for withdrawal from SNO provisions in their SNO agreements.

The Connecting for Health “Model Contract for Health Information Exchange” also provides a model provision allowing for a Participant to withdraw from a SNO if a serious breach of its patient data has occurred, as described here. See relevant sample contract excerpt below:

Section 12.03 Withdrawal of a Participant. ... The following shall constitute adequate cause for the withdrawal from this Agreement:

(a) A significant breach of another Participant’s duties of confidentiality under ARTICLE V of this Agreement with regard to Information stored on [or transmitted over] the Network by the withdrawing Participant, or a significant breach of [the SNO’s] duties under ARTICLE VII or ARTICLE VIII with regard to Information stored on [or transmitted over] the Network by the withdrawing Participant (provided that the Participant has allowed a reasonable time for [the SNO] to cure any such significant breach). Any claim of a significant breach by a Party shall be submitted to the Management Committee which will determine, pursuant to Section 10.02 of this Agreement, whether a claimed breach is significant enough to constitute cause under this Agreement. This determination shall be an advisory opinion and shall not be binding on any party to this Agreement and shall not act as a waiver or determination of any Party’s rights under federal, state, or local laws. In a vote to determine whether a breach is significant, the complaining party(ies) and the alleged-breaching party(ies) shall not participate. ...

Whether the SNO should have a mechanism for termination of a Participant for significant breaches of confidentiality could be an item for further discussion among Participants and SNOs. This typically would not be a problem in a model where individual users are not “Participants,” but rather are part of a Participant’s workforce. Thus, the Participant’s own internal policies would be invoked in the event of a breach of patient data by the individual user. The Connecting for Health “Model Contract for Health Information Exchange” includes several model provisions that could allow for a SNO to terminate a Participant’s Registration Agreement, including a model provision allowing for termination for cause.

Indemnification for Breaches of Confidentiality

Indemnification provisions may or may not be included in a SNO agreement. As noted above, the Connecting for Health “Model Contract for Health Information Exchange” provides a variety of model provisions concerning indemnification. A SNO may also choose to adopt special rules governing indemnification for particular situations, such as a breach of confidentiality of protected health information. For example, the SNO’s agreement could provide for mutual indemnification between all Participants for breaches of confidentiality of patient data, with the scope of the indemnification to be determined by the


Section 12.03 Indemnification by Participants. A Participant that breaches the confidentiality of the Information, or submits inaccurate, incomplete, or defamatory data to the Network ("Breaching Participant") agrees to indemnify and hold harmless any other Party against whom any claim or cause of action is brought ("Sued Party") by any individual arising out of or resulting from such breach of confidentiality or submission of inaccurate, incomplete, or defamatory data by the Breaching Participant or any individual for whom such Participant is responsible. Such indemnification shall include the payment of all costs associated with defending such claims or causes of action, whether such claims or causes of action are meritorious, including reasonable attorney fees and any settlement by or judgment against the Sued Party arising out of or resulting from any breach of confidentiality of the Information, or the submission of inaccurate, incomplete, or defamatory data to the Network by the Breaching Participant or any individual for whom such Participant is responsible. In the event a suit is brought against the Sued Party under circumstances where this Section applies, the Breaching Participant, at its sole cost and expense, shall defend the Sued Party in such suit if written notice thereof is promptly given to the Breaching Participant within a period wherein the Breaching Participant is not prejudiced by lack of such notice. If the Breaching Participant is required to indemnify and defend, it will thereafter have control of such litigation, but the Breaching Participant may not settle such litigation without the consent of the Sued Party, which consent shall not be unreasonably withheld. This Section is not, as to third parties, a waiver of any defense or immunity otherwise available to the Sued Party; and the Breaching Participant, in defending any action on behalf of the Sued Party, shall be entitled to assert in any action every defense or immunity that the Sued Party could assert in its own behalf.

SNO Participants might also require that the SNO have an obligation of indemnification in its role as Business Associate and/or as administrator of the network. See relevant sample contract excerpt below:

Section 12.04 Indemnification by [the SNO]. [The SNO] agrees to indemnify and hold harmless any other Party against whom any claim or cause of action is brought ("Sued Party") by any individual arising out of or resulting from any breach of confidentiality of the Information (whether through disclosure or through acts or omissions in the design and/or maintenance of the Network) by [the SNO] or any individual for whom [the SNO] is responsible. Such indemnification shall include the payment of all costs associated with defending such claims or causes of action, whether such claims or causes of action are meritorious, including reasonable attorney fees and any settlement by or judgment against any Sued Party arising out of or resulting from a breach of confidentiality of the Information by [the SNO] or any individual for whom [the SNO] is responsible. In the event a suit is brought against the Sued Party under circumstances where this Section applies, [the SNO], at its sole cost and expense, shall defend the Sued Party in such suit if written notice thereof is promptly given to [the SNO] within a period wherein [the SNO] is not prejudiced by lack of such notice. If [the SNO] is required to indemnify and defend, it will thereafter have control of such litigation, but [the SNO] may not settle such litigation without the consent of the Sued Party, which consent shall not be unreasonably withheld.

Note that this sample provision also includes indemnification for submission of inaccurate, incomplete, or defamatory data to the SNO network. Thus, the Participant who made an error in the data would have to hold harmless another Participant who acted on the erroneous data.
Breaches of Confidential Health Information

Note that these contract samples provide for full indemnification without a cap on liability or language limiting liability to gross negligence or some other threshold of culpability. What the SNO can negotiate, and what the Participants in the SNO’s network feel comfortable with, will dictate the breadth and scope of the indemnification provisions. The broader the indemnification provisions, the stronger the incentive for security compliance.

Some entities, such as governmental entities, may be prohibited by statute from entering into an agreement requiring them to indemnify another party. There also may be entities that are willing to provide patient data for use on the SNO’s network, but do not have any desire or need to access the network themselves. Whether an entity who merely stores data on the SNO network should be required to agree to an indemnification provision is also an issue for the SNO.

The SNO could consider adding a clause requiring Participants to carry certain levels of insurance. See Connecting for Health, “A Model Contract for Health Information Exchange,” Section 15.1 (Insurance).
Acknowledgements
The members of the Connecting for Health Policy Subcommittee have accomplished an extraordinary task in less than a year’s time—the development of an evolving piece of work that can serve as the core of nationwide health information exchange—the policy components of The Common Framework. During this time, we have been fortunate to work with respected experts in the fields of health, information technology, and privacy law, all of whom have contributed their time, energy, and expertise to a daunting enterprise. Our consultants and volunteers have worked long hours in meetings and conference calls to negotiate the intricacies of such issues as privacy, security, authentication, notification, and consent in health information exchange. We offer them our heartfelt thanks for taking on this journey with us, and look forward to the remaining work ahead.

In addition, we would like to offer special thanks to the volunteers and consultants who authored the initial drafts of this body of work—their hard work created a strong foundation upon which to focus the Subcommittee’s deliberations: Stefaan Verhulst, Clay Shirky, Peter Swire, Gerry Hinkley, Allen Briskin, Marcy Wilder, William Braithwaite, and Janlori Goldman.

Finally, we must note that none of this work would have been possible without the leadership and inspiration of our co-chairs, William Braithwaite and Mark Frisse. They have led us with steady hands and determination of spirit.

Connecting for Health Policy Subcommittee

William Braithwaite, MD, eHealth Initiative, (Co-Chair)

Mark Frisse, MD, MBA, MSc, Vanderbilt Center for Better Health, (Co-Chair)

Laura Adams, Rhode Island Quality Institute

Phyllis Borzi, JD, George Washington University Medical Center

Susan Christensen*, JD, Agency for Healthcare Research and Quality, United States Department of Health and Human Services

Art Davidson, MD, MSHP, Denver Public Health

Mary Jo Deering*, PhD, National Cancer Institute/National Institutes of Health, United States Department of Health and Human Services

Jim Dempsey, JD, Center for Democracy and Technology

Hank Fanberg, Christus Health

Linda Fischetti*, RN, MS, Veterans Health Administration

Seth Foldy, MD, City of Milwaukee Health Department

Janlori Goldman, JD, Columbia College of Physicians and Surgeons

Ken Goodman, PhD, University of Miami

John Halamka, MD, CareGroup Healthcare System

Joseph Heyman, MD, American Medical Association

Gerry Hinkley, JD, Davis, Wright, Tremaine LLP

Charles Jaffe, MD, PhD, Intel Corporation

Jim Keese, Eastman Kodak Company

Linda Kloss, RHIA, CAE, American Health Information Management Association

Gil Kuperman, MD, PhD, New York-Presbyterian Hospital

Ned McCulloch, JD, IBM Corporation

Patrick McMahon, Microsoft Corporation

Omid Moghadam, Intel Corporation
Joyce Niland, PhD, City of Hope National Medical Center

Louise Novotny, Communication Workers of America

Michele O’Connor, MPA, RHIA, MPI Services Initiate

Victoria Prescott, JD, Regenstrief Institute for Healthcare

Marc A. Rodwin, JD, PhD, Suffolk University Law School

Kristen B. Rosati, JD, Coppersmith Gordon Schermer Owens & Nelson PLC

Sara Rosenbaum, JD, George Washington University Medical Center

David A. Ross, ScD, Public Health Informatics Institute

Clay Shirky, New York University (Chair, Technical Subcommittee)

Don Simborg, MD, American Medical Informatics Association

Michael Skinner, Santa Barbara Care Data Exchange

Joel Slackman, BlueCross/BlueShield Association

Peter P. Swire, JD, Moritz College of Law, Ohio State University

Paul Tang, MD, Palo Alto Medical Foundation

Micky Tripathi, Massachusetts eHealth Collaborative

Cynthia Wark*, CAPT, United States Public Health Service Commissioned Corps, Centers for Medicare and Medicaid Services, United States Department of Health and Human Services

John C. Wiesendanger, MHS, West Virginia Medical Institute/Quality Insights of Delaware/Quality Insights of Pennsylvania

Marcy Wilder, JD, Hogan & Hartson LLP

Scott Williams, MD, MPH, HealthInsight

Robert B. Williams, MD, MIS, Deloitte

Joy Wilson, National Conference of State Legislatures

Rochelle Woolley, RxHub

Amy Zimmerman-Levitan, MPH, Rhode Island State Department of Health

*Note: Federal employees participate in the Subcommittee but make no endorsement
Connecting Americans To Their Health Care:

A Common Framework for Networked Personal Health Information

THE CONNECTING FOR HEALTH COMMON FRAMEWORK
Dec. 7, 2006

The collaborators of the Connecting for Health Personal Health Technology Council are pleased to release Connecting Americans to Their Health Care: A Common Framework for Networked Personal Health Information.

This document is intended to contribute to an expanding national discussion on the use of information technology to meet the critical needs of consumers, patients and their families.

Many efforts are underway to offer individuals electronic applications to manage their personal health information. This paper explores the possibilities and requirements of networking such applications across the fragmented landscape of health care data and services.

To better manage her family’s health, an individual may wish to download copies of her medication history, check her current deductible, exchange secure e-mail with her doctor, read her hospital discharge summary, update her drug allergy information at a clinic, check her son’s immunization records, etc. For most Americans, such services if offered at all, are typically provided by several different organizations. There is no convenient way for the consumer to tie them together.

This paper describes a networked environment in which individuals could establish secure connections with multiple entities that hold personal health information about them. It begins with a brief discussion of how consumer participation in networked environments has transformed other sectors, such as travel and finance. It contends that in the health care sector both individuals and organizations (existing health care entities as well as new entrants) could benefit from a properly designed network that enables consumer participation.

This report also raises key policy questions, such as how individual users should be authenticated and what are the necessary safeguards for maintaining the confidentiality of personal health information across a network? The development and implementation of commonly accepted solutions to such questions will be critical to the success of any network.

This document marks the beginning of a new round of Collecting for Health multi-stakeholder work groups to develop consensus recommendations to help improve health and quality of life by connecting Americans to their health care.
Connecting Americans to Their Health Care: A Common Framework for Networked Personal Health Information
The document you are reading is part of *The Connecting for Health Common Framework*, which is available in full and in its most current version at: http://www.connectingforhealth.org/. The Common Framework will be revised and expanded over time. As of October 2006, the Common Framework included the following published components:

**The Common Framework: Overview and Principles**

**Policy Guides: How Information is Protected**
- P1 The Architecture for Privacy in a Networked Health Information Environment
- P2 Model Privacy Policies and Procedures for Health Information Exchange
- P3 Notification and Consent When Using a Record Locator Service
- P4 Correctly Matching Patients with Their Records
- P5 Authentication of System Users
- P6 Patients’ Access to Their Own Health Information
- P7 Auditing Access to and Use of a Health Information Exchange
- P8 Breaches of Confidential Health Information
- P9 A Common Framework for Networked Personal Health Information

**Technical Guides: How Information is Exchanged**
- T1 The Common Framework: Technical Issues and Requirements for Implementation
- T2 Health Information Exchange: Architecture Implementation Guide
- T3 Medication History Standards
- T4 Laboratory Results Standards
- T5 Background Issues on Data Quality
- T6 Record Locator Service: Technical Background from the Massachusetts Prototype Community

**Future Technical Guides**

**Future Policy Guides**

**Model Contractual Language**
- M1 Key Topics in a Model Contract for Health Information Exchange
- M2 A Model Contract for Health Information Exchange
Connecting Americans to Their Health Care:
A Common Framework for Networked Personal
Health Information*

Section 1: Introduction

Rapid Consumer Adoption of
Transformative Technologies

The average person’s ability to access data and communicate electronically is proliferating exponentially. Consumer adoption of digitally networked services has transformed the culture of many industries — often in ways unimaginable barely a decade ago.

Consider these examples of rapid consumer adoption of web-based technologies:

- **Communications:** E-mail is now an indispensable tool of communication for hundreds of millions of people worldwide. Instant messaging and Voice over Internet Protocol (VoIP), such as skype.com, are increasingly accepted alternatives to traditional telephones.

- **Search:** The indexing of online information places enormous research power in the hands of individuals. People now “Google” or “MapQuest” without thinking of picking up a phone book or going to a library. Search engines are exposing ever more granular information, such as full-text searches of vast libraries of books, or the estimated value of your home, or the presence of a registered sex offender next door. Collective contributions by customers add value to search engine results, as demonstrated by the niche “layers” that individuals can add to Google maps.

- **E-commerce:** Web sites such as Amazon, eBay, and Craigslist create ever-expanding communities of buyers and sellers, which in turn create ever-expanding content, inventory, and transactions. Opening up online access to previously proprietary networks, such as real estate listings and flight schedules, has precipitated dramatic new conveniences for consumers and efficiencies for industry.

- **Personal finance:** Consumers embrace ATMs, debit cards, personal finance and tax software, and online banking and investment brokerage services. Such online transactions and self-management tools replace mail, phone, and retail encounters with financial institutions.

- **Entertainment:** The explosive popularity of Apple Computer’s iPod represents a progression toward individual manipulation and portability of entertainment media and other data. No longer passive consumers of radio program director decisions, individuals increasingly create and share their own “playlists” and “podcasts.” In another example, fantasy sports create networks of enthusiasts more deeply engaged than mere spectators of events.

- **Content:** Perhaps the most interesting techno-social trend is how newly networked consumers generate whole new bodies of content. Bloggers, who use software that makes it easy to self-publish on the web, are directly challenging political and journalistic institutions, among others. People are now pouring their innermost thoughts and images into the worldwide digital stream through

---

1 Connecting for Health thanks Josh Lemieux, Daren Nicholson, MD, Clay Shirky, and David Lansky, PhD for drafting this paper. See Acknowledgements on page 36.
online communities, such as MySpace.com and YouTube.com. Wikipedia represents a related and equally powerful trend: online collaborative publishing that derives its authority through the self-regulating nature of open communities. MySpace and Wikipedia in particular illustrate a phenomenal expansiveness of online community content creation. By most accounts, both have emerged in about 18 months to join the 20 most popular sites on the web. Wikipedia is now the most frequently visited reference site on the Internet.

Consumer-Based Transformation Is Slower in Health Care

A key ingredient to the successes cited above is a fresh openness toward consumer access to, and contribution of, information. By contrast, the health care industry is moving more slowly toward providing consumers with online access to data and services, as evidenced by a still-modest distribution of electronic personal health records (PHRs) with significant bi-directional capabilities.

PHRs encompass a wide variety of applications that enable people to collect, view, manage, or share copies of their health information or transactions electronically. Although there are many variants, PHRs are based on the fundamental concept of facilitating an individual's access to and creation of personal health information in a usable computer application that the individual (or a designee) controls. We do not envision PHRs as a substitute for the professional and legal obligation for recordkeeping by health care professionals and entities. However, they do portend a beneficial trend toward greater engagement of consumers in their own health and health care. (See Appendix A for a more detailed discussion of PHR platforms, data suppliers, data integrations, business models, and target audiences.)

A Markle Foundation survey indicates low consumer awareness about PHRs; many people simply have not been exposed to or even thought about the technology. When presented with the concept, however, consumers indicate a high level of receptiveness to the types of services a PHR might provide. Sixty percent of Americans favor the creation of secure, online PHR systems that would support their ability to view and refill prescriptions, get lab results over the Internet, check for mistakes in their medical records, and communicate with clinicians via secure e-mail.

Over the past few years, more than 100 PHRs and related technologies have proliferated in the United States and abroad. Despite the increasing availability of these technologies, only a small proportion of the population uses PHRs. Indeed, some observers express concern that PHRs will fail to ever catch on with the general public.

The low penetration of PHRs to date raises the question: Can PHRs be designed to contribute substantially to transforming health care in the way that other innovations have remodeled their sectors? This paper does not attempt a comprehensive analysis of such successful innovations in sectors other than health care, but we observe that they share a few basic traits:

1. They are highly useful. All of the examples cited above provide rapid utility and convenience by taking available digital data, making it digestible, and providing immediate value to consumers.

2. They are easy to use. Web applications that have diffused broadly typically deliver not only high utility, but also a simple user interface that does not limit or burden the consumer.

3. They are free or inexpensive. Whether supported through advertisements or not-for-profit foundations, dramatic-growth applications generally collect small or no fees from consumers.

These observations relate to the applications themselves and their business models. They are each clearly essential and deserve further evaluation. Our focus with this paper, however, is on a fourth characteristic of web-based technologies that have transformed culture in other sectors:

4. They rapidly proliferate due to the power of networks. Consumers connect to various networks via their credit cards, cell phones,
Network-Enabled, Consumer-Led Transformation: A Case Study

For decades, making flight reservations was a time-consuming task. Airline representatives kept passenger reservation data on handwritten index cards.

First big leap

In 1953, a chance meeting between then-president of American Airlines, C. R. Smith, and a sales representative for IBM, R. Blair Smith, led to the first electronic reservations system, called “Sabre.”

Second big leap

The success of Sabre motivated other airlines to create their own reservations systems. For example, United Airlines (UA) in the 1970s created the “Apollo” reservations network, which allowed travel agents to book tickets on UA flights as well as its competitors. United felt that the marketing power it gained from offering the reservations network outweighed the losses it might incur from travel booked on other airlines. In these early years, airlines attempted to gain competitive advantage by providing controlled access to their booking service and by various display and presentation approaches to the available flight options. Ultimately, four reservations networks emerged to serve the U.S. market.

Third big leap

For years only travel agents and airline reservations representatives used the airline reservations networks. However, following the emergence of Internet travel sites, consumers suddenly gained direct access to these systems. Consumers shifted to self-service for online comparative shopping. Two consequences of this consumer-driven change are the drastic contraction of the travel agent industry and the rapid ascendancy of low-price carriers. Today, travel reservation sites increasingly compete with each other based on other services, such as booking restaurants and selling event tickets.

Lesson

By providing consumers with direct access to networked data from multiple competing services, the electronic reservations systems enabled efficiencies and transformed the sector far beyond their original purpose. Similarly, online consumer access to the real estate industry's Multiple Listing Service (MLS) has shifted greater autonomy to homebuyers and sellers, and online banking services have streamlined transactions and services for both consumers and financial institutions.

---


In contrast, today’s PHRs are “un-networked.” They generally require the consumer to enter data manually or get a view of information from a single entity such as one health plan, one pharmacy, or perhaps one health care provider’s electronic health record (EHR). Yet most people have relationships with many different doctors and health care entities; particularly those Americans with multiple chronic conditions — more than 60 million today and estimated to reach 81 million by 2020 — must coordinate their care across several providers and entities. If the PHR is “tethered” to one particular relationship, say with one provider or one pharmacy service, it may not meet the long-term needs of those who need it most. Some people in a stable relationship with one integrated delivery system may today have their information adequately accessible through an application from that institution. However, for most people, over time, PHRs would be much more useful if they were networked to aggregate the consumer’s health information across multiple sources (e.g., the consumer’s insurance eligibility and claims, her records from all of her doctors, her lab results, her pharmacy services, her diagnostic imaging, etc.).

'Networked' PHRs as Tools for Transformation

The mere aggregation of the consumer’s data, however, should not be an end in itself. The true test is whether the network makes it easier for ordinary people to coordinate and engage more actively in their own health and health care. We see a networked environment for PHRs as a foundation for Americans to improve the quality and safety of the care they receive, to communicate better with their doctors, to manage their own health, and to take care of loved ones.

This paper argues that consumers can help accelerate transformative change, particularly in a networked information environment. However, we emphasize that clinicians also have a critical role in realizing the full potential of networked PHRs. Consumers continue to see doctors and other health professionals as the key agents of their care and the most trusted hosts of their personal health information. To take advantage of networked personal health information, both consumers and clinicians must be open to changes in their relationships, responsibilities, and workflows. The network-enabled efficiencies and safety improvements discussed in Section 3 are more likely to occur if consumers and health care professionals act as partners who share access to and responsibility for updating personal health information. The status quo — in which most personal health data are stored in silos controlled by providers, payers, and other entities — makes it more difficult for consumers to gather their data from multiple sources, more difficult to choose freely among providers, and thus more difficult to manage their health.

Designing a policy framework and architecture for networked PHRs does not guarantee that consumers or health professionals will widely adopt the technology. This paper does not attempt to overcome every barrier. Our intent here is to recommend a basic architectural approach for networked PHRs consistent with the goals of improving the consumer’s access to and confidentiality of personal health information.
Addressing Key Policy Concerns Will Be Core to the Transformation Process

Although a networked PHR would provide significant benefits to consumers, the exchange of health data over an electronic network poses serious concerns. Confidentiality of personal health information is a core American value. There is evidence that Americans support a network for health information exchange — if security and confidentiality safeguards are sufficient.

Thus, before encouraging the ubiquitous networking of PHRs to other health information systems, we must establish a common understanding and an adequate set of shared rules. We need a technical approach that allows access controls to keep information flowing among people authorized to see it — and protected from unauthorized access or use. The selection and implementation of technical elements are themselves aids or obstacles to confidentiality and security.

Policy principles derived from shared American values must precede, and in fact determine, the design of the network. Consumer representatives must therefore be equal partners with other stakeholders in policy-making bodies. Consistent with the Connecting for Health Common Framework model (see Section 4), we propose that efforts to network PHRs with other information systems be guided by the following path:

This paper recommends a course toward developing networked PHRs. It covers the first five stages of the above diagram. Its purpose is to begin a discussion of the technical architecture and policies necessary to enable consumers to use personal health technologies to connect to their health data and services.
Section 2: Values and Principles

Although there is great heterogeneity in the American population, as a nation we do embrace certain common values. Two of those values, privacy and autonomy, are deeply rooted in American history and remain relevant to many national discussions today, such as free speech and national security. The reach of these values extends to nearly every aspect of the American experience, particularly in health care.

Based on these core values, the Personal Health Technology Council† has offered a set of consumer- and patient-focused principles for the handling of electronic personal health information. The principles have been endorsed by many consumer groups12 and recommended to the American Health Information Community, an advisory body on health IT issues for the U.S. Department of Health and Human Services.13,14

The principles are:

1. Individuals should be guaranteed access to their own health information.

2. Individuals should be able to access their personally identifiable health information conveniently and affordably.

3. Individuals should know how their personally identifiable health information may be used and who has access to it.

4. Individuals should have control over whether and how their personally identifiable health information is shared.

5. Systems for health information exchange must protect the integrity, security, and confidentiality of an individual’s information.

6. The governance and administration of health information exchange networks should be transparent and publicly accountable.

Many PHRs today may aspire to these basic principles. However, it is not plausible to expect any current PHR offering on its own to fulfill all of the principles so long as the average individual’s personal health information is scattered across multiple, unconnected entities. Furthermore, there are no clear, consensus-based, overarching policies and practices that would guide PHR suppliers toward fulfillment of these objectives.

We conclude that, with the possible exception of individuals receiving all of their care from a single integrated delivery system, only a “networked PHR” has the potential to offer consumers an electronic health information environment that lives up to the principles. To create a trusted network that fulfills these principles, the companies and institutions that hold consumer health data must embrace the values underlying these principles. Fundamentally, personal health data custodians must not attempt to gain or retain market share by forcing consumers into exclusively proprietary mechanisms to access their personal data. Rather, entities should compete to serve consumers with services driven by data that the consumer authorizes them to use. Simply put, consumers should choose PHR applications in a free market.

Connecting for Health argued this same position when it advised the Centers for Medicare & Medicaid Services to set an example for the health care industry by not providing an exclusive portal for beneficiaries to view their claims data, but instead experimenting with beneficiary data downloads into PHR applications that they select.15

If PHRs can be authorized to connect securely to multiple data streams on the network, then the competition among PHRs will be based on service, features, and value to the consumer, not mere custody of the consumer’s data. To illustrate this argument by analogy, the custodianship of personal health data should be more like that of personal cash. Consumers, not banks, own personal cash. People use banks to store and transfer their cash. The banks

† The Personal Health Technology Council is a collaborative body convened by the Markle Foundation and includes representatives who work in government, industry, health care, consumer advocacy organizations, and the professions. See the Acknowledgements for a description of the process we used to develop this paper. For more information about the Council, see http://www.connectingforhealth.org/phti/index.html.
compete based on services that they provide in exchange for those deposits. Of course, this analogy is not perfect. People are much more accustomed to managing cash than personal health information. Furthermore, the information generated by the health care system is vastly less structured, more complex, and more sensitive than financial data. Lastly, financial fraud is a well-understood personal and business risk, with well-established remedies supported by business practices, tax law, FDIC, etc. The improper disclosure of personal health information, on the other hand, can inflict a very different kind of damage, which is hard to prove or fully remedy. This underscores the importance of designing a health information network based on principles that are consistent with American values.

All of the participants within the networked environment — including health care institutions and professionals, insurance companies, labs, pharmacy services, employers, and consumers themselves — must agree to basic principles for providing individuals access to personal health information, and security and confidentiality protections must be “baked in” to the network design.

The overarching principles must be translated into specific policies and authorizations, which may vary depending on the location of a given piece of information at a given point as it flows across a network. For example, imagine two applications: one controlled by a doctor and a networked PHR controlled by a patient. The doctor records a diagnosis, and the patient receives a copy of that diagnosis through the networked PHR system. The patient will now control all access by third parties to the copy of diagnosis data in the patient’s own application. However, just as with paper records, once information has been entered into the physician-maintained medical record, the doctor needs to retain the original data, without alteration. Further, existing regulations under the Health Information Portability and Accountability Act (HIPAA) authorize the doctor to share the data with authorized third parties for purposes of treatment, payment and operations without getting the patient’s explicit permission.

Before exploring these network-design and policy principles and policy questions in greater detail, in the next section we propose how networked PHRs may be helpful in improving our broken health care system.
Section 3: Opportunity Analysis in the Current Health Care Landscape

Entrenched problems in the American health care system are well-documented. Among the oft-cited deficiencies:

• Fragmentation that leads to inefficiency and duplication of efforts and costs.\(^{16,17}\)

• Disappointing levels of safety and quality that lead to high rates of medical errors.\(^{18,19,20}\)

• Frequent unavailability of vital information at point of care.\(^{21}\)

• High costs that are growing at an unsustainable rate.\(^{22,23}\)

• An overall lack of patient-centeredness.\(^{24}\)

Connecting for Health focuses on how health information technology can help transform the industry to reduce these problems and enable new forms of personal health management. We contend that strategic acceleration of the following trends can catalyze the long-awaited transformation:

1. **Widespread use of digital data systems.** If health information remains paper-based, little can be done to leverage data to improve health research, quality, and outcomes.

2. **Adoption of EHRs.** Clinicians need to use EHRs so that the clinical data they generate can be captured for sharing, coordinating care, and quality assessment.

3. **Interoperability of EHRs.** Only a minority of clinicians use EHRs today, and most of these EHR users have implemented proprietary systems that are not interoperable with other systems.

4. **Proliferation of PHRs.** Consumers are a logical point of aggregation for copies of their own health information. PHRs can be essential tools to make the task easier and place individuals at the center of their care.

5. **Distribution of technology to the patient and family.** Other technologies, such as health monitoring devices, can add the home as a key collection point for important personal health data. Such monitoring opens possibilities for more collaborative care and early intervention when monitored values reach certain thresholds.

6. **Reallocation of roles, responsibilities, and money to the patient and family.** PHRs and other new technologies must support a shift from episodic and acute care toward continuous healing relationships between patients and families and the health care professionals who serve them, as envisioned by the Institute of Medicine’s landmark report *Crossing the Quality Chasm*.\(^{25}\) Consumers, aided by new technologies, can assume added responsibility for self-care, personal health management, and care-giving. A shift in financial incentives to reward clinical follow-up, outcomes, and quality is a key part of this trend, since current rewards favor fragmented and episodic care. The goal is to reinforce the benefits of improved collaborative relationships among consumers, their families, and their trusted health professionals.
Networked PHRs Would Help Meet IOM Design Rules

In 2001, the Institute of Medicine (IOM) published the landmark Crossing the Quality Chasm report with six widely cited, broad goals for redesigning health care in the 21st Century. It envisions a health care system that is:

1. **Safe** — By avoiding injuries to patients from the care intended to help them.
2. **Effective** — By providing services based on scientific knowledge to all who could benefit, and refraining from services not likely to benefit (i.e., avoiding underuse and overuse, respectively).
3. **Patient-centered** — By providing care that is respectful of and responsive to individual patient preferences, needs, and values and ensuring that patient values guide all clinical decisions.
4. **Timely** — By reducing waits and sometimes-harmful delays for both those who receive and those who give care.
5. **Efficient** — By avoiding waste, including waste of equipment, supplies, ideas, and energy.
6. **Equitable** — By providing care that does not vary in quality because of personal characteristics such as gender, ethnicity, geographic location, and socioeconomic status.

There is broad consensus that clinician adoption of electronic health records (EHRs) is critical to progress toward these worthy aims. In the same report, the IOM issued ten design rules that are less frequently cited, but more specific about the need for an advanced role for patients and their families (particularly those with asterisks below):

1. Care based on continuous healing relationships.*
2. Customization based on patient needs and values.*
3. The patient as the source of control.*
4. Shared knowledge and the free flow of information.*
5. Evidence-based decision-making.
6. Safety as a system property.
7. The need for transparency.*
8. Anticipation of needs.*
10. Cooperation among clinicians.

Clearly, a strategy that relies on clinicians' adoption of EHRs alone will not achieve all ten of the IOM's design principles. The IOM envisions consumers as full information partners with the health care professionals and institutions that serve them. Thus, a fully formulated strategy for accomplishing these ten goals would also include promotion of networked personal health records (PHRs).

PHRs will be critical to achieving more than half of these design principles (see asterisks above) if they collect, anticipate, and reflect the needs and values of individual health care consumers. PHRs can foster long-term healing relationships between individuals and their health care providers if they are networked to chronicle care longitudinally across multiple points of care. PHRs also have the potential to provide consumers with an unprecedented level of control over their information and health decisions that affect them. Further, PHRs can be vehicles for transparency about treatment options and transactions, ranging from the evidence base for various treatments to the costs of medical services.

In summary, we do not believe that the IOM's worthy aims can be attained without PHRs networked to the plurality of institutions through which consumers receive care.

---

We do not view the above trends as perfectly sequential steps of transformation, each one dependent on one prior. Instead, we view them as concurrent processes that will reinforce each other. In evaluating the highest leverage approach to take over the coming years, we offer a best guess assessment of how far along the United States is likely to be in advancing each of these trends by 2008.

1. **Widespread use of digital data systems by 2008:**
   - Nationwide, more than 90 percent of pharmacy claims transactions will be computerized and increasingly available through national clearinghouses, consistent with the National Council for Prescription Drug Programs’ (NCPDP) coding.
   - As many as half of all laboratory results available electronically will be using Logical Observation Identifiers Names and Codes (LOINC) standards (although it is not as clear how much of the lab information will be available through distributed networks or whether most end-user applications will be ready to receive the data).
   - More than 95 percent of clinical claims will be in electronic format.

2. **Adoption of EHRs by 2008:**
   - Only one-third or fewer hospitals and health care practices will have an EHR installed.

3. **Interoperability of EHRs by 2008:**
   - Most EHR installations will continue to be based on proprietary software that is largely non-interoperable.
   - No more than ten percent of the public will live in communities where health information can be exchanged among interoperable EHRs.
   - Incentives for interoperability will remain very modest.

4. **Proliferation of PHRs by 2008:**
   - Several of the current barriers to PHR adoption (such as concerns about privacy and security, lack of consumer awareness, lack of brand, lack of a sustainable business model) will likely remain in place and limit growth.
   - The continuing stream of news reports about privacy breaches of electronic data in several sectors, including health care, may affect consumer demand for PHRs and even create backlash against EHRs.

5. **Distribution of technology to the patient and family by 2008:**
   - Control over technology and information will remain in the hands of health care organizations.
   - Public reporting efforts and information support for health care transparency and quality will be very modest.
   - Few incentives will be in place to entice consumers to adopt technology and to take a more active role in their care.

6. **Reallocation of roles, responsibilities, and money by 2008:**
   - Higher co-pays and health savings accounts (HSAs) have been promoted in part to shift greater responsibility for health care decision-making to the consumer. Additionally, there are government, payer, and employer initiatives to “pay-for-performance.” However, we predict that these efforts will have little effect on the underlying roles, responsibilities, and financial flows of the health care system as a whole by 2008.

Given the low expectations for EHR penetration and interoperability, health care transformation strategies that rely on EHRs and clinician-based health data sharing networks are not likely to yield substantial near-term impact. We recognize the importance of EHRs and the high value of their integration with PHRs. We support efforts to increase EHR adoption and interoperability. However, we contend that it would be a strategic mistake to wait for full fruition of trends 2 and 3 in order to achieve increased consumer participation through trends 4 and 5.

Rapid consumer adoption of newly networked services has proven to be possible — indeed phenomenal — in other sectors. Consumers can adapt to technology and culture transformation more rapidly than large health
care institutions with long histories of business processes and legacy systems. Furthermore, even as the majority of clinicians continue to keep consumers’ data on paper, other important personal health information — namely claims, pharmacy, diagnostic images, and lab data — are available in digital form today. We conclude that the immediate effort to catalyze health care transformation must include a strategy to create a networked environment for PHRs and related technologies that takes advantage of these currently available digital data streams.

Providers can gradually form and join networks as their systems increasingly interoperate. In fact, networked connections to PHRs could help accelerate the EHR adoption curve as clinicians see advantages to joining the network.

There are additional strong rationales for involving consumers in a much-needed transformation toward greater information access and transparency. First, the health care consumer has the largest stake in the contents of such information. The consumer’s life is put at risk when preventable errors occur due to lack of information. Second, the consumer is the ultimate payer of health care services. Consumers are being asked to pay directly for a larger proportion of their care.26,27 Third, younger generations expect to use technology in almost all aspects of their lives. Fourth, as the number and complexity of diagnostic and treatment modalities grows at a rapid pace, patients are increasingly required to share the responsibility of decision-making with their health care providers. Furthermore, patients are often in the best position to gather and share information with providers.28,29 For example, a physician might know that a medication has been prescribed for a patient. But without asking the patient, the doctor does not know whether the patient actually took the medication, how well it worked, what other remedies she is taking, or whether she had side effects.

Empowering health care consumers by placing information directly in their hands has the potential to radically improve health care.30,31 PHRs are still in the early development stages, and a great deal of study is needed to measure the benefits and risks of PHRs. Consumers, patients, and their families vary widely in the responsibilities they each wish to maintain in their own health. However, as noted in Connecting for Health’s 2004 report, Connecting Americans to Their Health Care, preliminary evidence suggests that PHRs have potential to:

- Empower patients and their families.32,33,34,35,36,37,38,39
- Improve the patient-clinician relationship.40,41,42,43,44
- Increase patient safety.45,46,47,48
- Improve the quality of care.49,50,51,52,53
- Improve efficiency and convenience.54,55,56,57,58,59
- Improve privacy safeguards.60,61
- Save money.62,63,64,65,66,67,68

Lastly, there is general agreement among many stakeholders, including those listed below, that PHRs should be a key part of health care modernization and reform efforts:

- Government bodies, like the National Committee on Vital and Health Statistics69 and the American Health Information Community.70
- Professional societies, such as the American Medical Association71 and the American Health Information Management Association.72
- Consumer groups, such as AARP and the American Diabetes Association.73
- Health insurance plan associations, like America’s Health Insurance Plans and the Blue Cross Blue Shield Association.74
- Bipartisan political leaders.75
Stakeholders do not share a consensus view on how to stimulate PHRs (or even what PHRs should ultimately be). We do not know what kinds of applications and functions will be most effective in encouraging the transformation we seek. The mere presentation of health data to consumers is unlikely to be transformative. Applications likely will have to interpret and apply the data in innovative ways that provide specific benefit to specific people, and connect them with their health team and caregivers. Although the next sections of this paper recommend a framework for enabling networked PHRs, we purposely avoid recommendations on what those applications should be or do. Development of a sufficiently flexible network will enable the use of a great variety of personal health technology applications, including many that we cannot imagine today.
Section 4: Background on the Common Framework Architecture

Connecting for Health has created a structure, called the Common Framework,§ which is specifically designed to strike an appropriate, consensus-based balance between the need to share personal health information electronically and the need to protect it from inappropriate access or use. Although the Common Framework was originally designed to guide personal health information exchange among health care providers, its underlying principles were developed to support consumer access. Below we briefly discuss these principles.

Common Framework Policy Principles

The Common Framework has endorsed a set of fair information practices to guide systems that support the exchange of personal health information. These principles are fully presented in “P1: The Architecture for Privacy in a Networked Health Information Environment.”76 Here we summarize them:

- **Openness and transparency:** Consumers should be able to know what information exists about them, the purpose of its use, who can access and use it, and where it resides. They should also be informed about policies and laws designed to ensure transparency on how privacy is assured.

- **Purpose specification and minimization:** The purposes for which personal data are collected should be specified at the time of collection, and the subsequent use should be limited to those purposes or others that are specified on each occasion of change of purpose.

- **Collection limitation:** Personal health information should only be collected for specified purposes and should be obtained by lawful and fair means. Where possible, consumers should have the knowledge of or provide consent for collection of their personal health information.

- **Use limitation:** Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified.

- **Individual participation and control:** Consumers should be able to control access to their personal information. They should know who is storing what information on them, and how that information is being used. They should also be able to review the way their information is being used or stored.

- **Data quality and integrity:** All personal data collected should be relevant to the purposes for which they are to be used and should be accurate, complete, and current.

- **Security safeguards and controls:** Personal data should be protected by reasonable safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure.

- **Accountability and oversight:** Entities in control of personal health information must be held accountable for implementing these principles.

- **Remedies:** Legal and financial remedies must exist to address any security breaches or privacy violations.

---

Common Framework Technical Principles

The Common Framework also prescribes several technical principles upon which health information exchange networks should be based. We summarize them below:

• **Make it “thin”:** Data exchange networks should impose the minimal requirements for storing and transmitting health data, leaving as much processing as possible to applications at the edges of the network.

• **No requirement of a national health ID:** We argue that a national health identifier is neither likely nor necessary.

• **Avoid “rip and replace”:** The health care industry has already invested heavily in technology. The network should take advantage of the technology currently in use, not require its replacement.

• **Separate applications from the network:** The roles of the network and of applications should be distinct. The purpose of the network is simply to transfer data. All other data-related functions should reside at the application level. This architecture provides for a stable infrastructure upon which application developers may build innovative functions. Because this distinction is critical to our recommendations for networked PHRs, we discuss it further in *Appendix B: How Applications Interact with Networks.*

• **Decentralization:** Data should remain with the originators of that data (e.g., providers, pharmacies, etc.). Consumers already have trusted relationships with these entities.

• **Federation:** A federation of network members based on mutual agreements is necessary given the complexities of a decentralized network.

• **Flexibility:** The network should be designed such that it can scale and adapt over time and allow participation by a wide variety of network members.

• **Security and privacy:** Privacy protection and security should be top priorities that guide the design and development of the network.

• **Accuracy:** There should be a low tolerance for errors with regard to identifying people and their data records. There should also be a means to correct data errors that are discovered.

*Connecting for Health* put these principles into practice in a three-region prototype documented in previous Common Framework technical and policy papers. This paper adds to a compendium of policy resources for interoperable electronic health information exchanges. Those resources consist of:

• An overarching “architecture” for privacy based on nine interdependent principles.
• Model privacy policies and procedures.
• Notification and consent policies.
• Policies for correctly matching patients with their records.
• Policies for authentication of system users.
• Patient information access rights summary based on the Health Information Portability and Accountability Act (HIPAA).
• Policies for audit logs.
• Policies for breaches of confidential health information.  

§ The *Connecting for Health* Common Framework Policy and Technical Resources are available at: [http://www.connectingforhealth.org/commonframework/overview.html](http://www.connectingforhealth.org/commonframework/overview.html).
The Common Framework as an Architecture for Networked PHRs

To date, the Connecting for Health policies have been designed to enable interoperable exchange of patient data among clinicians. It is a substantial challenge to add consumers to the exchange. From the policy standpoint, these principles must be translated into an adequate set of information-sharing policies to which both consumers and institutional data custodians can agree. On the technical side, a network architecture must be developed that is consistent with the above principles, yet scalable and adaptable to the many combinations of relationships that consumers have with various health care entities. These technical and policy challenges must be addressed in tandem.

Definitions in the Connecting for Health Common Framework Architecture

Previously released Common Framework documents described Connecting for Health's vision of a nationwide network for health information exchange. The fundamental design elements of that network architecture would not be changed by granting consumers access to the network. In fact, consumer access has always been a design principle of the work. Below we review some of the key architectural concepts described more fully in prior Common Framework reports.
In summary, the Common Framework architectural vision is a network of networks (one NHIN made up of many SNOs). Each SNO uses an RLS to locate the consumer’s records and an ISB to talk to other SNOs. Institutions that want to share information across the network must be members of a SNO, comply with Common Framework policies, maintain an RLS or equivalent service, and build an ISB.

As noted in Section 3, many important pieces of the consumer's record are already held in digital format. The custodians of this information include:

- Health insurance plans (both private and public).
- Pharmacy services and clearinghouses.
- Nationwide laboratory services.
- Self-insured employers’ data warehouse services.
- Large, integrated delivery networks.
- And, to a lesser extent, some small hospitals and smaller-practice EHRs.

The next section discusses how PHRs could become part of this network, connecting consumers to their own unique slice of data and enabling them to drive health care transformation.
Section 5: How Consumers Could Be Networked Via the Common Framework

Currently available PHRs either rely on existing data silos (i.e., patient portals offering access to non-interoperable health records) or create new silos (i.e., consumer-populated, non-interoperable records). Potential large-scale benefits of PHRs are unlikely to materialize if these applications remain dependent on limited data sources. For PHRs to become more universally useful to consumers, they must provide a convenient and secure means of connecting to personal data and interactive services from multiple sources, and they must provide a convenient and secure means of moving the data out of the PHR as well, in whole or in part.

A number of architectural approaches could permit consumers to deliver information from disparate data sources into a PHR and vice versa. At one end of the spectrum, the PHR could rely entirely on a centralized database of personal health information. A master database at the center of the network would aggregate data from other health information systems before the information becomes accessible in the PHR. Theoretically, the consumer could then have access via one interface to the central data repository, with potentially greater efficiencies than could be provided by queries across a distributed network. The primary problems with this centralized approach are:

1. **Data management**: Copying all personal health data to a single database, and keeping it all up to date, is impractical at population scale given the vast amounts of data that exist across systems.

2. **Data quality**: Sending all data to a central database may magnify data quality problems (although such an effort may also reveal data problems). The centralized repository model would make error checking and data reconciliation difficult compared to a model that keeps personal health information close to the entity that creates it and knows the patient. Organizations closest to the consumer are in the best position to validate, adjudicate, or update the consumer’s data.

3. **Business case**: It is implausible that any one entity can emerge to garner the trust of all health care systems and all consumers in the fragmented U.S. health care environment. A single, central database would raise questions central to trust such as who controls the data, who governs the process, what secondary uses and resale of data will be allowed, etc. A single source of control for the database would risk the shortcomings of monopolies in general: low innovation, poor customer service, and higher prices. It also limits the power of the network to grow organically and incrementally.

4. **Security and privacy**: While breaches are a concern for all information holders, a centralized model poses significant risk to privacy since a single security breach could lead to a catastrophic data leak.

Centralized systems can provide valuable efficiencies and controls, and may be very appropriate at various network nodes, which should have flexibility with regard to data-storage solutions for the information that they each hold. If centralization is the only model by which health information can be shared across disparate entities, however, there is a high risk that many entities will not participate.

The polar opposite of the centralized architecture is an entirely peer-to-peer network. Under this model, a consumer would have to create and manage separate data streams between her PHR and each system that holds her data. The primary problems with the completely decentralized approach are in many ways the mirror image of the problems of absolute centralization:

1. **Data management**: If each consumer is expected to aggregate her data, she will become both her own registrar and her own system administrator. This burden will be too much for the majority of consumers.
2. **Data quality:** Clinical data comes in both highly structured and very unstructured forms. The consumer would be responsible for managing these disparate forms of data — again, a task too challenging for most consumers.

3. **Business case:** Each person would pay for (or choose a sponsorship model for) a PHR, but the system would be highly fragmented and create few economies of scale.

4. **Security and privacy:** The security risk would be multiplied across many servers with varying levels of technical support and policy compliance. However, the breach of any given source of data would be more limited, reducing the potential for catastrophic data disclosures.

The pure point-to-point approach would place too much burden on the consumer to establish electronic transaction relationships with all of her health care services. It also would be cumbersome and pose high risks for each of the consumer’s data sources, given the current lack of standards for clinical information or of a trusted mechanism to authenticate each consumer. Further, providers would be less likely to access and use the consumer’s data if they were confronted with a hodgepodge of information aggregated from a series of unstructured point-to-point transactions.

**How Could Consumers Aggregate Their Data?**

Creation of centralized data repositories should not be an architectural requirement for data sharing, however, data aggregation at the level of the consumer could be very beneficial, for all of the reasons cited in Section 3 of this paper. How, then, can the individual aggregate her health data without relying upon a single repository at the center of the network or learning to manage a completely peer-to-peer model?

Any practical strategy for networking PHRs must avoid the negative consequences of these two extremes while satisfying the consumer- and patient-focused principles discussed in Section 2.

The Common Framework vision of a federated, decentralized network of SNOs was created to meet this core requirement. Under the Common Framework, authorized clinicians are able to query the network (e.g., request an index of the locations of a patient’s records) on the basis of their organization’s membership in a SNO. To establish a chain of trust, the participating SNOs must have common understandings and expectations, such as how to authenticate and authorize clinicians to use the network and how to log their actions.

Consumers also need a chain of trust to interconnect across networks. Yet they represent a greater challenge than clinicians for authentication, authorization, liability, and security. There is no commonly accepted set of practices today to provide credentials to consumers for health information exchange across different systems and data repositories. It is reasonable to expect that consumer applications could become more easily “networked” if such a set of common practices existed — that is, if some type of enforceable arrangement required all participants to operate under a common set of policies and agreements to mitigate risks such as misidentification or identity theft.

In the Connecting for Health model, a network of interconnected SNOs is viewed as the most flexible and practical means to untether applications from data silos, as well as to enforce a common set of rules among participants. To integrate PHRs into the NHIN, we assume that the same model for connecting users — a chain of trust, brokered by an ISB that can talk to other entities in the system — must be available to patients and consumers. This paper considers the functions and requirements of an entity that provides consumers with access to the nationwide network of SNOs.
Consumer Access Services Could Act as Intermediaries

We start with three assumptions about how consumers could gain access to their data in the future. The first is that there will be services acting on the consumers’ behalf as aggregators of personal health information. Other kinds of networked services with many sources of data, from e-mail to online bill paying to airline booking sites, aggregate data on behalf of the user. It may become technically possible for the consumer to access her health data (via a personal computer) directly from the hospitals, labs, and other organizations that hold it. However, even in such a scenario, many services will arise to hold and manage the data on the consumer’s behalf. Issues of backup, remote access, and economies of scale are in fact already driving the creation of these sorts of services. (Some models may offer storage services of all of the consumer’s data; others may emerge simply as gateways for access without actually storing the data. Ideally, consumers would choose which aggregation model best serves them.)

The second assumption is that there will be services that issue identity and authentication credentials to the consumer and pass those credentials or proof of authentication to other organizations in the NHIN, on the consumer’s behalf. Today, we have no generally accepted methods or policies for initially proving the identity of each individual for the issuance of online credentials based on that identification, nor for the initial and repeated authentication of that individual’s identity in an online environment. In a nationwide health information network, those who hold personal health data will need to be confident that the person to whom they transmit data is indeed who she claims to be. Common, reliable policies for initial proofing and repeated verification of identity will be essential functions of these intermediary services. (Although a complex set of issues surround identity, authentication, and authorization, we will group all of these issues under the label “authentication” for the rest of this document.)

Given the high cost of the initial consumer identification and the low cost of the subsequent authentications, economies of scale will drive the creation and growth of these functions. These intermediary services would be contractually obligated to comply with the rules governing participation in the network. Likewise, they would be expected to enforce those rules in the event of any violation by one of their authorized users (and to successfully exclude unauthorized users). By the same logic, the entities that issue identity credentials to individual consumers must have the organizational standing to enforce nationwide policies within their network.

Third, we assume that the aggregation and authentication functions will be combined. While aggregation and authentication could be offered separately, the economic logic driving the creation of the services will also drive their combination. As a result, competing services would act as proxies for many consumers, potentially millions at a time, holding both their authentication tokens and their data. These authentication/aggregation service providers would not necessarily be covered entities under HIPAA. For the rest of this document, we will assume that authentication and aggregation functions will be offered in tandem by entities we will call “Consumer Access Services.” We will also assume that the interaction between Consumer Access Services and other entities in the NHIN will use the service-oriented architecture of the Common Framework, including both SOAP messages and message brokering by Inter-SNO Bridges.
Following the diagram below, such a combined authenticating and aggregating service would perform key NHIN functions including, at a minimum, authenticating individual users, providing an ISB interface to bridge between those users and the rest of the NHIN, and aggregating information into PHRs on those users’ behalf.

A number of entities may be interested in offering these combined services to enable consumer access to the NHIN, including the following examples:

- **Provider organizations** could strengthen their role as primary care providers and care coordinators by accessing all of a patient’s data when authorized and playing the role of interpreter and coach.

- **Health insurance plans and government programs** (e.g., Medicare, Medicaid, VA) could apply their data analytic- and decision support-capabilities to the clinically rich patient data available across the network and compete on their ability to deploy beneficial interventions based on that analytic intelligence.

- **Pharmacy services** (i.e., pharmacy benefit managers, retail pharmacies, clearinghouses) could offer new services to attract consumers.

- **Application vendors** could benefit from a more efficient marketing and distribution environment by offering their products to a range of Consumer Access Service suppliers with large populations of consumers.

- **Affinity and patient advocacy groups** could create their own intermediary services to help members select and use appropriate products, while using aggregate data as a platform for improving health and advocating for shared concerns.

- **Employers** could steer employees toward consumer access services that allow secure access to personal health information and other benefits.

- **Web portals and other non-traditional health care players** could enter the health care space, both leveraging their brand credibility and gaining appropriate access to data that the consumer wants them to have without negotiating separate access agreements with each trading partner.
• **Regional Health Information Organizations (RHIOs)** could offer services to connect consumers.

**Connecting for Health** wishes to enable consumers to aggregate and manage their health care data while protecting them against “silo-ization” (the difficulty or inability to move their personal data easily from one source to another, especially data they may have added to their own records) and against the misuse or loss of personal data. Two key questions will need to be addressed:

1. **What qualifications must a Consumer Access Service possess?**

One broad answer could be: “Only current participants in the health care system would be allowed to offer consumers access to their data.” This restriction would assure that all those offering consumer access are already covered entities under HIPAA. An alternative answer could be: “Any organization that ensures accurate authentication and accountable handling of consumer data would be allowed to act as a Consumer Access Service.” One possible middle ground would be to insist contractually that all Consumer Access Services abide by HIPAA regulations, regardless of their status as a covered entity.

2. **What policies, contracts, and other governing mechanisms should be applied to these services?**

Consumer Access Services must be trusted partners of every other SNO and NHIN participant. These organizational partners must be confident that the entity to which they pass personal health information will handle it properly, and only share it with the intended and authenticated user. What sorts of contracts, standards support, and other mechanisms of governance would constitute a sufficient chain of trust to enable Consumer Access Services to participate fully in the NHIN?

One set of issues involves identification and authorization of the patient, including, but not limited to:

- Minimum standards of original proofing.
- Minimum procedures for authentication.
- “Levels of sensitivity” authentication methods (stronger authentication for more sensitive data) and how those levels are established.
- Bonded access to ensure some sort of penalty for misuse by third parties.
- Co-issuance of credentials across the network.
- Contracts that specify responsibilities and liabilities.

Another set of issues is related to access, including, but not limited to:

- Whether the consumer must be offered a store-and-forward capability (like e-mail).
- Whether the consumer must be offered an encrypted cache (to secure the data on the server).
- Whether the consumer must be asked for consent for secondary uses of the data, and what constitutes “consent.”
- Whether the consumer must have access to an audit trail that tracks every time her data is viewed or used by someone else.
- Whether the consumer must have the right to get a full copy of her data in an appropriate format.

These issues should be resolved by a process that maximizes the value of these intermediary services for the consumer while limiting the risk of misuse of that data by other parties (including the Consumer Access Services themselves.)

Public policy must make it possible for each person to access personal health information regardless of where it was originally acquired and where it is now maintained. In solving a problem like authentication, the NHIN needs to make sure that every American has an opportunity to gain the necessary credentials and take advantage of the information channels that exist, without being subservient to any particular gatekeeper.
Section 6: Charting a Path Toward Fully Networked PHRs

A number of significant projects to deploy PHRs are now underway. With this document, we have offered a vision of how these multiple approaches to the PHR might coexist and even support each other. We began by presenting a set of values and principles that assert the right of the individual to control personal health information and eventually to share that information with a variety of innovative health care services. We then outlined a strategy to put those principles into practice by developing a networked PHR. The first step toward achieving our goal is to develop policies that will enable consumers to participate in health information exchange.

Connecting consumers to a health information exchange network raises a number of policy questions:

- How will individual consumers be authenticated?
- How will authorized users of an individual’s PHR be authenticated and allowed access?
- How does the consumer know she is communicating with who she thinks she is through the network? How does she verify the source and accuracy of data received?
- What consent procedures will be followed before granting consumers access to the network?
- Which secondary uses of the data, if any, are to be sanctioned?
- How will unauthorized uses of data be handled?
- How will personal health applications be certified to access data sources?
- Will standards for patient-sourced data be defined?
- Will patient-entered data (e.g., errors, changes in medication use, etc.) be propagated back to data suppliers?
- How will the consumer’s ability to control the sharing of her data be ensured?
- By what procedures will consumers grant access to other users such as providers and caregivers?
- How will relationships among consumers, Consumer Access Services, and other NHIN participants be formalized?
- What mechanisms will assure accountability?

All of the policy issues above cannot be solved at once. Therefore, we have chosen to focus on a few priority problems in 2006 and 2007. These significant policy issues can be grouped into the following categories:

- **Authentication:** How does a network participant know that a consumer user is really who she says she is? The discussion of this issue should include a thorough exploration of private sector and federal sector roles in determining adequate policy.

- **Consumer Access Service policy requirements:**
  - What are the key principles and characteristics of a Consumer Access Service?
  - What specific capabilities and liabilities must a Consumer Access Service assume to maintain a chain of trust with the participants of other SNOs?

**Connecting for Health** will convene multi-stakeholder Working Groups that will formulate policy recommendations for each of these challenges. We recognize that each stakeholder has its own set of interests. To successfully develop an open market of networked PHRs, each stakeholder must make a commitment to enable portability of personal health data with the consumer in control.

*Organizations should make the data that they hold available — at the consumer’s request — to applications offered by other entities, as long as those entities comply with a Common Framework of rules and practices for information stewardship.*
This approach would allow consumers to access their information through applications of their choosing, as opposed to having access exclusively through the application offered by each entity that captured their data. The networked model opens up possibilities for existing entities and new entrants to compete on innovation, value, and service to consumers. This model holds more promise than proprietary silos, because no one organization holds all of the data valuable to most consumers. We therefore recommend that organizations aim to exploit the power of networks by developing and adopting a Common Framework for networked PHRs.

A networked PHR environment cannot be achieved without collaborative efforts and consensus agreements among all stakeholders. To achieve our national vision of networked PHRs for every American who wants one, we need to agree on the characteristics of the network and the means by which personal health information will be shared and managed. We must create an environment of trust and confidence. Without a Common Framework of policies for information stewardship, even a thousand interesting projects and product offerings are not likely to produce a trustworthy, interoperable PHR.

This paper provides a vision of a plurality of organizations that offer opportunities for consumers to connect to networks of personal health information and services. An individual could connect via a Consumer Access Service offered by a provider group, a RHIO, a retail chain, a payer, an affinity group, a web portal, a bank, etc. We seek a free and fair competitive environment in which all players agree to a minimum set of common rules. The precise path toward this vision is not completely knowable now. However, we envision several steps over the next five years:

1. Collaboration among multiple stakeholders to recommend policies, beginning with the key areas cited above.
2. Development of one or more prototype Consumer Access Services with multiple PHR connections.
3. Broad dissemination of the prototype findings and requirements.
5. Evaluation of potential methods to validate and enforce rules for Consumer Access Services and the applications that connect to them.

As we have witnessed in the short history of the Internet, market demand and the power of networks can combine to make consumers a driving force for change. This paper outlines a framework aimed at allowing a similar phenomenon to happen in the particularly complex and sensitive area of personal health information.
Connecting Americans to Their Health Care: A Common Framework for Networked Personal Health Information


23 OECD [homepage on the Internet]. Paris: OECD; [updated 2004 March 6; cited 2006 June 14]. Health Spending in Most OECD Countries Rises, with the U.S. far Outstripping all Others; [about 4 screens]. Available from: http://www.oecd.org/document/12/0,2340,en_2649_201185_31938380_1_1_1_1,00.html.


38 Neville R, Greene A, McLeod J, Tracy A, Surie J. Mobile Phone Text Messaging can help Young People Manage Asthma. BMJ. 2002 Sep 14;325(7364):600.


46 Potts AL, Barr FE, Gregory DF, Wright L, Patel NR. Computerized Physician Order Entry and Medication Errors in a Pediatric Clinical Care Unit. Pediatrics. 2004 Jan;113(1 Pt 1):59-63.

Von Knoop C, Lovich D, Silverstein MB, Tutty M. Vital


.

.

.

.

.

Available online at: http://www.connectingforhealth.org/commonframework/docs/P1_CFH_Architecture.pdf
.

.
Appendix A: Definitions of PHRs

"Personal health record" (PHR) is a widely used but loosely defined term for a variety of emerging technologies that enable people to manage their health information and health care transactions electronically. The following brief discussion outlines key characteristics of PHRs.

PHRs Are Distinct from EHRs

It is important to distinguish PHRs from electronic health records (EHRs). EHRs are electronic systems used by health care providers to record and manage information about their patients. EHRs are designed to replace the paper “patient chart” that clinicians have a legal and professional obligation to maintain throughout the course of each patient’s care and for many years afterward. In contrast, PHRs are optional tools for consumers, who do not have similar legal and professional obligations for health record-keeping.

Attributes of a PHR

The Connecting for Health Personal Health Working Group described the PHR as an electronic tool that "...enables individuals or their authorized representatives to control personal health information, supports them in managing their health and well-being, and enhances their interactions with health care professionals."¹

Connecting for Health has put forward the following as seven attributes of an ideal PHR:

1. Each person controls his or her own PHR.
2. PHRs contain information from one’s entire lifetime.
3. PHRs contain information from all health care providers.
4. PHRs are accessible from any place at any time.
5. PHRs are private and secure.
6. PHRs are transparent. Individuals can see who entered each piece of data, where it was transferred from, and who has viewed it.
7. PHRs permit easy exchange of information across health care systems.²

The American Health Information Management Association has a similar definition: "The personal health record (PHR) is an electronic, universally available, lifelong resource of health information needed by individuals to make health decisions. Individuals own and manage the information in the PHR, which comes from health care providers and the individual. The PHR is maintained in a secure and private environment, with the individual determining rights of access. The PHR is separate from and does not replace the legal record of any provider."³

As noted in Section 2 of this paper, few if any current PHRs provide an easy means to reach the full ideals of all seven Connecting for Health attributes. Attributes three and seven are particularly difficult to achieve in today’s health information technology environment.

Dimensions of PHRs

There is a heterogeneous group of applications that describe themselves as PHRs. Below we describe a set of six dimensions to classify the many PHRs on the market today. As a visual aid, we illustrate these dimensions as sides of a cube. Each side of the cube has a taxonomy to help understand the diversity of offerings.

© 2006, Markle Foundation
This work was originally published as part of The Connecting for Health: Resources for Implementing Private and Secure Health Information Exchange and is made available subject to the terms of a license (License) which may be viewed in its entirety at: http://www.connectingforhealth.org/license.html. You may make copies of this work; however, by copying or exercising any other rights to the work, you accept and agree to be bound by the terms of the License. All copies of this work must reproduce this copyright information and notice.
Many PHRs are intended to serve the general public. Others are offered to selected populations, such as employees of a certain company or members of a health plan. The size of these population segments ranges from small (e.g., parents of children with hydrocephalus) to very large (e.g., people who have diabetes).

Perhaps the most recognizable characteristic of a PHR system is its relationship to other health information systems. A PHR may be integrated (or sometimes said to be “tethered”) to an EHR. This type of PHR is often called a patient portal, because the PHR provides the patient’s view into an extract of the provider’s EHR. Other PHRs are integrated with non-EHR systems. For instance, a PHR may have a relationship with an insurance company’s claims system, a pharmacy’s information system, or a health-monitoring device. The other type of PHR is called independent or “stand-alone” (i.e., not integrated with another information system, and typically reliant on patient-input data).
The third dimension relates to the source of data that PHRs capture and store. This is closely related to the type of integration with other health information systems that the PHR offers. There are three main types of PHR data: consumer-sourced, professionally sourced, and device-sourced data. Consumer-sourced data are captured, typically via manual entry, from the individual or individual's authorized proxy. Professionally sourced data are from clinicians and other health care entities (e.g., payers, pharmacies, labs, etc.). Device-sourced data are generated via uploads of information from monitoring tools, such as blood glucometers or blood pressure cuffs. Of course, PHRs can implement any combination of these data sources.

PHRs may also be categorized based on the type of platform on which the application runs. Most PHRs are web-based. However, some PHRs may run on the user's PC or a portable device. These portable devices include USB keys, mobile phones, smart cards, and even implantable devices. PHRs may evolve to interoperate across several platforms.
PHRs may also be differentiated by the entity that sponsors the product, and there are a wide variety of such entities. Employers, large and small health care providers, insurance plans, pharmacy services, affinity groups, dot-coms, device makers, and disease management companies are among those sponsoring PHR applications. **Note:** A PHR sponsor often does not directly supply a PHR product to its target population, but rather contracts with a PHR vendor for the service.
Closely related to sponsorship is the final dimension: the business model or value proposition. PHRs’ applications differ according to the value proposition that they promise their vendors and sponsors. PHR vendors generally rely on revenue from some combination of licensing fees, services or transaction fees, advertisements, and subscription fees. PHR sponsors are generally seeking to derive value from one or more of the following:

- **Loyalty and marketing**: For example, a health plan or integrated delivery network may offer the PHR as a means to differentiate its service from competitors and build loyalty and/or dependence among its membership.

- **Process efficiency**: For example, an integrated delivery network may offer a PHR with online appointment scheduling or online prescription refills to reduce the number of telephone calls from patients to its physicians.

- **Messaging**: For example, an employer may offer a PHR to communicate health and health benefits information to its employees, including the availability of disease management programs for people with certain conditions.

- **Behavior and outcomes**: For example, some PHRs may offer functionality to improve adherence to prescription regimens or exercise programs with the goals of improving behavior and outcomes.

An important note about all of these diagrams is that the categories within each dimension are not mutually exclusive. Many existing models are blended. For example, a PHR can have all three types of data sources or have several different business objectives.
More Than Merely a Repository

In its 2004 report, *Connecting Americans to Their Health Care*, Connecting for Health emphasized the importance of integrating services into PHRs beyond the mere storage of health data.

Similarly, the National Committee on Vital and Health Statistics concluded: “The term ‘record’ in ‘personal health record’ may itself be limiting, as it suggests a singular status repository of personal data. The Committee found that a critical success factor for PHRs is the provision of software tools that help consumers and patients participate in the management of their own health conditions. A ‘personal health record system’ provides these additional software tools.”

A Symposium of the American Medical Informatics Association’s College of Medical Informatics reported: “Personal health record systems are more than just static repositories for patient data; they combine data, knowledge, and software tools, which help patients to become more active participants in their own care.”

At this early stage of development, we believe that it is important not to restrict innovation by defining PHRs too narrowly. Different populations of consumers are likely to embrace various types of personal health applications. Thus, health information exchange networks should be designed to support a broad diversity of personal health applications and technologies.

---

Appendix B: How Applications Interact with Networks

How Applications Interact with Networks

As previously discussed, there should be a clear distinction between the role of the network and that of the end-user application. Application vendors and their clients are in a much better position to determine what sorts of data integration, manipulation interactivity, and display are required for different users. The optimal network specifies only the minimum necessary network configuration to permit flexible data access and effective protections of privacy and security. This minimalist approach will allow a great variety of personal health technology applications to connect to the network, including those applications that exist today and others yet to be developed. The diagrams below illustrate the respective roles of the network and applications:

Data Standards, Security, and Privacy

**Policy:** The network defines the minimum security and privacy requirements necessary to participate in the network. The sub-network organizations (SNOs) enforce these requirements among the SNO members. Actual implementation of these policies occurs at the application level.

**Technical:** Similarly, the network establishes which technical data standards are acceptable. Ensuring compliance with these standards is the responsibility of the SNO. The applications, which must be capable of sending and receiving data in a specified format.

Data Routing

The NHIN connects the SNOs, but does not touch the data shared among them. It merely allows them to connect and transport the data. SNOs route the data. Again, the main burden is on applications to supply, receive, interpret, and apply the data for end-users.
Authentication

The NHIN is not involved in the authentication of individuals or the location of their records. In each SNO, a record locator service stores identifying information on individuals and pointers to each person’s records. Applications authenticate users and maintain their authorization levels.

End-User Function

All end-user functions should be addressed at the application level. The network and SNO layers need not provide end-user functions.
Acknowledgements
This paper is a collaborative work of the Personal Health Technology Initiative — a major effort by the Markle Foundation Health Program to advocate for patient empowerment through personal health records (PHRs) and other health information technologies.

The Markle Foundation wishes to thank the following people for drafting this paper: Josh Lemieux, Daren Nicholson, MD, David Lansky, PhD, and Clay Shirky. We also thank the members of the Personal Health Technology Council who reviewed this paper. The Council was established within Connecting for Health to identify and recommend solutions for policy challenges affecting the adoption of PHRs and related technologies with a sharp focus on the needs and concerns of consumers.

Personal Health Technology Council

Lead
David Lansky, PhD, Markle Foundation (Chair)

Staff
Josh Lemieux, Markle Foundation
Daren Nicholson, MD

Members
Tim Andrews, Health Innovation Partners
Wendy Angst, CapMed, A Division of Bio-Imaging Technologies, Inc.
Rodney Armstead, MD, FACP, AmeriChoice, United Health Group
Annette Bar-Cohen, MPH, National Breast Cancer Coalition
Cynthia Baur, PhD, Office of Disease Prevention and Health Promotion, United States Department of Health and Human Services
John Benton, Epic Systems Corporation
Adam Bosworth, Google
Marc Boutin, JD, National Health Council
Patti Brennan, PhD, University of Wisconsin-Madison
Helen Burstin, MD, MPH, Agency for Healthcare Research and Quality, United States Department of Health and Human Services

Rex Cowdry, MD, Maryland Health Care Commission
Mary Jo Deering, PhD, National Cancer Institute, National Institutes of Health, United States Department of Health and Human Services
Richard Dick, PhD, You Take Control
Stephen Downs, Robert Wood Johnson Foundation
John P. Driscoll, Medco Health Solutions, Inc.
Joyce Dubow, AARP Public Policy Institute
Esther Dyson, CNET Networks
Stefanie Fenton, Intuit
Ed Fotsch, MD, Medem, Inc.
Peter Frishauf, Healthcare Marketing & Communications Council, Inc.
Gilles Frydman, Association of Cancer Online Resources, Inc.
Janlori Goldman, Health Privacy Project
Ken Goodman, PhD, University of Miami
Jonathan Hare, Resilient
Jim Karkanias, Microsoft
J.D. Kleinke, Omnimedix Institute
Connecting Americans to Their Health Care: A Common Framework for Networked Personal Health Information

Linda Kloss, RHIA, CAE, American Health Information Management Association

J.P. Little, RxHub, LLC

Kathleen Mahan, SureScripts

Jack Mahoney, MD, Pitney Bowes, Inc.

Phil Marshall MD, MPH, WebMD

Gail McGrath, National Patient Advocate Foundation

Omid Moghadam, Intel Corporation - Digital Health Group

Jonathan Parker, Americans for Health Care, Service Employees International Union

George Peredy, MD, Kaiser Permanente, HealthConnect

Ginger Price*, Department of Veterans Affairs

Alain Rappaport, MD, PhD, Medstory, Inc.

Alison Rein, National Consumers League

Marie Savard, MD, Savard Systems

Albert Shar, PhD, Robert Wood Johnson Foundation

Clay Shirky, New York University Graduate Interactive Telecommunications Program

Michael Simko, RPh, Walgreen Pharmacy Services

Joel Slackman, BlueCross BlueShield Association

Justin Starren, MD, Marshfield Clinic Research Foundation

Paul Tang, MD, Palo Alto Medical Foundation / American Medical Informatics Association

Randy L. Thomas, FHIMSS, IBM Center for Healthcare Management Business Consulting Services

Tony Trenkle*, Centers for Medicare & Medicaid Services

Rochelle Woolley, Woolley & Associates

Anne Woodbury, Fleishman-Hillard Health Solutions Navigator

Matthew Wynia, MD, Institute for Ethics, American Medical Association

*Note: State and Federal employees participate in the Personal Health Technology Council but make no endorsement.
The Common Framework:
Technical Issues and Requirements for Implementation
The Common Framework: Technical Issues and Requirements for Implementation
The document you are reading is part of *The Connecting for Health Common Framework*, which is available in full and in its most current version at: [http://www.connectingforhealth.org/](http://www.connectingforhealth.org/). The Common Framework will be revised and expanded over time. As of October 2006, the Common Framework included the following published components:
The Common Framework: Technical Issues and Requirements for Implementation*

What is this document?
This document is an overview of the technical philosophy and decisions behind Connecting for Health's Common Framework, and to the policy issues related to those technical requirements. It describes, in broad outline, a vision for a nationwide health information network (NHIN) that preserves patient privacy while allowing health information to be accessed by authorized persons; that leverages the existing investments in health care IT that have been made by existing institutions; and which preserves a high degree of both authority and autonomy for the institutions that currently provide care. It is not a technical guide; rather it is a general overview of the issues, accompanied by pointers to the relevant policy and implementation documents.

In particular, this document provides an outline of the technical issues and choices implicit in creating collaborative networks of health care providers. We call these collaborative networks sub-network organizations (SNOs) because they are components of the larger nationwide network. A SNO will adopt and contractually enforce local standards and policies among its members, and adopt standards and policies that will allow it to inter-operate with other SNOs. The NHIN is simply a network of these SNOs; there is no centrally managed database or set of services within the NHIN separate from those provided by the SNOs themselves.

This document is part of The Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange, and is accompanied by several other companion technical and policy guides for health information exchange. These documents are intended for anyone in the health care or technology industries interested in health information exchange, but, taken as a sequence, represent various levels of increasing technical detail and complexity.

This document, “The Common Framework: Technical Issues and Requirements for Implementation,” provides the most basic level of technical overview. The “Health Information Exchange: Architecture Implementation Guide” covers a deeper level of detail, and the XML files and source code used in the technical prototype test, available through http://www.connectingforhealth.org/commonframework/prototypes.html, provide a further level of technical detail. These latter files have been provided only to demonstrate the code that a technical developer created to implement specifications.

Implementation of the technologies described herein assumes that the health care entities engaging in health information exchange have already made significant strides using health information technology (HIT) locally. This requirement does not refer to the complexity or sophistication of the technology, but rather the basic capabilities presumed by the following:

* Connecting for Health thanks Clay Shirky, Chair, Technical Subcommittee, and Adjunct Professor, New York University Graduate Interactive Telecommunications Program, for drafting this paper.

©2006, Markle Foundation
This work was originally published as part of The Connecting for Health: Resources for Implementing Private and Secure Health Information Exchange and is made available subject to the terms of a license (License) which may be viewed in its entirety at: http://www.connectingforhealth.org/license.html. You may make copies of this work; however, by copying or exercising any other rights to the work, you accept and agree to be bound by the terms of the License. All copies of this work must reproduce this copyright information and notice.
• The participating entities can receive and use digital clinical data, e.g., information brought in from remote sources such as laboratories.
• The participating entities are already in compliance with HIPPA and state requirements governing data privacy and security, and are capable of implementing the requirements for providing only authorized access to identified individuals within their enterprise or organization.
• The participating entities are comfortable disambiguating patient identities using probabilistic matching algorithms within their enterprise or organization. (Comfortable solving the "John Smith" problem in large databases, in other words.)
• The participating entities have or are willing to acquire the hardware, software, and technical expertise necessary to support secure information exchange over the Internet, using Web Services standards and Secure Socket Layer (SSL) certificates.
• The participating entities are willing to collaborate on the design and implementation of standards and policies for health information exchange among themselves, establish or identify an existing entity to host the Record Locator Service and put in place a governance model consistent with the policy principles.

Part I: Understanding the NHIN
The Connecting for Health Common Framework describes and defines relationships between three kinds of organizations: individual health care entities, groups of those entities joined together to form a sub-network organization (SNO),¹ and the nationwide health information network (NHIN) as a whole.

**Entity:** An entity refers to functionally independent participants within the health care system, from single doctor practices up to hospital chains and national organizations, whether public or private.² An entity is any organization, institution, or practice; the only parts of the health care system that are not entities are the patients themselves.

**SNO:** A SNO is any group of entities (regionally or non-regionally defined) that agree to communicate clinical data with one another using a single Record Locator Service (RLS), using shared policies and technological standards, and operating together under a single SNO-wide set of policies and contractual agreements. A SNO has two sets of interfaces, one internal, which binds its member entities together, and one external, which is where traffic to and from other SNOs and outside entities come from.

**NHIN:** The NHIN is the sum of all SNOs. It is a network of networks whose participants agree to the Common Framework. The NHIN is not a separately funded entity; it is a framework of cooperation and compliance.³ If the individual SNOs externally facing interfaces work, the NHIN will work. There are no required "top level" services in the NHIN; at the national level, adherence to standards and policies, however defined

---

¹ Another common acronym for this type of organization is RHIO, which stands for Regional Health Care Information Organization. Though a SNO is conceptually similar to a RHIO, we use SNO because there are a number of national or supra-regional institutions such as the VHA, the CDC, health plans, pharmacy chains, and State regulatory agencies that are not defined by regional boundaries and that need to connect with entities in more than one geographic region. Unlike the regional focus of RHIO, a SNO is any group of data-sharing entities that agree to be bound contractually by technical and policy standards, regardless of actual geographic proximity.

² Though we chose the word entity for its obvious parallel to the definition of 'covered entities' under HIPAA, there may be entities in a SNO that are not covered under HIPAA, such as data centers. These entities nevertheless need to comply with the Common Framework, or the entities that employ them need to agree to take on the responsibility of ensuring that compliance.

³ This is sometimes called the 'thin NHIN' model; it assumes a high degree of autonomy and control remains with today’s health care information providers, and that no significant new national technical organization is required to ‘operate’ the NHIN as a whole. Instead, the existence of policies, standards, and connectivity allows the secure sharing of data with authorized persons nationwide without staffing new sites of central management or control.
and affected, are the key elements. All the actual infrastructure of the network is either hosted within the SNOs, or uses the existing internet.

The following diagrams illustrate the relations between entities, the SNO, and the NHIN.

Diagram 1: Inter-communicating entities within a SNO.

A SNO is a collection of clinics, hospitals, labs, and other entities. They can communicate directly with one another, and are all governed and contractually bound by SNO-wide policies. With the exception of Common Framework technical standards and policy requirements, SNOs are free to design the organizational form that best fits their members. For instance, some SNOs will want to offer a number of SNO-hosted technical services such as data validation, while others will want those functions handled by the member entities.

Diagram 2: Two SNOs communicating securely over the Internet.

Every SNO must maintain an interface to other SNOs. This interface is called the Inter-SNO Bridge (ISB.) As the name implies, the ISB is the point of contact between SNOs. While data traffic within a SNO can pass directly between member entities, traffic between entities in different SNOs must pass through an ISB. The ISB exists both to simplify nationwide traffic (so that every entity does not have to know the address of every other entity), and to improve security, by providing a single point of observation for data traffic going to and from the SNO.
Diagram 3: The NHIN is the sum of intercommunicating SNOs.

The NHIN is the sum of all such intercommunicating SNOs, plus those entities required to design, promote and enforce those standards and policies that need to be implemented at a national level. As the nation's health care institutions join together in SNOs, in order to increase the quality of local care while reducing costs associated with incomplete or duplicated data, the NHIN grows as a side effect.

Creation of a SNO

The SNOs are the principal site of implementation of the Common Framework. The size and scope of a SNO is variable; the commonest model for a SNO is likely to be formal incorporation of a group of entities that have already frequent dealings with one another. The principal function of a SNO is to provide a way to share information securely and among authorized users while protecting patient data against accidental or inappropriate disclosure or misuse. The SNO will contractually mandate and ensure compliance with Common Framework standards and policies, and will adopt or enact any additional standards or policies it deems necessary, with the consent of its members.

Levels of SNO Guidelines

There are four conceptual levels at which a given policy or technical standard can be set: national, SNO-wide, per member institution, or no standard.

<table>
<thead>
<tr>
<th></th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>National</td>
<td>Encryption standards for sending data securely</td>
</tr>
<tr>
<td>Per SNO</td>
<td>Acceptable fields for patient ID</td>
</tr>
<tr>
<td>Per Entity</td>
<td>Management of user ID and authentication</td>
</tr>
<tr>
<td>No Standard</td>
<td>Clinical applications and interfaces</td>
</tr>
</tbody>
</table>
In keeping with a desire to make the Common Framework as broadly adoptable as possible, we have tried to specify the minimum necessary, assuming that above some floor, different entities will have the flexibility to do more; and we have tried to specify policies and standards at the appropriate level of adoption and enforcement.

For example, we must have a national standard for encryption of data as it passes between SNOs, both to assure that the data is secure and to provide interoperability. Coordination of acceptable identifiers for patients in the absence of a national identifier, however, cannot be handled nationally, because different states regulate e.g., the use of Social Security Numbers (SSNs) differently. This level of standardization must therefore be done by the SNO. Procedures for handling user identity and authentication must be in place, but we cannot require that they be handled at the level of the SNO, because in many cases, members of a SNO will have existing procedures which they will not be able to replace quickly or easily. In these cases, the policy and technical documents set minimum levels of compliance, but do not require SNO-wide standardization.

Lastly, and most importantly, there are those aspects of the health care system that the Common Framework does not propose to standardize. For example, we do not propose standardizing the 'look and feel' or behavior of clinical applications, because such standardization would stifle innovation and is not necessary for different applications to share data (so long as the data itself is in a standard format). The design and implementation of clinical applications is best served by allowing those applications to be tailored to local needs and requirements -- a well-funded research hospital will have different application requirements than a safety-net clinic with only web browser access to remote data.

Our view has been that where it is not necessary to standardize, it is necessary not to standardize. Though it is tempting to believe that one can upgrade the entire health care system at once, experience has shown that every required standard raises the cost and difficulty of complying, while lowering the overall rate of adoption. In a system as large and diverse as this one, the essential tasks of improving data quality and creating applications better able to take advantage of that data must be approached incrementally. We believe that the best way to catalyze those improvements are to decisively separate the functions of the network for discovering and transporting that data from the applications that request and consume it.

Part II: Applications and Interactions

Modeling Interactions

The relationship between health care entities in the NHIN can be understood by imagining five sample interactions:

1. Transfer of patient’s clinical data between entities in a single SNO
2. Between entities in two different SNOs
3. From an entity in a SNO to an unaffiliated entity
4. From an entity in a SNO to a public health entity or other aggregator
5. Subscription Models for the above 4 Interactions

1) Transfer of Clinical Data Between Two Entities in a Single SNO

Step 1: Asking for Record Locations

A patient, Elizabeth Smith, presents at a clinic complaining of shortness of breath. She has never been seen there before, and after she provides basic demographic data,
the clinic queries the local RLS for her records. Assuming the clinic is a member of the SNO, and has presented the proper credentials for authentication and authorization, the RLS will compare a set of identifiers, for example Ms. Smith's name, DoB, gender, Zip, and SSN, with those records whose locations are listed in the RLS database. Those record locations that have a sufficiently high probability of matching the patient data (as determined by a matching algorithm specifically designed for that purpose) will be returned from the RLS.

The RLS answers all queries from authorized sources within a SNO.

**Step 2: Aggregating the Identified Records**

Once the RLS has matched Ms. Smith's identifying details against record locations it contains in its database and returned information necessary to retrieve those records, its work is done. The next step is to use those locations to aggregate the actual records themselves, by querying the record locations for the actual patient data. Because the site of the aggregation has significant ramifications for the contractual relations within the SNO the site of aggregation of records can vary SNO by SNO. There are several options for aggregating the actual records whose locations have been returned by the RLS. The Connecting for Health prototype tried three; others may be possible.

**Client Aggregation:** One method is to have the original requesting client do the aggregating. In this model, the client receives one or more record locations. (Zero locations returned is a failed search.) The client then decides which of these records it would like to attempt to retrieve, e.g., only records from a particular institution, or only records from labs, or all records. Client-side aggregation was tested in Massachusetts. The advantages of client aggregation are refined control over record requests, and possibly tighter integration with other local electronic data systems. The disadvantage is higher technical requirements at the participating entities in the SNO.

**Central Aggregation Service:** A second method of aggregation is to create a central aggregation service, a server that sits between the entities and the RLS itself. The server takes incoming queries and passes them on to the RLS, and then takes the record locations returned and queries each listed location, handing off only the final, aggregated record to the requesting client. Centralized aggregation was tested in Indiana. The advantages of such a service are that it creates economies of scale for the SNO. The disadvantages are less control of the record by the original requestor, and higher security risk, since the aggregation service will hold, even if only for a moment, considerable clinical data about the patient.

**Aggregation Proxy:** A third possibility is to run a proxy service that can receive record locations and aggregate them, but is not a required service, allowing some clients to use the remote server for aggregation, and others that want to receive the record locations and do the aggregation locally to do so. The proxy aggregation model was tested in California. The advantages of such a system are that it allows aggregation or records to happen either centrally or at the requesting site. The disadvantage is that it potentially more complex, in terms of interaction, than the other two models.

---

4 The application that does the querying could be as simple as a secure web browser, or as complex as an integrated medical record system.

5 The decision about which of the records to request can be done either with human intervention or by an automated process.

6 It is critical, in fact, that any such aggregation service not cache the clinical data it is handling, so that it doesn’t become a significantly attractive hacking target.
In all three aggregation scenarios, some sort of authentication and authorization must be in place between the requestor and the source of the data, whether peer-to-peer (each entity authenticates directly to each other entity) or, more likely, through the operation of a SNO-wide directory service that allows the entities to identify one another. (See the section on Identity, Authentication, and Authorization, below.)

Importantly, under the Common Framework the actual sources of clinical data are not required to respond to any given request for that data. Individual entities are the stewards of the records, and of the patient's expectation of confidentiality. As a result, those entities may add constraints on data access. Examples include added restrictions to a particular set of records at the patient's request, or added restrictions for anyone who does not have admitting privileges at a particular hospital.

**Step 3: Displaying or Otherwise Using the Records**

The third step involves taking the actual clinical records, wherever aggregated, and making them useful, whether by displaying them directly to the clinician, integrating them into an existing electronic health record (EHR) system, feeding them into a decision support tool, or any of a number of other present or future possible uses of the data.

A key aspect of the current model is that it places no constraints on how the records are made useful, other than to require that the consuming applications abide by policy requirements around privacy, security, auditing, etc. The role of the network is to carry useful data from existing sources to authorized requestors; whether that data is then displayed directly in a browser window or becomes part of a complex database transaction is entirely up to the local user. The goal of the Common Framework is to advance the conversation between application designers and users, by making data more accessible and better formatted. The Common Framework is not intended to either replace or interfere with those conversations.

### 2) Transfer of Clinical Data Between Two Entities in Different SNOs

A similar scenario can occur when a clinic in one SNO (A) looks for a patient's records in a second SNO (B) of which the clinic is not a member. The basic three-step transaction is the same, with these differences:

**Step 1: Asking for Record Locations**

1. In addition to the patient's demographic details, the clinic needs some information on which other SNOs to query, whether the name of an institution, an affiliation with a particular network (e.g., the VHA), or a region where she previously received care. There is no national index of patients; the reasons for this are discussed in the ISB section below.9
2. All traffic leaving SNO A goes out through SNO A's ISB -- the clinic does not make remote requests directly.

---

7 Uniform response to intra-SNO requests for records are not required, nor are they forbidden. An individual SNO can, as a matter of policy, mandate such uniform access if it decides to do so. This requirement would override the ability of individual institutions to differ in data access policies.

8 This design pattern is known as the End to End principle ([http://web.mit.edu/Saltzer/www/publications/endtoend/endtoend.pdf](http://web.mit.edu/Saltzer/www/publications/endtoend/endtoend.pdf)).

9 There is nothing to prevent a group of SNOs, for example all SNOs in a given region or state, to develop independently their own inter-SNO index of patients.
3. Once a request is validated by the receiving ISB, that request is forwarded to the RLS in SNO B and handled as are internal requests, except that the response goes back to the ISB of SNO B for return to SNO A.
4. All traffic coming into SNO B from entities that are not members of B comes in through B's ISB. This simplifies contact with the outside world, and provides a single spot for watching remote traffic (which has a lower level of trust than local traffic.)
5. The trust model between SNOs specifically assumes that each SNO's ISB has a valid SSL certificate, and each SNO will accept the other's certificate.
6. The requesting SNO must provide an identifier of the person authorizing the request. (See the policy document, “Authentication of System Users.”) The receiving SNO does not need (and will in most cases be unable to) re-authenticate the original requestor.

**Step 2: Aggregating the Identified Records**

1. The clinic can, optionally, ask either for a set of pointers to the data, or can ask the ISB to act as an aggregator, and return the aggregated record directly. The ISB must support both types of request.
2. Inter-ISB communications are always asynchronous. ISB A passes along the clinic's request for data to ISB B. B responds that it has received the request. When it is time to return data to A, it starts a transaction with A to deposit that data. Each ISB must therefore be able to both initiate outbound requests to other ISBs and to accept other transactions from ISBs.
3. It is up to SNO A to determine how the material is to be transferred from its ISB back to the initial requesting entity. The ISB can require the original requestor to check back periodically; can maintain an open connection via streaming until the data returns from ISB B; can even email or fax the data if those methods are supported.

**Step 3: Displaying or Otherwise Using the Records**

As with records received from within the SNO, the current model is that it places no constraints on how the records are made useful, other than to require that the consuming entity abides by policy requirements around privacy, security, auditing, etc.

**3) Transfer of Data from an Entity in a SNO to an Unaffiliated Entity**

A similar scenario can occur when an entity A, which is not part of any SNO, requests a patient's record held in SNO B. The scenario is critical for the network to grow organically, since the early days of any such network will necessarily cover only a minority of potential participants. The basic three-step transaction is the same as the transfer of data between SNOs, with these differences:

**Step 1: Asking for Record Locations**

The trust model between unaffiliated entities and SNOs assumes that any SNO accepting queries from unaffiliated entities will subject such requests to a high standard of scrutiny, and to higher levels of audit, and will in any case not automatically honor such requests without some form of scrutiny.

**Step 2: Aggregating the Identified Records**

---

10 It is possible to imagine an entity in a SNO requesting data from an outside entity unaffiliated with a SNO, the reverse of this transaction, but such a transaction would be completely ad hoc, as it involves a data-holding entity ungoverned by the Common Framework.
Communication from an ISB to any outside entity is always asynchronous. As a result, any clinic asking for material through an ISB must either have an accessible online receiver for the results, or must have access to a third-party service that offers such a receiving service. The Common Framework is designed to allow for the creation of such third-party services, though in all cases, the sending and receiving parties are responsible for care of the patient's data, and will be liable for any loss occurring through third-party services they hire or subscribe to.

**Step 3: Displaying or Otherwise Using the Records**

As above, the current model is that it places no constraints on how the records are made useful, other than to require that the consuming entity abides by policy requirements around privacy, security, auditing, etc.

4) From an Entity in a SNO to a Public Health Institution or Other Aggregator

The 2004-2005 work on the Common Framework concentrated on clinical data. However, in addition to handling identified clinical records about individual patients, there are many reasons to handle aggregate and partially anonymized records, including satisfying public health reporting requirements, quality reporting, and fraud detection. This scenario is quite different from any transfer of clinical data, and is handled differently in the Connecting for Health model.

Because the Record Locator Service contains no clinical data, aggregate and anonymized requests are not dispatched directly to the RLS, but instead to the individual institutions, which reply with those requests directly. It is currently up to the individual SNO, in negotiation with the entities who are allowed access to aggregate or anonymized data, to determine whether such requests should go through the ISB or should be handled as direct connections between the entities and the aggregators of the data. This allows the partitioning strategy for protection of data to continue to operate even when handling aggregate data, even when such requests are not governed by HIPAA, as with required public health reporting. Our model for direct aggregation from the source is the Shared Pathology Informatics Network (SPIN), and modeling of SPIN-style interactions in the Common Framework is part of the 2006 effort.

5) Subscription Models

Any of the above transactions may be modeled as a subscription to a particular source of data as well, where an authorized user can request that when a piece of remote content is updated, they receive either a notification of the update, or receive the updated data itself. However, this pattern is not yet specified. The Common Framework is based on Web Services, which enormously lowers the required coordination among network participants, both in advance of and during a transaction. As a result of this loose coupling, subscription models of data transfer (e.g., "Notify me when this patient has new lab results.") can be modeled in two ways. The first is 'scheduled pull' -- scheduled requests from the querier to the RLS or data holder, which requests automatically repeat periodically, in intervals between seconds and months depending on the nature of the query. The other is 'triggered push', where the RLS or data holder watches for updates to data, and pushes out any such updates to a list of subscribers or their designated proxies.

The design and implementation of such models is complex and highly dependant on the technical savvy of the member entities of the SNO. A number of variables affect decisions about subscriptions, such as who assumes the costs of maintaining the subscription information (the

querier, in the case of scheduled pull, and the holder of the data, in the case of triggered push.) As a result, like aggregation, the design and implementation of subscription models is currently envisioned as a per-SNO design choice, though with the assumption that observation of the various implementations in 2006 will provide a guide to any nationwide standardization.

**Broad Policy and Technical Requirements**

The Common Framework provides a list of the minimal set of policies and standards that must be adopted by any participating SNO. On the policy and governance side, all incorporated members of a SNO must:

1. Adopt the policies of the Common Framework (See the policy documents contained in *The Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange.*)
2. Agree to any SNO-wide policies in place

In addition, each SNO has three technical services it must offer:

1. A SNO-wide Record Locator Service, to allow authorized entities within the SNO to look for patient data
2. A matching algorithm, to match patient demographics contained in incoming requests with the records stored in the Record Locator Service.
3. An Inter-SNO Bridge (ISB), to allow authorized outside parties to look for and retrieve patient data

The basic rationale behind these governance and technical requirements are discussed below; the detailed policy recommendations are contained in *The Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange,* the detailed technical implementation guides are contained in the “Health Information Exchange: Architecture Implementation Guide”, contained in *The Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange.*

A health care entity can belong to more than one SNO; this would of course entail the additional expense of listing patient demographics and record location information in more than one place, and reconciling contractual requirements where they differ between SNOs. There is no conceptual obstacle to multi-SNO membership, however. There is no minimum or maximum size for a SNO; a single institution can be a SNO so long as it adheres to the principles and standards of the Common Framework. In practice, only very large institutions will do this, as having a single institution as a SNO creates little of the efficiencies or cost-savings that multi-entity SNOs can have.

**Software Requirements: RLS, Matching Algorithm, ISB**

One of the key design principles of the Common Framework is that no particular software application is required; in the same way that email software from different organizations all read the same email data standards, the technical infrastructure of a SNO can be built on any suitably

---

12 Note that patients may in some cases be considered ‘members’ of a SNO, if they access their data from interfaces supported by the SNO. These patients are not covered by Common Framework requirements, as they enjoy a different degree of control over their data than incorporated entities do.
secure hardware and software platform, so long as it produces and consumes common data standards.

The three applications a SNO is required to host are the Record Locator Service, a matching algorithm for matching queries for clinical data with patient records, and an Inter-SNO Bridge, for traffic between the SNO and the outside world.

**RLS**

One of the basic software requirements of a SNO is the operation of a Record Locator Service (RLS.) The institutions with the right to list patient demographics and record locations in the RLS are the members of a SNO, by definition. Thus the RLS is the practical locus of most SNO-wide activity. The details of the RLS are covered in the “Health Information Exchange: Architecture Implementation Guide,” and the relevant policies in *The Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange*, but the basic functions are described here.

*The Common Framework makes the following assumptions about the design of the RLS:*

1. There is one RLS per SNO, which holds the universe of records that can be queried using the RLS service within that SNO. There is no meta-RLS, in keeping with the “No requirement for national services” design.
2. The RLS is designed only for patient-centered queries. Aggregate queries (e.g., "Find all admissions in the last 24 hours presenting with shortness of breath") must be dispatched to the participating institutions, or run against aggregated databases that are collected and kept separately. The lack of clinical data at the RLS keeps the RLS from being a target of loss or theft of clinical data, and allows interactions to be optimized for a single, simple case.
3. The RLS participates in two types of transactions -- the addition, modification, or deletion of listed patient record locations from the entities that hold data on the patient, and requests for information about a particular patient from entities that want those locations.
4. All transactions to and from the RLS are logged and audited.
5. The RLS must have a valid SSL certificate, and may only communicate with requestors who support encrypted web communications (https).
6. The RLS is designed to take a query from authorized users in the form of demographic details or, alternatively, a query in the form of a unique provider ID plus a Medical Record Number, which would enable them to use the RLS to find other records for the patient whose MRN they know.
7. The RLS must support patient data in incoming queries expressed in the HL7 2.4 format

---

13 During the proof-of-concept testing in 2005, interoperating systems used a mix of platforms and tools, including the .Net framework (1.1) running on Windows XP servers and Java application and Web Services servers (Tomcat and Axis) running on Linux.
14 Note that these requirements don’t foreclose optional support of additional data types or interaction patterns. They are simply minimum requirements, so that new entities joining a SNO have an obvious and small set of required standards to support, and so that an entity that wants to belong to more than one SNO is not caught by requirements to support multiple standards.
15 Because identity, authentication, and authorization services are already required by HIPAA, we treat them separately below.
16 Note that there may be records held by institutions within the SNO that exist but are not listed in the RLS, because of some institutional or patient preference for keeping them unlisted. This is an option for entities in the SNO unless SNO-wide policy overrules such a thing, and is not itself overruled by another regulation such as a state-wide requirement.
17 This second format assumes that the querier has some method of obtaining such a record number, either because the patient has provided it or because the querier has used it in the past for the same patient.
8. The RLS may support incoming queries expressed in the HL7 3.0 format described in the “Health Information Exchange: Architecture Implementation Guide.”

9. The RLS must support both synchronous queries, where the data is returned in a single round trip, and asynchronous queries, where the data is delivered in a new session, some time after the original query. The querier may request either synchronous or asynchronous queries; the RLS may also default to asynchronous return of results if it is unable to complete a given query in a timely fashion.

10. The RLS must implement a probabilistic matching algorithm for patient queries so that the chance of incidental disclosure (presenting a false match) is minimized. (See the policy document “Correctly Matching Patients with Their Records.”)

11. In responding to such queries, the RLS will return zero or more matching demographic records, each including a locator (usually an Institution code and a Medical Records Number) to a set of clinical data for that patient. The locator contents are used for subsequent queries for clinical data.

12. The RLS will return only records which meet or exceed a minimum probability level. (See the policy document “Correctly Matching Patients with Their Records.”)

13. The RLS will not provide a “Break the Glass” procedure in which a physician or other inquirer can request an emergency exception to allow examination of records below the minimum probability level. Besides having a high probability of incidental disclosures and false positive matching, there is no logical additional method that the inquirer can use to positively identify the correct record. If a user has certainty that a record related to a specific patient exists at a particular entity, that user should work directly with that entity to attempt to locate the record.

14. The RLS will return "as matched" data for any data transformations it performed in matching the data (e.g., noting that it matched a name provided as Elizabeth with a patient whose first name is listed as Liz.)

15. The RLS should not return demographic data in fields not submitted by the querier. The RLS may well have demographic details about a patient that a clinician has not submitted; these details should not be displayed, to avoid incidental disclosure, and the risk of authorized users fishing for data.

16. The SNO must maintain a logical separation of clinical from demographic (identifying) data. The RLS itself will not hold clinical data or metadata; all of that is controlled by the entities that created the data, or who hold copies because they provide the patient with care.

17. The design of the RLS assumes that the clinical data itself may be served from cached or other copied versions of the "live" clinical data, and it is acceptable to centralize the physical storage of this data, in order to control costs and guarantee service levels. However, wherever it is located, the data itself should remain in the control of the providing institution, which should be deferred to as the final source of truth on issues of data accuracy and cleanliness.

18. At the time or shortly after records are published to the RLS from entities, the RLS must report obvious errors back to the publishing entity. Such errors include but are not limited to non-numeric characters or incorrect number of digits in numeric data such as SSN, day, month and year designations in Date of Birth; dates that are out of range (e.g., February 31); etc. The requestor is not required by the Common Framework to act on these reports, but the RLS must make them available, and the individual SNO may have a policy requiring particular responses to such errors.

19. At the time of publishing records to the RLS from an entity, the RLS may report possible errors, including but not limited to name and gender fields with a high probability of inconsistency (e.g., Sylvia, M), pairs of records above the matching threshold with
different dates of birth; patient records above the matching threshold with different local record numbers, etc. The publishing entity is not required by the Common Framework to act on these reports, but the RLS must make them available, and the individual SNO may have a policy requiring particular responses to such errors.

20. The RLS must be able to provide an audit log indicating all entities that have published records on behalf of an individual patient and all users that have received record locations in response to requests regarding an individual patient.

Adoption of a Matching Algorithm

The RLS stands between authorized queriers (either entities within a SNO, including possible aggregation services, or the ISB) and a database of patient demographics and record locations. The RLS’s job is to take the incoming queries, format the contents of the message, and make a query to a matching algorithm that determines which records in the database are likely matches. Those records, and only those records, are returned by the matching algorithm to the RLS. The policies governing the matching algorithm are covered in “Correctly Matching Patients with Their Records.”

There is not any standard matching algorithm that can be adopted nationwide, because the work on matching is highly sensitive to local regulations, as with regions that forbid the use of Social Security Numbers (SSNs) for matching and to the relative “cleanliness” of the underlying data. The more accurate the collection and storage practices are, the more likely that highly accurate matching will occur with fewer fields. (See “Background Issues on Data Quality” in The Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange for a discussion of this issue.)

Such algorithms are also highly sensitive to local characteristics of the data set being queried. A last name of Smith is a better predictor of uniqueness in Wewoka, OK than Waltham, MA; NYSIIS-transformed\(^{19}\) names are better matches for Anglo-Saxon names than French names; and so on. The adoption of a matching algorithm that satisfies the conditions below is a nationwide requirement; the nature and tuning of the particular algorithm must be left to the SNO itself.

*The Common Framework makes the following assumptions about the matching algorithm:*

1. The algorithm itself is not specified; each SNO is free to use and tune any algorithm that meets the below criteria. Two of our prototype sites have made their matching algorithms available as part of this release, Indianapolis and Mendocino County. Boston uses a commercially available product, as do many existing health care systems.
2. Authorized queriers present a set of demographic details, and receive in return zero or more matching record locations. Only records meeting a minimum level of probability should be returned. That minimum level is calculated at each RLS such that the probability of returning a false positive match is very low (e.g., one chance in 100,000). Matches approaching but not reaching that level (sometimes called “fuzzy matches”) should not be returned to avoid incidental disclosures. Further, the querier should not be told which data elements do not match since that could encourage fishing. It is legitimate to suggest that the querier provide additional data fields if these were not provided in the initial query. The details of how those matches are calculated must be hidden from the querier by the RLS, to preserve the ability of SNOs to use different and selectively tuned matching algorithms while maintaining standard interfaces.
3. Should the algorithm use transformations of the presented demographic data (e.g., treating Maggie and Margaret or off-by-one errors in numerical data as approximate

\(^{19}\) New York State Identification and Intelligence System (http://www.nist.gov/dads/HTML/nysiis.html).
matches) then the data returned should indicate both the fact of the match and the fact that a transformation was used in the match. The details of the display are up to the receiving application, but the information is provided to allow the requester, possibly in conversation with the patient, to add a check step against false positives, which are possible even with a high probability match.

4. Because delivering too little information is far less dangerous than delivering the wrong information, the algorithm must be tuned to minimize false matches, even at the expense of increasing the number of failed matches (false negatives). The algorithm must meet the policy requirements for accuracy, currently described in “Correctly Matching Patients with Their Records.”

5. A national health identification number is not required. Demographic matching can work at population scale, without triggering either the enormous expense or political risk of failure that will attend any work on unique patient IDs. Should such an identifier exist, however, its use would still require the mechanics for matching and record location created by the RLS. Social security number, although far from perfect as an identifier, and other types of identifying numbers, can increase the probability of achieving a correct match.

6. Individual SNOs may allow or require local IDs to be used as identifiers for the RLS (e.g., a SNO in a region with a primary employer may add employer IDs to the criteria to be matched.)

7. If there are records in the RLS that are below the matching threshold, the querier may not be presented a list to choose from, as this would create the very incidental disclosure the algorithm must be designed to avoid. (This restriction also forbids “wild card” searching, disallowing a search for e.g., all patients with the last name Smith.) Instead, the querier may be offered the ability to provide additional demographic details.

8. The RLS cannot assure that all records that exist for a given patient will be located, even in principal, because the patient may have received care outside the SNO, and because even within the SNO, there may be records that refer to the patient but are beneath the matching threshold, or that are being kept confidential for reasons of patient preference or legal constraints from the State or local policies set by the SNO or participating entities. The SNO may, at its discretion, require that displays of results returned from the RLS contain a reminder that the data may only be partial.

ISB

The other application a SNO is required to host is the Inter-SNO Bridge (ISB.) The ISB is the interface to data held by a SNO but used by institutions outside the SNO. It serves as a single point of access for all remote queries to entities inside any given SNO. The technical details of the ISB are in the “Health Information Exchange: Architecture Implementation Guide.” The relevant policies are contained in The Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange.

The Common Framework makes the following assumptions about the design of the ISB:

1. There is one ISB per SNO, which handles all per-patient clinical requests coming from or going to that SNO.
2. The ISB is only for patient-centered queries. Aggregate queries (e.g., “Find all admissions in the last 24 hours presenting with shortness of breath”) should be dispatched to the participating institutions, or run against aggregated databases that are collected and kept offline. The lack of centralized clinical data keeps the ISB from being a target of loss or

theft of clinical data, and allows interactions to be optimized for a single, simple case.

3. All transactions to and from the ISB are logged and audited.

4. The ISB must have a valid SSL certificate, and may only communicate with requestors who support encrypted web communications (https).

5. The ISB, like the RLS, is designed to take a query from authorized users in the form of demographic details or, alternatively, a query in the form of a unique provider ID plus a Medical Record Number.

6. The ISB must support patient data in incoming queries expressed in the HL7 2.4 format described in the “Health Information Exchange: Architecture Implementation Guide.” The ISB may support incoming queries expressed in the HL7 3.0 format described in the “Health Information Exchange: Architecture Implementation Guide.”

7. The ISB must support two possible patterns of request. The 'one pass' pattern has the requestor presenting patient details and receiving back the aggregated records. In this case, the ISB has acted as the aggregator, as described in Step 2 of the section Modeling Interactions, above.

8. The other pattern that must be supported is a 'two pass' interaction, in which the ISB acts like a standard RLS, returning locators to the remote querier, who then replies with a list of records they would like access to.

9. The ISB must support asynchronous delivery of records, where the requestor, whether a remote ISB or other entity, sends a request in, and then makes available a server for later delivery of the results of the request. "Later" may only be measured in seconds, but the asynchronous pattern is important because there is no guarantee that the ISB can dispatch and resolve all the required transactions local to the SNO quickly enough to support a synchronous return.

Part III: External Dependencies and Open Issues

Security: Identity, Authentication, and Authorization

Trust is the essential glue enabling transfer of medical records, and distrust is a key defense against their misuse. All the hardware and software in the world will not provide adequate defenses against users who are allowed to have copies of records from your institution, if those users fail to protect the records properly, or if they actively misuse those records. It is thus critical to provide the holder of any given set of records enough information to enable them to answer the question "Do I trust the person making this request, and the institution they work for?"

In a large network, it will be impossible for every possible pair of sender and receiver of a request to know one another in advance. Particularly for remote queries, some sort of transitive trust will be necessary -- "If I trust Institution A, I trust Institution A’s employees." To make such a judgment, the requestor must be able to identify Institution A. In addition, the recipient of the request may need to review one or more queries, after the fact; it is essential, in this case, that the recipient be able to communicate quickly and effectively with the sender of the request. Being able to provide the time, date, entity identifier and person identifier will make such reviews considerably simpler, quicker and cheaper than merely having a transaction ID and requiring the counterparty to look it up in order to discover those identifiers on their own.

The federal HIPAA Privacy and Security Rules and applicable state laws provide the baseline for the Connecting for Health Common Framework, although in some cases greater privacy protections and individual rights are recommended by the CFH Policy Subcommittee. In no instance does the Common Framework permit less protection of personal health information than those required by federal or state law; however, participation in an SNO is not a surrogate for determining whether a Participant is a HIPAA Covered Entity or is in compliance with the HIPAA
regulations. Importantly, the Common Framework permits SNO Participants to establish and follow their own more protective data management, privacy and security policies and procedures. In addition, some customization may be necessary at the SNO and Participant level to ensure consistency and compliance with applicable state laws. In addition to HIPAA, Connecting for Health recommends (but does not require) use of the use of the Common Criteria (ISO 15408) to analyze the security procedures of the SNO and of each participating entity.

In addition to HIPAA requirements, the transitive trust model requires reliable reporting of identity between parties participating in a record exchange, which in turn requires the issuing of identifiers for employees, and the maintenance of an authentication and authorization systems. Identifiers, authentication, and authorization are all required by HIPAA; what the Common Framework specifies are the reporting requirements necessary for transitive trust, plus the additional policies related to the transitive trust model, as laid out in “Authentication of System Users” in The Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange.

These reporting requirements have three levels:

1. Reporting of SNO identity for inter-SNO communications
2. Reporting of entity identity (the HIPAA-mandated identity)
3. Reporting of the identity of the individual who authorized the query.21

**Reporting of SNO Identity:** As noted above, the Common Framework assumes a ‘thin NHIN’; the NHIN is a network of networks, with no NHIN-wide services required other than basic connectivity. Both the data and the contextual functions required for inter-SNO transfers of data rely on capabilities provided by the aggregate group of SNOs. There are no “top-level” service providers required.22 In particular, we do not envision a single top-level identity service. Instead, individual health care entities will use the identifiers mandated under HIPAA, and the SNOs are required to provide an invariant name, expressed as a URI,23 that is unique within the NHIN.24 In practice, the URI will also be the URL of the SNO, thus using the Domain Name System as the basic guarantor of uniqueness.

**Reporting of Entity Identity:** In the case of inter-SNO communications, it is not enough to know which SNO has dispatched a message; the source entity (e.g., clinic, hospital, lab) must also be identified. In practice, this identifier will be the HIPAA-mandated National Provider Identifier (NPI),25 plus a human-readable name of the institution.

**Reporting of Individual Identity:** In the case of inter-SNO communications, it is not enough to know which SNO and entity has dispatched a message; the requesting

---

21 In the case of automatic queries, the individual identity should be that of the person most directly responsible for dispatching the query, e.g., the clerk who oversees the system doing the querying. This is because the goal of the identity reporting is to aid subsequent audits.
22 We do envision the possibility of third party providers offering network access to their services, but these services exist at the same conceptual layer as the SNOs themselves.
23 Uniform Resource Identifier, which is effectively a location-insensitive version of a URL. For more on URIs and URLs, see http://www.w3.org/TR/uri-clarification/.
24 Though guaranteed uniqueness presents interesting theoretical problems in large systems, it does not in small systems. Therefore, while we hope that someday the NHIN has enough participants to merit inclusion of one or more health care-specific schemes for mandated uniqueness, along the lines of the Internet's Domain Name System (DNS), we do not envision a system that large for 3 years at the earliest.
25 Because the NPI suffers from the same drawbacks as the SSN -- it is a public identifier with no accompanying authentication method -- the presentation of a HIPAA number must never be regarded as authenticating the requesting institution.
individual must also be identified. There is no person equivalent of the NPI under HIPAA; therefore some form of username or employee ID unique within the domain of a particular NPI must be reported, along with the human-readable name of the person making the request.

One possibility we explored but did not require was the additional reporting of the role of the requesting individual, e.g., clerk, admitting physician, etc. The reporting of such roles would be valuable in cases where the institution receiving the request wanted to limit responses to quereners with certain roles. However, the reporting of roles today is not universally adopted, and where it is in use, the definitions of the roles themselves are variable between institutions. If role-based access becomes important to the operation of the NHIN, considerable work will need to be done to standardize the expression of such roles.

As noted above, the reporting of these three identifiers -- SNO, entity, person -- serves two separate functions. The first is to allow judgment about whether to honor a given request for records, based on past expectations. The second is to simplify future audits should a particular transaction or set of transactions come under suspicion.

Based on the transmission of these identifiers, there are four conceptual levels of record exchange:

1. Within a single entity
2. Between entities in a SNO
3. Between entities in different SNOs
4. Requests from an entity not affiliated with a SNO

**Within an Entity:** Because this takes place beneath the level of SNO-wide traffic, these transactions are governed by the entity alone, and raise no SNO-wide identity reporting requirements.

**Between Entities in a SNO:** These transactions are governed by SNO-wide policies, but in all cases, the entity making a request, either to the RLS or to other entities, must report its NPI and the username and name of the person making the request. Because both sender and receiver are part of the same SNO, we presume that most of these requests will be routine, and will be subjected to a routine level of scrutiny.

**Between Entities in Different SNOs:** These transactions are not governed by any mutual contractual obligations, as entities in a single SNO are. Instead, they are governed by HIPAA and other national regulations and by the adoption of the Common Framework by each SNO. In all cases, the entity making the request must report the SNO of which it is a member, its NPI, and the username and name of the person making the request. Because sender and receiver of a query are not part of the same SNO, we assume these queries will be relatively rare (in comparison to the volume of local traffic), and should be subjected to a higher level of scrutiny.

**Requests from an entity not affiliated with a SNO:** The entity making a request to the SNO must report its NPI and the username and name of the person making the request. Because the sender is not part of the any SNO, we presume that most of all requests will be regarded as unusual, and will be subjected to the highest level of scrutiny.

---

26 It is possible to imagine an entity in a SNO making an outbound request to an unaffiliated entity, but as the recipient would not have implemented the Common Framework, the question of standards and policies for such a transaction would be ad hoc.
Preventive Security: Encryption and Certificate Exchange

Preventive security encompasses defenses against outside attack, insider misuse of data, accidental loss or deletion, and so on. Outside the issues particular to identity, authentication and authorization, preventive security involves defending against access to data by unauthorized parties, misuse of data by authorized parties, unauthorized alteration of data, and accidental disclosure or deletion of data.

As noted above, the principal governing requirement for security is HIPAA, which describes administrative, physical, and technical safeguards required for securing data. In addition to HIPAA requirements and the policy requirements of Identity, Authentication, and Authorization, the Common Framework makes the following two specific security requirements:

- **SSL/TLS Encryption:** All traffic within and between SNOs will be encrypted using Secure Socket Layers 3.0 (SSL) or Transport Layer Security v 1.0 (TLS)
- **Exchange of SNO Certificates Between Pairs of SNOs:** Each ISB must have an SSL certificate, and any two ISBs planning to exchange data must each have the other's certificate. (This is implicit in the required asynchronous data exchange pattern between ISBs.)

Note that making each new SNO exchange credentials with all current SNOs will become problematic as the NHIN grows large. We believe, however, that exchange of certificates between pairs of SNOs is the proper model for the NHIN in its early years, for two reasons: first, the number of SNOs (and therefore of ISBs needing certificates) will be small. Second, the trust of the participants in the system is a critical predictor of its success -- a system that is technically feasible but unpalatable to real-world institutions will simply fail.

Taken together, we believe that requiring that each new entrant announce itself to the existing members, and requiring some formal per-pair handshake, will not be technically onerous for a network containing even a hundred separate SNOs (something that would occur in 2008 at the earliest), and would be beneficial in terms of assuring participants that the network contained no unknown actors. It will also provide a better environment for actually watching trust develop, thus providing experience valuable to the design of any later-stage certificate brokering system.

Two proposed but not currently adopted questions around encryption merit further examination: the encryption of data as stored on a disk, and the special issues involved in handling SSNs.

With regards to encryption, there is considerable work being done on on-disk encryption, where the contents of every file are stored in an encrypted format, and are only able to be decrypted when running in a trusted environment (e.g., with proper user authentication.) This means that should hardware containing information on patients be physically stolen (as happened frequently in recent years), the material contained would not be available to the holders of the physical disk without their also having access to the password or any other required forms of identification. Though such systems are not so widely adopted today that we

---

27 The Internet's Domain Name System (DNS), which we have studied as an example of a distributed system, grew out of the failure of such addressing schemes as the number of Internet nodes approached 1,000.

28 Another reason for caution in this domain is that while generic federated identity systems have been under development for much of the last decade, no such systems have achieved widespread use, and most current multi-party identity systems are industry- or institution-specific. Because of the unique responsibilities of health care providers as stewards of data whose misuse can be both catastrophic and irremediable for the patient, we have generally erred on the side of accepting less efficiency in return for more safety.
feel comfortable mandating their use as part of the Common Framework, the increasing threat of identity theft, coupled with the increasingly large aggregated data sets being generated by the health care industry, means that continued attention needs to be paid to the possibility of including such a requirement.

The use of SSNs also creates a special set of problems. A patient's SSN can be a valuable tool in improving match accuracy, and is in use in many medical record systems. However, the SSN is also a weak and poorly designed authentication token, and a key input to identity theft and other forms of personal intrusion. As a result there are good reasons to both use and not use SSN, and while there are health information networks in operation today which require its use, there are others that forbid it.

It is clear that the rise in identity theft is going to lead to some regulation of the use of SSNs, whether industry-by-industry, state-by-state, or on a national level. As a result, any SNO implementing an RLS must take special care in deciding whether to use SSN as a match field, and, if so, must take special care in protecting the SSN, never returning the SSN when a match is made, even if an SSN was submitted for a patient, so as to prevent fishing. Though use of the last 4 digits of the SSN is on the rise, this is simply re-creating the original difficulty. An attacker who has the last 4 digits of a full SSN, but only needs to report those 4 digits to gain access to material, has the same advantage as an attacker who has the full SSN when the full SSN is required.29

Reactive Security: Auditing and Logging

In addition to preventive security, procedures need to be in place for detection of security breaches and other misuse of data. While detection is an important part of securing any system, it is especially vital in the health care system. Health is not money, and health care is not banking -- where many industries can tolerate a relatively high degree of inconvenience in their user transactions, health care cannot. Waiting a couple of days to get a new ATM card is an inconvenience; waiting a couple of hours to get data on a patient's allergies can be fatal.

Because of this, there is a presumption towards disclosure in cases where a physician reports a critical need for the data, a presumption reflected in, for example, Break the Glass modes of access. In addition to preventive measures against accidental or intentional misuse of data, maintaining a good log of the use of the system, and periodically auditing that log to look for negative events or patterns is critical.

While preventative security requires a high degree of standardization, so that everyone can, for example, use the same encryption scheme, reactive security requires less standardization. Instead, the ability to detect and react to events after the fact requires policies that set a minimum level of technical requirements, which requirements can be met in ways most compatible with the rest of a particular SNO's technological choices.

For the first phase of this work, we have specified two sets of policies regarding reactive security:

1. Logging and Auditing
2. Managing breaches

29 We also examined the use of one-way hashes as ways of allowing the RLS to use SSN-like accuracy in matching records, without ever holding any patient's actual SSN. While the work on this method is impressive, the implementation overhead is large both in terms of original cost and in negative effect on speed of individual queries. Like mandated on-disk encryption, we believe this is an area that merits further study.
Logging and Auditing: It is essential that information about all relevant transactions that touch clinical data be logged, so that the system can be periodically audited, and so that, should there be misuse of data, the events leading up to that misuse can be examined, and it is essential that these logs be immutable, so that once written, they cannot be edited or deleted (in order to prevent sophisticated attackers from removing traces of their work.) The other essential constraint is that such logs not contain the full record being transmitted, so that the logs themselves do not become an alternate target for attackers looking for clinical information. The Common Framework policies regarding logging and auditing are contained in Connecting for Health, “Auditing Access to and Use of a Health Information Exchange.”

Managing Breaches: In addition to preventing breaches of identifying or clinical data where possible, every SNO needs a set of policies for reacting to such breaches where they occur, and these policies will necessarily differ between cases such as accidental disclosure, suffering from a successful external attack, or having an authorized employee misuse data. The Common Framework policies regarding breaches of information are contained in “Breaches of Confidential Health Information” in The Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange.

External Standards

Though the Connecting for Health prototype is obviously standards-based, rather than assuming homogeneity of underlying technology, we are principally a consumer of standards rather than a producer of them. Much of the prototype work was an attempt to avoid setting standards where possible, either by designing a system tolerant of multiple standards (as with the separation of clinical message contents from their delivery envelope) or by taking advantage of existing standards.

Many of the technical issues requiring standardization were solved by adopting Web Services standards; there are two cases where that has not been sufficient:30

1. Coordinating asynchronous communication between SNOs
2. Making assertions about the individuals responsible for a request

In the case of coordinating asynchronous communications, the obvious standard to use is WS-Addressing.31 In the case of assertions about the identity of requesting individuals, the obvious standard to use is SAML 2.0.32 In both cases, the standard as proposed has not been widely adopted, nor has it been implemented in many key Web Services platforms. WS-Addressing is also not yet an official standard, despite two years of work.

Our solution in both cases has been to narrowly and provisionally adopt those parts of the two standards most compatible with our goals, but to make it clear in the documentation and in the headers of the messages that these are provisional standards and may change.

Beyond the issues having to do with Web Services generally, there are two additional sources of standards that any working system will require. The first, of course, is clinical standards. Though the model we have designed for requesting and receiving data is insensitive to what data is being carried -- lab results, medication lists, radiology reports, etc. -- the system as a whole requires good clinical standards, in order to be able to support increasing automation of record

---

30 There may be only two such cases because we have intentionally restricted our work to a well-defined set of problems. As the work continues, we expect to encounter more of the issues that arise when a standard is required, and there are one or more unfinished or impractical candidates to choose from.
31 http://www.w3.org/Submission/ws-addressing/.
handling and exchange, decision support, and other clinical functions. Our goal here has been to
design a system that is insensitive to what the actual standards are, so that when and as they
arise, they can be used in this network model without significant re-engineering. It is our hope
that the increased attention to health care IT will result in improved definition and adoption of
clinical standards.

In the multi-region test of the proposed Connecting for Health architecture, we tested the
exchange of both medication history and laboratory results. For the medication history standard,
we adopted an XML serialization of the NCPDP standard, covered in the “Medication History
Standards.” The expression of the lab results were taken from the ELINCS standard, though our
work revealed some areas where the proposed standards may need to be modified to cover a
larger potential range of uses. The laboratory standards we used are documented in the
“Laboratory Results Standards.”

Medical history and laboratory results are essential parts of any working medical network, but
they cover only a small fraction of the currently available data types, and as the health care
industry continues to embrace IT, the number of data types will grow. As a result, Connecting
for Health will continue to look to external designers and validators to guide our adoption of
clinical standards.33

The other required source of external standards is naming. Naming, which is to say the
creation and assignment of identifiers, is in many ways more complex than standardization, since
the two key requirements of naming -- uniqueness34 and permanence35 -- generally require
sophisticated schemes for generating and maintaining those identifiers. The key concept in
naming is the namespace; any given identifier needs to be unique in a particular namespace,
which is the conceptual superset of all such identifiers. Any NHIN will require a namespace for all
SNOs; each SNO will need to manage the namespace of its member entities; and each entity will
need to manage the namespace of its employees and other individuals who may have access to
the records IT system.

In all these cases, we have used existing namespaces where possible. For uniqueness of
SNOs, we have relied on the fact that each SNO must register a URL, and that all URLs are
globally unique; for entity naming, we have assumed the use of the HIPAA-mandated NPI; and
for person identification within an entity, we have assumed that the HIPAA-required security
measures will guarantee the presence of unique identifiers for employees and others with system
access.

We believe that these choices will take care of the basics of naming participant institutions
and individuals for the early NHIN. However, there are a number of ways in which naming could
become more complex over time. In particular, if our architecture succeeds, there will be a
number of third parties who are not themselves covered entities under HIPAA, and will therefore
lack an NPI, but will nevertheless need identification in the context of the NHIN (e.g., service
providers for translation or off-site storage of clinical records.) Some way of assigning names
compatible with the NPI may need to be designed. Our current solutions to naming should

33 Note that this does not presuppose the involvement of formal standards development organizations (SDOs) in all cases;
there are many examples of proposed standards that failed to get any adoption in the field, as well as examples of de
facto standards that were only blessed by standards bodies after the fact, if at all. Given Connecting for Health’s
focus on practical implementation and incremental development, we have tended to prefer de facto but unannointed
standards to proposed but unadopted ones.
34 Uniqueness in this case is contextual. A URL only needs to be disambiguated from another URL, and email address
from another email address, and so on.
35 Permanence is the characteristic of an identifier being unique in time. A permanent identifier, once issued, is never re-
used to refer to anything else. A permanent identifier may stop being valid, when the thing it points to may disappear,
but it will never point to anything else.
therefore be regarded as provisional, with future examination of additional requirements for naming being part of later phases of work.

Open Issues

The Common Framework is a work in progress; we have attempted to provide the starting technical and policy framework necessary for creating an interoperable nationwide health information network. Given the size of the task, however, such a framework necessarily leaves open technical issues, which will need to be addressed in subsequent iterations.

What follows is a brief list of such issues. Note that the list only addresses concerns that are largely or solely technological; issues such as financial structures or incentives, while vital, are out of the scope of this document.

Subscription to Data Sources

The basic transactions modeled here are request/response -- ask for and receive a record. There are obviously cases where an institution wants to subscribe to a particular data source, and receive updates when the data at that source is updated or modified.

As we have seen from the growth of http-based subscription models in other domains (e.g., the Atom syndication format36), it is possible to model subscription models by using timed or triggered updates from the data host, or timed or triggered requests from the requestor. Working out which of these patterns are most appropriate in what situations is still to be done.

Aggregated Record Access

The basic transactions modeled here are requests for one individual's records. Use cases such as data quality and biosurveillance require the delivery of aggregated data from the source entities. Current programs have a mix of direct access (e.g., CDC's Biosense program) and hierarchical access (e.g., reports to State entities who in turn report to CDC.) While the interfaces required by the Common Framework provide a method for both direct and hierarchical aggregation of records, and that such aggregation does not require and should not use the RLS, it is not clear what role, if any, the SNO should play in providing or managing those interfaces, including especially whether the ISB should provide an interface for aggregate queries, or some other SNO-wide interface should be provided, or no such interface should be provided above the level of the individual entities.

This is an especially complex and important set of questions, as it involves balancing improved measurement and observation of the health care system with risks to patient privacy, and because many of the entities with the right to access aggregate data are not covered by HIPPA, making the regulatory framework for assumptions about privacy and security more complex.

Federated Trust

Though we have adopted a transitive trust model (to trust Institution A means to trust their employees, and to trust that A manages identifiers, authentication, and authorization well), the growth of the NHIN will put that system under some strain. There is considerable work being done on federated trust models, where information and assertions about authentication and authorization are more fully described and communicated between parties. Future work on the

36 http://www.atomenabled.org/developers/syndication/.
NHIN will need to consider this work, and, if it proves viable, figure out how to implement it within the NHIN itself.

**Patient Authentication and Access**

One core goal of the Common Framework is to make it simpler for patients to gain access to their own records. We believe that the network as designed lowers the cost and raises the effectiveness of providing access to patient data; however, many hurdles still exist before there is widespread use of patient-facing access points to clinical data. A key hurdle is authentication. There is no obvious way to allow a patient to authenticate their own identity outside the context of a relationship with existing care providers; the hurdle this poses could potentially be overcome if there were a way to authenticate patients directly. Examination of possible direct patient authentication solutions may be a valuable area of inquiry. These issues are also addressed in “Patients Access to Their Own Health Information,” part of The *Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange.*

**Third Party Participation**

There is currently no mechanism for allowing entities not covered under HIPPA direct access to the NHIN. Possible rationales for allowing such access would be third-party data cleaning or warehousing solutions; third party format translations, and secure repositories acting on behalf of the patient. Presently, any third party connected to the system must be a sub-contractor to a single entity or SNO, so that the legal liability remains with that entity. There may need to be a framework for allowing third party participation in a way that increases the flexibility of the network without decreasing security.

**Multi-SNO Patient Lookup**

There is no national interface for search in the system as envisioned. This is to preserve the partitioning of clinical data, so as to prevent major privacy spills. However, such a system also requires the requesting party to have enough information to know which remote SNO to query. As the number of participating SNOs grows large, this requirement could become problematic, but a single national interface for lookup could be a significant risk to privacy, by making fishing easier. As the network grows, understanding how to balance effectiveness with privacy protection in multi-SNO lookups will be critical.

**National Services**

The NHIN as currently envisioned has no national services separate from the ISB interfaces. With the spread of National Provider Identifier numbers, increased complexity of multi-SNO lookups, data translation requirements, etc, there may be some services best provisioned for the NHIN as a whole. Some mechanism for providing these services, probably by providing for modified ISB-style interfaces, will need to be designed so that these services, should they be required, are broadly interoperable from launch.

**Response Time and SLAs**

The Common Framework Technical prototype was designed to demonstrate interoperability among diverse actors. Significant optimizations remain to be performed in order to reduce the systems response time, and profiling will be required before Service-Level Agreements can be implemented (agreements that promise, for example, sub-5 second response time for standard queries.)
Metadata and Request Filtering

The state of medical data is currently quite variable, and there is no obvious way to suddenly and dramatically increase the quality of that data, either by providing it in more structured formats or by increasing the accuracy of the fields. However, as the number of data sources grows, clinicians could find themselves moving from a world of little to no data to seeing a flood of data. Some way of pre-filtering the incoming data will be required, ideally by being able to specify relevant data types (e.g., medication history, radiology, etc), but such filtering will require relatively clean and well-formatted metadata, and must respect policy constraints such as the separation of demographic from clinical data in the system. Understanding how to improve metadata, how to integrate it in a way that respects policy constraints, and how to extract value from semi-structured data as it currently exists will be vital to future work on the NHIN.

Stemming Proliferation of Duplicate Records

As we move to a world where more data is shared, duplicate records will proliferate. Hospital A receives and stores patient data from Lab B; later, when Clinic C requests data on that patient from both A and B, C will get two copies of the lab data. Some method of identifying and rationalizing duplicate data will need to be provided as the number of data sources and frequency of requests increases.

Conclusion

We began the technical work for Connecting for Health in early 2004, and are very pleased to have arrived, in a little over two years, at a proof-of-concept system that demonstrates the core goal of the technical work to date:

It is possible to link disparate entities and regions together in a way that improves information sharing while protecting privacy, and to do so using mainly existing standards, across many hardware and software platforms, and at relatively low cost.

With three different regions involved in deploying the actual hardware and software required, we've seen that standards-based communications can provide secure links between different health care entities and networks, and that the deployment will not require massive hardware or software upgrades; will not require uniformity of hardware, software, or implementation strategies; and can be undertaken by different groups of programmers all working to an agreed set of standards.

As important as this test has been, however, we want to emphasize the modesty of the achievement relative to the enormity of the task. The actual deployment in the three regions is still early and there is insufficient usage to gauge its success. While lowering the cost of implementation and working to integrate existing IT investments where possible is necessary, it is not sufficient. If we want nationwide adoption of interoperable health IT, there is considerable additional work to be done both on extending the technical work documented here and on problems outside the technical domain, such as improving incentives for interoperability, and raising data quality at the point of collection.

We are optimistic that by taking on the issues of packing and transporting data securely among diverse sets of participants, we can create an environment where it will be easier to understand the non-technical problems, and easier to imagine solutions for them. To reach this goal, however, we need feedback on our efforts to date. In 2006, Connecting for Health will continue to host public forums for discussing the issues relevant to improving health care, and we welcome any feedback you might have on this document, on the technical architecture this
document covers, and on the related policies documented in the accompanying The *Connecting for Health* Common Framework: Resources for Implementing Private and Secure Health Information Exchange.
Acknowledgements

The working groups in the three regions of the Connecting for Health prototype and the Technical Subcommittee have worked for over two years to create a prototype of a decentralized, standards-based, and privacy-protecting architecture for the exchange of health records. During that time, we have been fortunate to work with respected experts in the fields of health and information technology, all of whom have contributed their time, energy, and expertise to the transition from a basic set of principles to a working prototype. Our consultants and volunteers have worked long hours in meetings and conference calls to negotiate high-level questions of architectural design and low-level details of particular technical protocols. We offer them our heartfelt thanks for taking on this journey with us, and look forward to the remaining work ahead.

In addition, we would like to offer special thanks to the working groups who took the conceptual technical model and instantiated it as running code: for the Massachusetts test, John Halamka, Greg DeBor, Gail Fournier, Vinod Muralidhar, and John Calladine; for the Indiana test, J. Marc Overhage, Clement McDonald, Lonnie Blevins, and Andrew Martin; and for the California test, Will Ross and Don Grodecki.

Finally, we must note that none of this work would have been possible without the leadership and inspiration of Clay Shirky, who encouraged us to turn theory into practice, and whose unmatched skills at navigating and then capturing each progressive phase of our work over the last two years allowed us to do so.

Connecting for Health Technology Subcommittee

Clay Shirky, New York University, (Chair)

Laura Adams, Rhode Island Quality Institute

Steve Adams, RMD Networks

William Braithwaite, MD, eHealth Initiative, (Co-Chair, Policy Subcommittee)

Deleys Brandman, First Consulting Group

Bryan Breen, Cisco Systems, Inc.

Sophia Chang, MD, MPH, California HealthCare Foundation

Art Davidson, MD, MSPH, Denver Public Health

Didi Davis, Eclipsys, Healthcare Information and Management Systems Society, and Integrating the Healthcare Enterprise

Greg DeBor, Computer Sciences Corporation

Lyman Dennis, Partnership HealthPlan of California, Healthcare Information and Management Systems Society, and Integrating the Healthcare Enterprise

George Eisenberger, IBM Corporation

David A. Epstein, IBM Software Group

Linda Fischetti*, RN, MS, Veterans Health Administration

Mark Frisse, MD, MBA, MSc, Vanderbilt Center for Better Health (Co-Chair, Policy Subcommittee)

Don Grodecki, Browsersoft, Inc.

John Halamka, MD, CareGroup Healthcare System

Bob Hedgcock, Wisconsin Health Information Exchange

Noreen Hurley, Tufts Health Plan

Charles Jaffe, MD, PhD, Intel Corporation

Timothy Kenney, GE Healthcare
Josh Lemieux, Omnimedix Institute
J.P. Little, RxHub
Christopher Lindop, Eastman Kodak Company
David Lubinski, Microsoft Corporation
Janet Marchibroda, eHealth Initiative
Gregory Andre Marinkovich*, MD, FAAP
J.P. Little, LTC, Marine Corps, Office of Secretary of Defense/Health Affairs
Patrick McMahon, Microsoft Corporation
Omid Moghadam, Intel Corporation
Don Mon, PhD, American Health Information Management Association
Bruno Nardone, IBM Corporation
J. Marc Overhage, MD, PhD, Indiana Health Information Exchange; Indiana University School of Medicine, Regenstrief Institute for Healthcare
George Peredy, MD, Kaiser Permanente, HealthConnect
Nick Ragouzis, Enosis Group, LLC
Rick Ratliff, SureScripts
Jere Retzer, Oregon Health and Science University
Wes Rishel, Gartner Group
Barry Rhodes*, PhD, Center for Disease Control, United States Department of Health and Human Services
Scott Schumacher, PhD, Initiate Systems, Inc.
Raymond W. Scott, Axolotl Corporation
Don Simborg, MD, American Medical Informatics Association
Geoff Smith, Meditech
Jonathan Teich, MD, PhD, Healthvision
Micky Tripathi, Massachusetts eHealth Collaborative
Charlene Underwood, Healthcare Information and Management Systems Society, EHR Vendor Association
Karen Van Hentenryck, HL-7
Jukka Valkonen, California HealthCare Foundation
Cynthia Wark*, CAPT, United States Public Health Service Commissioned Corps, Centers for Medicare and Medicaid Services, United States Department of Health and Human Services
Jon White*, MD, Agency for Healthcare Research and Quality, United States Department of Health and Human Services
Scott Williams, MD, MPH, HealthInsight
Amy Zimmerman-Levitan, MPH, Rhode Island Department of Health

*Note: Federal employees participate in the Subcommittee but make no endorsement
Health Information Exchange:
Architecture Implementation Guide
Health Information Exchange: Architecture Implementation Guide
The document you are reading is part of *The Connecting for Health Common Framework*, which is available in full and in its most current version at: http://www.connectingforhealth.org/.

The Common Framework will be revised and expanded over time. As of October 2006, the Common Framework included the following published components:
Health Information Exchange: Architecture Implementation Guide

1 Purpose of This Document

This document specifies a technical architecture designed by Connecting for Health for communication of protected health information between sub-network organizations (SNOs) on a Nationwide Health Information Network (NHIN). The architecture and messaging standards discussed here make up part of Connecting for Health's Common Framework, a proposed collection of technical standards and policies designed to make it possible to build a NHIN that is effective and achievable in incremental steps, and supports the required discovery and transport of patient records between authorized parties while protecting those records from unauthorized access or use.

The technical goal of the Common Framework is to define a minimal set of commonly adhered to standards and policies that allow for the SNO-based implementation of health information networks that are nationally interoperable. In the Connecting for Health view, the National Health Information Network is an interoperable network of networks, achieved through incremental creation of Common Framework-compliant SNOs.

In addition to the messaging standards, it provides information to support the implementation of Record Locator Service (RLS) and Inter-SNO Bridge (ISB) communication services, including messaging protocols, standards, authentication, and security for the transactions. The RLS is a community Master Patient Index (MPI) that stores only the location of patient records, plus enough demographic details to match a query with the appropriate records, and is designed to let entities within a SNO locate one another's records. The ISB is the interface for communications between entities in different SNOs. The RLS and the ISB have been designed to be platform-neutral. Although the RLS will be, in practice, databases accessible through secure web servers, the definition of a Common Framework-compliant RLS or ISB has to do with interfaces, messages, and behaviors, not with any particular technology.

The NHIN assumes the use of encrypted communications over the internet among participants, and models all interactions as Web Services conversations in SOAP. (This document assumes a familiarity with the Web standards SSL, XML 1.0, and SOAP 1.1, as well as the clinical standard HL7 2.4; we do not reproduce the documentation for those standards here.) Modeling the NHIN transactions in SOAP provides a degree of flexibility to support various messaging types within a single framework. The messages described here also support exchange of some types of non-protected information. Due to the generic nature of the NHIN query message structure, we anticipate extending the architecture to support additional types of communications required by a NHIN, from additional forms of clinical information to administrative messages.

Connecting for Health thanks Clay Shirky, Chair, Technical Subcommittee, and Adjunct Professor, New York University Graduate Interactive Telecommunications Program; Vinod Muralidhar and John Calladine, Computer Sciences Corporation (CSC); Lonnie Blevins and Clement McDonald, MD, Regenstrief Institute for Healthcare; and Don Grodecki, Browsersoft, Inc., for documenting this implementation guide.

©2006, Markle Foundation
This work was originally published as part of The Connecting for Health: Resources for Implementing Private and Secure Health Information Exchange and is made available subject to the terms of a license (License) which may be viewed in its entirety at: http://www.connectingforhealth.org/license.html. You may make copies of this work; however, by copying or exercising any other rights to the work, you accept and agree to be bound by the terms of the License. All copies of this work must reproduce this copyright information and notice.
2 Interaction Overview

Technical interactions between entities in the NHIN involve transactions between software clients (typically an EHR, secure browser, or proxy server, and called NHIN clients throughout) and either the RLS or the ISB.

2.1 RLS Use Cases

The Record Locator Service (RLS) is essentially a master patient index within a SNO that refers to record locations at more than one institution within that SNO. It has two required interactions with the participating entities in a SNO: it accepts updates to patient demographics and record locations; and it accepts queries for the location of patient records and returns record locations when it finds matches.

Accepts Updates to Patient Record Location

The RLS accepts updates to patient record locations held by participating sources of clinical data. These updates contain identifying details of the patient, the identifier of the source system, and a medical record number (MRN) unique key for the location of that record within the source system. In practice, this will often be expressed as a Uniform Record Identifier (URI), but may include other formats, such as fax numbers as contact details for those queries that can't be made over the Web.

The intent of these updates is to provide the raw information necessary to accept demographic queries for patient records, and to be able to return a unique pointer to the data for patient records that do match. The four possible modes of behavior that a clinical data source may request of the RLS are: add a new record number and attendant identifying data; update an existing record; remove a record; and merge or unmerge two records (though merge is actually a composite function, acting as an atomic update+remove function acting on two records at once.)

The updates will generally be in batch mode, and may in some cases even be loaded from physical media. While a rapid cycle for updating pointers to materials held in the various source systems is desirable, the loading of the data and the return of the confirmation can be asynchronous.

Because of the variability of delivery of data sources from participating entities and of the patient databases underlying any given RLS, the methods for loading records may vary SNO by SNO, and are not specified in this guide.

Accepts Queries and Returns Record Locations

The RLS accepts queries from authorized entities looking for patient records. The queries will include demographic details of the patient whose records are being sought, and, optionally, an institution ID and MRN.

The RLS must have a method for determining which patients, if any, match the demographics presented, and must guarantee that the chance of a false positive falls below the target threshold for incidental disclosures. This matching algorithm is not part of the RLS itself, but is an internal service the RLS relies on, and can vary between SNOs, so long as whatever matching algorithm is used produces sufficient accuracy of matches.

The RLS should return the locations of the records that match the submitted demographics and are above the target threshold for accuracy of match. These records will be ideally expressed as a URL that fuses the institution location with the MRN. However, other methods for requesting record information, such as phone or fax numbers of those institutions operating without an electronic health record (EHR) system may be returned when the location can't be expressed as a URL.
Patient queries will generally be in synchronous request-response mode, and should be optimized to operate as near real time as possible. It is possible that a clinic, for example, will want to submit batch or asynchronous individual queries to obtain record locations for the following day's visits, but the querying capability should be designed and optimized for real-time and synchronous requests as the principal interaction. Additionally, the SNO can allow or provide for the use of proxy servers to aggregate the clinical results on behalf of the requesting client. For a more complete description of questions of synchrony and aggregation, see "The Common Framework: Technical Issues and Requirements for Implementation document."

The interaction between the RLS, the clinical data sources, and the requestor of data locations can be seen in the following diagram. Note that the requesting and return of the actual records does not involve the RLS directly, but is listed here for conceptual completeness:

![Figure 1 RLS Interactions](image)

### 2.2 ISB Use Cases

The Inter-SNO Bridge (ISB) is an interface to a particular SNO, for queries originating from outside the SNO (either from another SNO, or from unaffiliated entities.) It exists to simplify conversations between remote entities, so each institution is not required to know the names of all other institutions (which would create significant problems of scale.) Instead, by routing NHIN traffic between SNOs, and by having each SNO manage its own internal traffic (which is has to do anyway), the problem becomes much smaller. In addition, it provides a highly observable point for all remote traffic, benefiting security.

The ISB has a single required interaction with outside entities -- it receives requests for patient records in exactly the same format as an RLS does, and it returns either a) the locations
of those records for further use by the requestor (the 'two-pass' pattern) or b) acts as an aggregator of the records themselves, and returns the aggregate clinical data (the 'one-pass' pattern.)

Two Pass

The ISB accepts queries from other SNOs looking for patient records. The canonical conversation is between the ISB of the requestor and the ISB being queried; both ISBs must have valid SSL certificates. Other than specifying an address of the SNO to be queried, the queries are otherwise identical to those made to an RLS, and will include demographic details of the patient whose records are being sought, and, optionally, an institution ID and MRN.

The ISB will confirm receipt of the query, record the address where the results should be returned, and then pass the query to its local RLS, exactly as if were an ordinary entity within the SNO. If the requesting SNO has requested a two-pass interaction, the ISB will receive the record locations from the RLS (or, optionally, any additional proxy servers used by the SNO), and will then initiate a second transaction with the original requestor.

The original requestor may then choose any or all of the record locations it would like to receive data from, and will dispatch a second query to the ISB listing those locations. The ISB will confirm receipt of the second query, record the address where the results should be returned, and then ask the local entities (or any optional proxies) for the records themselves, exactly as if were an ordinary entity within the SNO. The ISB will receive the records from the local entities (or proxies), and will then initiate a transaction with the original requestor to deliver the aggregate records.

Interactions with the ISB will always be asynchronous; the requestor must specify an address where the results of the query will be deposited. For a more complete description of questions of synchrony, see “The Common Framework: Technical Issues and Requirements for Implementation document.”

The two-pass interaction between the ISB, the local clinical data sources, and the requestor of data locations can be seen in the following diagram:
Figure 2 ISB Two Pass Interactions

One Pass

The ISB accepts queries from other SNOs looking for patient records. The canonical conversation is between the ISB of the requestor and the ISB being queried; both ISBs must have valid SSL certificates. Other than specifying an address of the SNO to be queried, the queries are otherwise identical to those made to an RLS, and will include demographic details of the patient whose records are being sought, and, optionally, an institution ID and MRN.

The ISB will confirm receipt of the query, record the address where the results should be returned, and then pass the query to its local RLS, exactly as if were an ordinary entity within the SNO. If the requesting SNO has requested a one-pass interaction, the ISB will receive the record locations from the RLS (or, optionally, any additional proxy servers used by the SNO), and will then initiate a second set of transaction with the local holders of the record specified by those locations. The ISB will receive the records from the local entities (or proxies), and will then initiate a transaction with the original requestor to deliver the aggregate records.

Interactions with the ISB will always be asynchronous; the requestor must specify an address where the results of the query will be deposited. For a more complete description of questions of synchrony, see “The Common Framework: Technical Issues and Requirements for Implementation document.”
The one-pass interaction between the ISB, the local clinical data sources, and the requestor of data locations can be seen in the following diagram:

Figure 3 ISB One Pass Interactions

2.3 NHIN Data Interchange

All messages in the NHIN, whether within or between SNOs, are specified as client/server SOAP conversations. A client requesting information within a SNO of which it is a member formulates its data query and sends it to the SNO’s RLS. A client requesting information from a SNO of which it is not a member formulates its data query and sends it to the remote SNO’s ISB.

NHIN queries are based on the HL7 query model. A single NHIN query-and-response may consist of one SOAP conversation (a “synchronous” query-and-response) or two SOAP conversations (an “asynchronous” query-and-response, where the request and the subsequent delivery of results are two separate transactions.) In the synchronous query-and-response case, the query is sent in the SOAP request message and the query results are returned in the SOAP
response message. In the case of the asynchronous query-and-response, the query is sent as the SOAP request and simply acknowledged in the SOAP response. In a subsequent SOAP conversation, the query results are sent back to the query client as the SOAP request message and simply acknowledged in the corresponding SOAP response.

**RLS Data Interchange**

When a NHIN client sends the SOAP query to the ISB (the NHIN server), the ISB immediately acknowledges receipt of the query and terminates the SOAP communication. The ISB probes the databases(s) within its SNO to get the requested data. Once that is complete, the ISB generates the query response, opens a new communication channel back to the client or its designee, and returns the response information.

When the RLS receives a query, it may satisfy that query in any manner it so chooses, as long as it interprets the query according the rules set forth in his document and responds to the query in the format prescribed herein. For example, one SNO might contain a central server on which health data is aggregated from all of the other SNO members. That SNO's ISB responds to a patient-based NHIN query by reading data from its single aggregation server and responding to the NHIN client. Another SNO might have no central aggregation of data. When that SNO's ISB receives the same NHIN query, it would interrogate all of its other SNO systems to obtain the requested data. Several NHIN prototype systems have an approach somewhere in between these two paradigms. Those SNOs maintain an aggregated (community) Master Patient Index (MPI), but do not aggregate any other clinical content. For a patient-based query, the ISB for one of those SNOs would query the aggregated MPI to find out which other SNO nodes might contain the requested data and then query only the potential data-bearing nodes for information.

**SNO Data Interchange**

When a NHIN client sends the SOAP query to the ISB (the NHIN server), the ISB immediately acknowledges receipt of the query and terminates the SOAP communication. The ISB probes the databases(s) within its SNO to get the requested data. Once that is complete, the ISB generates the query response, opens a new communication channel back to the client or its designee, and returns the response information.

When an NHIN server receives a query, it may satisfy that query in any manner it so chooses, as long as it interprets the query according the rules set forth in his document and responds to the query in the format prescribed herein. For example, one SNO might contain a central server on which health data is aggregated from all of the other SNO members. That SNO's ISB responds to a patient-based NHIN query by reading data from its single aggregation server and responding to the NHIN client. Another SNO might have no central aggregation of data. When that SNO's ISB receives the same NHIN query, it would interrogate all of its other SNO systems to obtain the requested data. Several NHIN prototype systems have an approach somewhere in between these two paradigms. Those SNOs maintain an aggregated (community) Master Patient Index (MPI), but do not aggregate any other clinical content. For a patient-based query, the ISB for one of those SNOs would query the aggregated MPI to find out which other SNO nodes might contain the requested data and then query only the potential data-bearing nodes for information.
3    RLS/ISB Development Goals

3.1    Overall Directions

All communications are SSL-encrypted SOAP 1.1 messages.

ISB-to-ISB communication is always asynchronous. Upon receiving the SOAP query message, the ISB may immediately return an acknowledgment (ACK) message to the CLIENT. In that case, if a SOAP fault is generated, the CLIENT does not expect any further reply from the query server. If the message is accepted, the CLIENT expects to receive an asynchronous reply containing the query results. That is, the CLIENT creates a thread that will accept the eventual query results SOAP message from the ISB. The CLIENT system decides how to act if the return message does not arrive in a timely manner.

Errors in message validation are reported as SOAP faults. Errors in asynchronous processing logic are reported back to the client service within the SOAP response message.

Every NHIN request message includes information about the specific user making the request. The ISB logs the requestor identity information along with the query and the response. In other words, the ISB keeps a complete log of “who, what, when, and where” for all of the NHIN queries that it processes.

Most of the patient information in the query and response messages is represented as XML-encoded version 2.4 HL7. HL7’s formal specification of the XML encoding for version 2.4 resides at http://www.hl7.org. Patient medication dispensing history is returned in the query response message in NCPDP Scripts 8.1 format.

NHIN query messages are pure HL7, represented in XML per HL7’s documentation. Responses are all HL7, except for the medication dispensing history mentioned above. SNOs should readily be able to interpret and construct these familiar messages without re-inventing their message content creation services and functions. The NHIN should also be able to take advantage of new HL7 developments without having to change this fundamental NHIN message architecture.

3.2    Directions for ISB/RLS Design

All communications are SSL-encrypted SOAP 1.1 messages.

ISB-to-ISB communication is always asynchronous. Upon receiving the SOAP query message, the ISB immediately returns an acknowledgment (ACK) message to the CLIENT. If the message is rejected (a SOAP fault is generated instead of the ACK), the CLIENT does not expect any further reply. If the message is accepted, the CLIENT expects to receive an asynchronous reply containing the query results. That is, the CLIENT creates a thread that will accept the eventual query results SOAP message from the ISB. The CLIENT system decides how to act if the return message does not arrive in a timely manner.

Errors in message validation are reported as SOAP faults. Errors in asynchronous processing logic are reported back to the client service within the SOAP response message.
Every NHIN request message includes information about the specific user making the request. The ISB logs the requestor identity information along with the query and the response. In other words, the ISB keeps a complete log of “who, what, when, and where” for all of the NHIN queries that it processes.

Most of the patient information in the query and response messages is represented as XML-encoded version 2.4 HL7. HL7’s formal specification of the XML encoding for version 2.4 resides at http://www.hl7.org. Patient medication dispensing history is returned in the query response message in NCPDP Scripts 8.1 format.

NHIN query messages are pure HL7, represented in XML per HL7’s documentation. Responses are all HL7, except for the medication dispensing history mentioned above. SNOs should readily be able to interpret and construct these familiar messages without re-inventing their message content creation services and functions. The NHIN should also be able to take advantage of new HL7 developments without having to change this fundamental NHIN message architecture.
3.3 HL7 XML Background

HL7 is a well-established standard for communication of medical information between computer systems. HL7’s long standing encoding of 2.x HL7 messages has been “piped” delimited ASCII, with ASCII RETURN (ASCII 13) and/or LINE FEED (ASCII 10) characters demarking the end of HL7 message “segments”, and other delimiters defining the field and subfield boundaries. This is well-described in the HL7 manual available at http://www.hl7.org. HL7 has also now defined an XML encoding for version 2.x messages.

The tags for the XML encoding are defined by HL7’s existing abbreviations for segment, field and subcomponent names. For example, the tags names for segments are the three character HL7 segment names. “OBX” is the tag for the observation segment. The tag names for fields and data type components are the HL7 field abbreviations, e.g. the tag for the third OBX field would be OBX.3, and e.g. the tag for the third component of a CE data type would be “CE.3”. The XML schema for a given message identifies the segments and fields that are required.

Version 3 of HL7 is version 3. uses only XML encoding. However, almost all institutions currently use a 2.x version of HL7 and almost no clinical care system has adopted version 3. New 2.x HL7 versions continue to be developed in addition to the work on HL7 version 3.

We represent our messages in the widely used HL7 2.4 format so that it can be easily implemented in today’s institutions and because everyone in the industry is familiar with it. Using version 2.4XML gives us the advantage of the unified methods of processing the content of SOAP messages as well as direct translatability between pipe delimited HL7 messages and their XML equivalents. The HL7 content that is relevant to this project is listed in the following HL7 manual chapters.

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Broad description of the HL7 message format</td>
</tr>
<tr>
<td>2</td>
<td>defines HL7 data types and control segments</td>
</tr>
<tr>
<td>3</td>
<td>defines Patient Identification (PID) segments</td>
</tr>
<tr>
<td>5</td>
<td>defines HL7 Query messages</td>
</tr>
<tr>
<td>7</td>
<td>defines Observation Reporting segments for transmitting patient reports and results</td>
</tr>
</tbody>
</table>

We designate some HL7 fields as “not used” for this project. Those field values will be ignored in the communications. No error will be signaled if these fields are populated.

HL7 content will be sent within the “body” of our SOAP messages with standard SOAP message headers and SOAP wrappers. The SOAP standard is defined at http://www.w3.org/TR/soap/.

Appendix B contains general guidelines for formatting the HL7 content. In the near future, we hope to simply point developers to an existing HL7 implementation guide, such as the ELINCS specification, for this information.

4 General SOAP Message Structure

NHIN queries use a single SOAP service named “NHINQuery”. The two SOAP query operations for this service support an XML “wrapper” for sending an HL7 query via a SOAP message and an XML “wrapper” for receiving the response back in a SOAP message. Hence, the
contents of the query message define the type of search performed and data returned rather than the SOAP operation.

The top-level SOAP <BODY> elements within the SOAP message are in the namespace “http://www.nhin.gov/messaging”. The SOAP header always contains message routing information and data elements describing the user sending the query. Section 4.1 describes the contents of the SOAP header.

At the topmost level of the SOAP message <BODY>, each request contains only the <NHINQuery> node. The WS-Basic Profile 1.0 requires a single node within the SOAP <BODY>, so there will never be a second node at this level. Within the <NHINQuery> node, we find two other nodes. One contains control information about the query settings and the other contains the actual query. For example, the topmost level of the PatientDataQuery SOAP message <BODY> looks like:

```xml
<soapenv:Body>
  <nhin:NHINQuery>
    <nhin:EvaluationSettings>
      <nhin:MaxResponseInterval>60</nhin:MaxResponseInterval>
      <nhin:ResponseStyle>I</nhin:ResponseStyle>
    </nhin:EvaluationSettings>
    <nhin:Query format="HL7" version="2.4">
      <QBP_Z01 xmlns="urn:hl7-org:v2xml">
        ...
      </QBP_Z01>
    </nhin:Query>
  </nhin:NHINQuery>
</soapenv:Body>
```

The <Query> node defines the information that is actually being requested. The SOAP service and operation are merely wrappers in which to pass this generic “query” specification. The format and version attributes define the format in which the query is expressed. Currently, only HL7 version 2.4 queries are supported. NHIN is considering support of HL7 version 3.0 as its use becomes more widespread.

At the topmost level of the SOAP message <BODY>, each response message also contains a single node. The <NHINResponse> node contains two data-bearing nodes, just like the NHINQuery node. One echoes the CLIENT control information and the other contains the query response. For example, the topmost level of the PatientDataQuery SOAP message <BODY> might look like:

```xml
<soapenv:Body xmlns:nhin="http://www.nhin.gov/messaging"
  xmlns:nhin="http://www.nhin.gov/messaging">
  <nhin:NHINResponse>
    <nhin:EvaluationSettings>
      <nhin:MaxResponseInterval>60</nhin:MaxResponseInterval>
      <nhin:ResponseStyle>I</nhin:ResponseStyle>
    </nhin:EvaluationSettings>
    <nhin:Response format="HL7" version="2.4">
      <RSP_Z01 xmlns="urn:hl7-org:v2xml">
        ...
      </RSP_Z01>
    </nhin:Response>
  </nhin:NHINResponse>
</soapenv:Body>
```
All NHIN queries are expressed as HL7 2.4 messages and segments. Most of the query responses are also standard HL7 messages and are represented in a single <Response> node. However, queries that return medication history do so in the NCPDP Scripts 8.1 XML format (an XML representation of NCPDP) rather than in HL7. To accommodate this, and future, mixed data representations within a query response, multiple <Response> nodes are permitted. Data formats are not mixed within one <Response> node. For example, an HL7 response will never be intermixed with an NCPDP Scripts response, although they may be wrapped within the same query response message.

Every <EvaluationSettings> node has the same schema definition across all messages, as documented in Appendix C. Values within this node define general query processing settings, like the maximum time interval before the querying system expects a response, as per the example above.

We define the following SOAP operations, which cover the current use cases:

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PatientDataQuery</td>
<td>Requests patient health data for a single patient.</td>
</tr>
<tr>
<td>PatientDataQueryResponse</td>
<td>Returns the requested patient health data for all registrations found for the specified person.</td>
</tr>
</tbody>
</table>

4.1 XML Namespaces

NHIN query messages currently use two namespaces for NHIN-specific elements and attributes, one for the query data and one for the header attributes used to route the asynchronous query responses (see next section of this document). The header attributes used for response routing are defined in the "http://www.nhin.gov/addressing" namespace, which is qualified as "nhinWsa:" in the examples used in this document. (Note that nhin.gov is a URI but not a URL; we have adopted it simply to guarantee uniqueness of namespace.) All other NHIN-specific elements and attributes are defined in the "http://www.nhin.gov/messaging" namespace, which we qualify with "nhin:" in the examples in this document. The SOAP envelope tags for a typical NHIN query might look like:

```xml
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:nhinWsa="http://www.nhin.gov/addressing"
    xmlns nhin="http://www.nhin.gov/messaging" >
</soapenv:Envelope>
```

4.2 Asynchronous Query-and-Response Messaging Between ISBs

We expect that the WS-Addressing 1.0 W3C Recommendation will become a W3C standard within the next year. We believe it will enjoy widespread use following standardization, and that tools for implementing it will then proliferate. Of special interest to the NHIN project are the WS-Addressing 1.0 controls (in the SOAP header) for defining an asynchronous SOAP conversation, since all initial NHIN SOAP conversations will be asynchronous.

However, NHIN is not comfortable making WS-Addressing 1.0 a requirement for initial NHIN participants. WS-Addressing is not easily implemented across SOAP server platforms, at least in the versions that are currently in wide use. Newer implementations, as they currently exist,
would make it difficult to communicate with NHIN servers on their present SOAP server platforms. Hence, NHIN defines its asynchronous conversations using a subset of the tag names that WS-Addressing would use, but in NHIN’s own XML “namespace”. The NHIN architecture also defines its logically asynchronous query-and-reply conversation as a pair of physically synchronous SOAP conversations, one conversation for the query and one for the response. These variances from real WS-Addressing enable immediate use of the NHIN message infrastructure, but simplify the move to full WS-Addressing in the future. For now, a WS-Addressing-style value, in the SOAP message header, defines where the asynchronous query response will be sent by the NHIN server.

In an asynchronous NHIN query and reply, a NHIN client sends a query to an NHIN server in a SOAP message. The NHIN server immediately returns a SOAP “ACK” message (see Appendix F) to the NHIN client, signifying that the query has been received and understood. This initial SOAP conversation, representing the NHIN “query”, is now complete as far as the SOAP servers are concerned. Once the NHIN server has read and formatted the query results, it initiates a new SOAP conversation. The NHIN server sends the query response to the destination it found in the <ReplyTo> node of the original SOAP query message. Once the NHIN client receives the query response, it returns a SOAP “ACK” to the NHIN server. This completes the NHIN “response” SOAP conversation. To summarize, the NHIN logical query-and-respond conversation is implemented as two physical SOAP conversations: a query-and-ACK SOAP conversation followed by a separate respond-and-ACK SOAP conversation. This logically asynchronous conversation can be implemented on virtually all SOAP server platforms.

Suppose the ISB receives a message whose SOAP message begins with the following:

```xml
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:nhinWsa="http://www.nhin.gov/addressing"
  xmlns nhin="http://www.nhin.gov/messaging" >
  <soapenv:Header>
    <nhinWsa:MessageId>1234</nhinWsa:MessageId>
    <nhinWsa:ReplyTo>
      <nhinWsa:Address>https://1.2.3.4:8443/myapp/services/NHINQuery</nhinWsa:Address>
    </nhinWsa:ReplyTo>
  </soapenv:Header>

  <nhinWsa:Address>https://1.2.3.4:843/myapp/services/NHINQuery</nhinWsa:Address>
</soapenv:Envelope>
```

The ISB will send the `NHINPatientDataResponse` query response to the URL `http://1.2.3.4:8080/myapp/services/NHINPatientDataResponse`.

An example of a SOAP header with full NHIN addressing information follows:

```xml
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:nhinWsa="http://www.nhin.gov/addressing"
  xmlns nhin="http://www.nhin.gov/messaging" >
  <soapenv:Header>
    <nhinWsa:MessageId>1234</nhinWsa:MessageId>
    <nhinWsa:ReplyTo>
      <nhinWsa:Address>
      </nhinWsa:Address>
    </nhinWsa:ReplyTo>
  </soapenv:Header>
```

The ISB will send the `NHINPatientDataResponse` query response to the URL `http://1.2.3.4:8080/myapp/services/NHINPatientDataResponse`.
4.3 Identifying the Query User

Every query must identify the user who initiated the query, as per HIPAA guidelines, and log the user identification along with a description of the data that was accessed. The Inter-SNO Bridge service that receives the NHIN query trusts that the user was properly authenticated by the sending SNO. The mechanism for reaching that understanding is beyond the scope of this document.

We consulted the OASIS SAML specification to find the format in which it represents username information in the SOAP header, hoping to use their format. However, the “UsernameToken” 1.0 profile does not specify some attributes that we require, like the user’s full name in any concrete manner. Instead then, NHIN queries identify the query-requesting user in an NHIN-specific <QueryRequestor> node within the SOAP header. NHIN plans to harmonize its user identification format with the SAML specification in the future. Currently though, the query user’s identity in the <QueryRequestor> node is in the same data format that one would use to retrieve the access log information about that query user. That is, the query user is defined in the same format that would be found within an HL7 query or response.

NHIN queries represent the query-requesting user in a familiar HL7 2.4 XCN data type. An example follows:

```xml
<nhin:Security>
  <nhin:QueryRequestor>
    <XCN.1>JoeUser</XCN.1>
    <XCN.2>Smith</XCN.2>
    <XCN.3>Joseph</XCN.3>
  </nhin:QueryRequestor>
</nhin:Security>
```

This is the same manner in which that user would have been represented within any of the HL7 2.4 messages sent across the NHIN.

4.4 NHIN SERVER ERROR HANDLING
Upon receipt of a request message from a CLIENT system, the SERVER acknowledges receipt of the message, validates the syntax of the incoming message, and asynchronously starts processing the message. If an error occurs after the “valid message” indication, the error information must be returned to the CLIENT system in the asynchronous SOAP response. If the error occurs before the SERVER validates the query message and responds with the “ACK” SOAP message, a SOAP Fault can be generated. Appendix D lists the potential fault codes returned and the information that should be included in the accompanying detail.

When an error/fault occurs after the NHIN server has sent its ACK back to the NHIN client, it is impossible (or at least very difficult) to return a SOAP Fault using a current SOAP server. Therefore, the error/fault must be sent back in the asynchronous query response message. In that message, the MSA.1 (ACKNOWLEDGMENT CODE) value is “AE” (Application Error) instead of “AA”. A descriptive fault message is also returned in the MSA.3 (TEXT MESSAGE).

The NHIN SERVER can encounter different types of errors once it receives a valid query message. An application error may occur within the SERVER itself. A SOAP fault may occur when the SERVER tries to send a SOAP message to another node within its SNO when that system is down, appropriate security certificates are not in place, network communications fail, the service rejects the message due a syntax error, etc. Finally, a true application error may occur inside the SNO node that is doing the query resolution on behalf of the NHIN server.

In the first case, the NHIN Server must create its own error code and error message. In the second case, the server retrieves the SOAP fault code and error message from the SOAP fault. In the third case, the server recovers the application error information from the response message it gets back from the SNO node. In any case, the NHIN server ends up with an error code and an error message that are sent back to the CLIENT within the MSA segment of the query response.
5  HL7 Queries Within PatientDataQuery Operation

Although there is a single NHIN SOAP operation, it may contain a variety of different HL7 queries. HL7 2.4 requires a formal “Conformance Statement“ be published for each of these queries. The sections that follow document the currently supported NHIN queries for patient data and their “Conformance Statements”. Table 1 below lists all of the currently defined HL7 queries supported within the NHINQuery service.

<table>
<thead>
<tr>
<th>Event Code</th>
<th>Query Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Z01</td>
<td>Observation Reporting Query</td>
<td>Requests clinical results and reports for one person.</td>
</tr>
<tr>
<td>Z02</td>
<td>Patient Identities Query</td>
<td>Requests demographics (PID) information for all registrations for a single person.</td>
</tr>
<tr>
<td>Z03</td>
<td>Access History Query</td>
<td>Requests history (log) of queries made for data about one person or by one person.</td>
</tr>
</tbody>
</table>
5.1 Observation Reporting Query for Patient Results and Reports

An Observation Reporting Query requests clinical results and reports for one person. Query “parameter” values may be used to limit the number and type of the returned results and reports. The query contains HL7’s MSH, QPD, and PID, and RCP segments, in that order. The response message is an HL7 response based on the ORU^R01 message for laboratory reports and results and/or a NCPDP Scripts 8.1 element for medication dispensing history. The official HL7 query “conformance statement” for the query is defined in section below, although it does not address the medication dispensing history portion of the returned data.

Most clinical data are supported by this query-response pair. Clinical laboratory results, pathology reports, vital signs, nursing notes, radiology reports, diagnosis lists, patient questionnaire results, discharge summaries, and more are easily represented in the response message. Refer to chapter 7 of the HL7 2.4 manual for more details on the ORU^R01 message and its great flexibility.

The HL7 ORU^R01 messages are formatted according to the ELINCS 2.0 standard, described at http://www.chcf.org/topics/chronicdisease/index.cfm. The ELINCS specification contains an implementation guide for constructing HL7 ORU^R01 messages. ELINCS defines LOINC codes to be used for common laboratory tests, types of HL7 data expected in each ORU^R01 data field, and general guidelines for HL7 message construction. “Laboratory Results Standards, part of The Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange, notes the deviations we make from the ELINCS standard. For the most part, these deviations are simply the permission to populate HL7 data fields in cases where ELINCS prohibits those data fields from being valued.

The NCPDP Scripts 8.1 XML in which the medication dispensing history is returned is described in “Medication History Standards,” part of The Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange.

5.1.1 Observation Reporting Query Conformance Statement

<table>
<thead>
<tr>
<th>Query Statement ID:</th>
<th>Z01</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type:</td>
<td>Query</td>
</tr>
<tr>
<td>Query Name:</td>
<td>Observation Reporting Query</td>
</tr>
<tr>
<td>Query Trigger (= MSH-9):</td>
<td>QBP^Z01^QBP_Z01</td>
</tr>
<tr>
<td>Query Mode:</td>
<td>Both</td>
</tr>
<tr>
<td>Response Trigger (= MSH-9):</td>
<td>RSP^Z01^RSP_Z01</td>
</tr>
<tr>
<td>Query Characteristics:</td>
<td>Patient will be identified by searching the NHIN server’s Master Patient Index (MPI) or MPIs based on patient attributes defined in the query’s PID segment. Results and reports may be returned for zero, one, or more patient registrations found by the NHIN server.</td>
</tr>
<tr>
<td>Purpose:</td>
<td>Queries an NHIN server for clinical patient data. Input is list of known patient identifiers and attributes. Output is clinical results and reports for that patient, as specified in the other query parameters.</td>
</tr>
<tr>
<td>Response Characteristics:</td>
<td>Results and reports are returned in standard HL7 ORU message format.</td>
</tr>
<tr>
<td>Based on Segment Pattern:</td>
<td>R01</td>
</tr>
</tbody>
</table>
### Query Grammar Pattern

<table>
<thead>
<tr>
<th>QBP^Z01^QBP_Z01</th>
<th>Query Grammar:</th>
<th>Group Control</th>
<th>Comment</th>
<th>Support Indicator</th>
<th>Sec Ref</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSH</td>
<td>Message Header</td>
<td></td>
<td></td>
<td></td>
<td>2.16.9</td>
</tr>
<tr>
<td>QPD</td>
<td>Query Parameter Definition</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PID</td>
<td>Patient Identification</td>
<td></td>
<td></td>
<td></td>
<td>3.4.2</td>
</tr>
<tr>
<td>RCP</td>
<td>Response Control Parameter</td>
<td></td>
<td></td>
<td></td>
<td>5.5.5</td>
</tr>
</tbody>
</table>

### Response Grammar Pattern

<table>
<thead>
<tr>
<th>RSP^Z01^RSP_Z01</th>
<th>Response Grammar:</th>
<th>Group Control</th>
<th>Comment</th>
<th>Support Indicator</th>
<th>Sec Ref</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSH</td>
<td>Message Header</td>
<td></td>
<td></td>
<td></td>
<td>2.16.9</td>
</tr>
<tr>
<td>MSA</td>
<td>Message Acknowledgement</td>
<td></td>
<td></td>
<td></td>
<td>2..16.8</td>
</tr>
<tr>
<td>[ERR]</td>
<td>Error</td>
<td></td>
<td></td>
<td></td>
<td>2.16.5</td>
</tr>
<tr>
<td>QAK</td>
<td>Query Acknowledgement</td>
<td></td>
<td></td>
<td></td>
<td>5.5.2</td>
</tr>
<tr>
<td>QPD</td>
<td>Query Parameter Definition</td>
<td></td>
<td></td>
<td></td>
<td>5.5.3</td>
</tr>
</tbody>
</table>

```plaintext
{ Begin Patient Result

[ PID ]

[ PD1 ]

[ { NK1 } ]

[ { NTE } ]

[ PV1 ]

[ PV2 ]

[ ORC ]

OBR

[ { NTE } ]

{ OBX }

[ { NTE } ]

[ CTI ]

{ Close Patient Result
```

{ Close Result
```
## QPD Input Parameter Specification

<table>
<thead>
<tr>
<th>Field Seq</th>
<th>ColName</th>
<th>Key / Search</th>
<th>Sort</th>
<th>LEN</th>
<th>DT</th>
<th>Opt</th>
<th>R P / #</th>
<th>Match Op</th>
<th>TBL#</th>
<th>Segmen t Field Name</th>
<th>Service Identifier Code</th>
<th>Element Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>MessageQueryName</td>
<td>CE</td>
<td>R</td>
<td>60</td>
<td>CE</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>QueryTag</td>
<td>ST</td>
<td>R</td>
<td>32</td>
<td>ST</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>WhatData</td>
<td>CE</td>
<td>O</td>
<td>Y</td>
<td>0048</td>
<td>QPD.9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>ServiceCode</td>
<td>CE</td>
<td>O</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>DepartmentCode</td>
<td>CE</td>
<td>O</td>
<td>Y</td>
<td>NHIN_0001</td>
<td>QPD.10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>EarliestDataTime</td>
<td>TS</td>
<td>O</td>
<td>Y</td>
<td>OBR.7, OBX.14</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>LatestDataTime</td>
<td>TS</td>
<td>O</td>
<td>Y</td>
<td>OBR.7, OBX.14</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>TimeFilterDirection</td>
<td>ID</td>
<td>O</td>
<td>Y</td>
<td>NHIN_0002</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## QPD Input Parameter Field Description and Commentary

<table>
<thead>
<tr>
<th>Input Parameter</th>
<th>Comp Name</th>
<th>DT</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MessageQueryName</td>
<td>CE</td>
<td>Z01^Observation Reporting Query^NHIN Query Code</td>
<td></td>
</tr>
<tr>
<td>QueryTag</td>
<td>ST</td>
<td>Unique to each query message instance. This is used to relate the response back to its original query.</td>
<td></td>
</tr>
<tr>
<td>WhatData</td>
<td>CE</td>
<td>List specifying the broad type(s) of clinical data for which the query is being submitted. HL7 Table 0048 contains a list of the current codes. Of potential interest in the first phase of this project are at least: DEM – demographics RES – result ORD – order ROR – pharmacy prescription information</td>
<td></td>
</tr>
<tr>
<td>ServiceCode</td>
<td>CE</td>
<td>List of specific service codes for which data should be returned. For laboratory queries, this would include a list of LOINC codes. For pharmacy dispensing queries, this would include a list of NDC codes. If this value is left empty in the query, data for all service codes will be returned.</td>
<td></td>
</tr>
<tr>
<td>DepartmentCode</td>
<td>CE</td>
<td>List of departments from which data should be returned. These are broad department codes, such as CLINICAL LABORATORY, NURSING, RADIOLOGY, PHARMACY, etc. Refer to Table NHIN_0001 in Appendix B for a complete list of supported department codes.</td>
<td></td>
</tr>
<tr>
<td>EarliestDataTime</td>
<td>TS</td>
<td>Earliest date and time for returned data. If not valued, there is no restriction on how old the returned data may be.</td>
<td></td>
</tr>
<tr>
<td>LatestDataTime</td>
<td>TS</td>
<td>Latest date and time for returned data. If not valued, there is no restriction on how recent the returned data may be.</td>
<td></td>
</tr>
<tr>
<td>TimeFilterDirection</td>
<td>ID</td>
<td>EARLIEST - if the filter on returned number of results is applied, then return the earliest data LATEST - if the filter on returned number of results is applied, then return the most recent data If not valued, the server system decides how to apply the filter on the number of returned results</td>
<td></td>
</tr>
</tbody>
</table>

## RCP Response Control Parameter Field Description and Commentary

<table>
<thead>
<tr>
<th>Input Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MessageQueryName</td>
<td>Z01^Observation Reporting Query^NHIN Query Code</td>
</tr>
<tr>
<td>QueryTag</td>
<td>Unique to each query message instance. This is used to relate the response back to its original query.</td>
</tr>
<tr>
<td>WhatData</td>
<td>List specifying the broad type(s) of clinical data for which the query is being submitted. HL7 Table 0048 contains a list of the current codes. Of potential interest in the first phase of this project are at least: DEM – demographics RES – result ORD – order ROR – pharmacy prescription information</td>
</tr>
<tr>
<td>ServiceCode</td>
<td>List of specific service codes for which data should be returned. For laboratory queries, this would include a list of LOINC codes. For pharmacy dispensing queries, this would include a list of NDC codes. If this value is left empty in the query, data for all service codes will be returned.</td>
</tr>
<tr>
<td>DepartmentCode</td>
<td>List of departments from which data should be returned. These are broad department codes, such as CLINICAL LABORATORY, NURSING, RADIOLOGY, PHARMACY, etc. Refer to Table NHIN_0001 in Appendix B for a complete list of supported department codes.</td>
</tr>
<tr>
<td>EarliestDataTime</td>
<td>Earliest date and time for returned data. If not valued, there is no restriction on how old the returned data may be.</td>
</tr>
<tr>
<td>LatestDataTime</td>
<td>Latest date and time for returned data. If not valued, there is no restriction on how recent the returned data may be.</td>
</tr>
<tr>
<td>TimeFilterDirection</td>
<td>EARLIEST - if the filter on returned number of results is applied, then return the earliest data LATEST - if the filter on returned number of results is applied, then return the most recent data If not valued, the server system decides how to apply the filter on the number of returned results</td>
</tr>
<tr>
<td>Field Seq</td>
<td>Name</td>
</tr>
<tr>
<td>-----------</td>
<td>------------------</td>
</tr>
<tr>
<td>1</td>
<td>Query Priority</td>
</tr>
<tr>
<td>2</td>
<td>Quantity Limited Request</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

No other RCP fields should be valued.

5.1.2 Observation Reporting Query HL7 Message Description

The QPD segment defines the type of data, amount of data, and reporting time frame of the data being requested. The PID segment defines the patient for whom data is being requested.

<table>
<thead>
<tr>
<th>HL7 Segment</th>
<th>Repeat</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSH</td>
<td>N</td>
<td>standard HL7 message header</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MSH.10 (MESSAGE CONTROL ID) should contain a unique message identifier. When the requested results and reports are sent back to the CLIENT in the response message, the unique message identifier value will be echoed back in field MSA.2 (MESSAGE CONTROL ID).</td>
</tr>
<tr>
<td>QPD</td>
<td>N</td>
<td>Query Parameter Definition – defines type of reports, results, and/or observations to return</td>
</tr>
<tr>
<td>PID</td>
<td>N</td>
<td>Patient identification attributes – defines patient whose reports, results, and/or observations are to be returned</td>
</tr>
<tr>
<td></td>
<td></td>
<td>We strongly encourage NHIN CLIENT systems to send as much PID data as possible, including patient middle name, alias patient names, all known address information, and all known identification numbers. NHIN servers are free to use as many of these attributes as possible in order to identify the target person in their database(s).</td>
</tr>
<tr>
<td>RCP</td>
<td>N</td>
<td>Response Control Parameters – max number of reports to return and definition of “immediate” versus “deferred” query response</td>
</tr>
</tbody>
</table>

5.1.3 Observation Reporting Query Response Message

This response message is based on the standard HL7 ORU^R01 message. It contains one <RSP_Z01> node for each registration for which results and/or reports exist. Each <RSP_Z01> node contains exactly one <RSP_Z01.PATIENT> node, which contains exactly one <PID> node.

Each <RSP_Z01> node also contains one or more <RSP_Z01.ORDER_ObservATION> nodes. Each <RSP_Z01.ORDER_ObservATION> node represents a single result battery or text.
The following table lists the HL7 segments that one can currently expect in the NHIN query response. Note that the HL7 specification defines additional segments for this message type; but that NHIN queries do not return those optional segments at this point in time. In fact, most of those optional segments will never be returned in NHIN query responses.

<table>
<thead>
<tr>
<th>HL7 Segment</th>
<th>Repeat</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSH</td>
<td>N</td>
<td>Standard HL7 message header</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MSH.10 (MESSAGE CONTROL ID) should contain a unique message identifier. When the requested results and reports are sent back to the CLIENT in the response message, the unique message identifier value will be echoed back in field MSA.2 (MESSAGE CONTROL ID).</td>
</tr>
<tr>
<td>MSA</td>
<td>N</td>
<td>The MSA (Message Acknowledgment) segment confirms that report was produced and echoes back the original query message's MESSAGE CONTROL ID so that the response can be matched up with the request.</td>
</tr>
<tr>
<td>ERR</td>
<td>N</td>
<td>Defines error information if the query response was an error rather than the expected query results.</td>
</tr>
<tr>
<td>QAK</td>
<td>N</td>
<td>HL7 Query Acknowledgement – not used, but included per HL7.</td>
</tr>
<tr>
<td>QPD</td>
<td>N</td>
<td>Query Parameter Definition – copy of query parameters sent to the query server.</td>
</tr>
<tr>
<td>PID</td>
<td>Y</td>
<td>Patient registration attributes. One PID is returned for each registration matching the query PID attributes. Each report, result, and/or observation is attached to exactly one PID registration in the query response.</td>
</tr>
<tr>
<td>OBR</td>
<td>Y</td>
<td>Observation Header - Each OBR represents one test panel, report, or similar unit/group of observable data returned from the query. For example, an OBR could represent a CBC panel, a surgical pathology report, an x-ray report, a panel of vital signs, a single culture, etc.</td>
</tr>
<tr>
<td>NTE</td>
<td>Y</td>
<td>Text comments about the data in an OBR or OBX.</td>
</tr>
<tr>
<td>OBX</td>
<td>Y</td>
<td>A single reportable value or observation. This might be as concise as a number plus its units, or as long as an entire, dictated text report. Refer to HL7 Chapter 7 (Observation Reporting) for a more detailed description of the OBR, NTE, and OBX HL7 segments used to represent clinical reports, results, and observations.</td>
</tr>
</tbody>
</table>

Note that the XML format for sending HL7 results requires some additional “grouping” tags that segregate the registration data from the reports. Our sample messages demonstrate this grouping.
5.1.4 Complete Example

Sample Query:

```xml
<QBP_Z01 xmlns="urn:hl7-org:v2xml">
  <MSH>
    <MSH.1/>
    <MSH.2/>
    <MSH.3>
      <HD.1>Query Application Name</HD.1>
    </MSH.3>
    <MSH.4>
      <HD.1>ST ELSEWHERE HOSPITAL</HD.1>
    </MSH.4>
    <MSH.5>
      <HD.1>Target ISB</HD.1>
    </MSH.5>
    <MSH.6>
      <HD.1>Target SNO Name</HD.1>
    </MSH.6>
    <MSH.7>
      <TS.1>200506171410</TS.1>
    </MSH.7>
    <MSH.9>
      <MSG.1>QBP</MSG.1>
      <MSG.2>Z01</MSG.2>
      <MSG.3>QBP_Z01</MSG.3>
    </MSH.9>
    <MSH.10>123456789</MSH.10>
    <MSH.11>
      <PT.1>P</PT.1>
    </MSH.11>
    <MSH.12>
      <VID.1>2.4</VID.1>
    </MSH.12>
  </MSH>
  <QPD>
    <QPD.1>
      <CE.1>Z01</CE.1>
      <CE.2>Observation Reporting Query</CE.2>
      <CE.3>NHIN Query Code</CE.3>
    </QPD.1>
    <QPD.2>Q123456</QPD.2>
    <QPD.3>
      <CE.1>RES</CE.1>
      <CE.2>result</CE.2>
      <CE.3>0048</CE.3>
    </QPD.3>
    <QPD.5>
      <CE.1>LABORATORY</CE.1>
      <CE.2>Laboratory</CE.2>
      <CE.3>NHIN_0001</CE.3>
    </QPD.5>
    <QPD.6>
      <TS.1>19980810</TS.1>
    </QPD.6>
    <QPD.8>LATEST</QPD.8>
  </QPD>
  <PID>
    <PID.1/>
    <PID.2/>
    <PID.3/>
    <PID.5>
      <XPN.1>
        <FN.1>THOMPSON</FN.1>
      </XPN.1>
    </PID.5>
  </PID>
</QBP_Z01>
```
Sample Response:

```xml
<RSP_Z01 xmlns="urn:hl7-org:v2xml">
  <MSH>
    <MSH.1/>
    <MSH.2/>
    <MSH.3>
      <HD.1>Target ISB</HD.1>
    </MSH.3>
    <MSH.4>
      <HD.1>Target SNO Name</HD.1>
    </MSH.4>
    <MSH.5>
      <HD.1>Query Application Name</HD.1>
    </MSH.5>
    <MSH.6>
      <HD.1>ST ELSEWHERE HOSPITAL</HD.1>
    </MSH.6>
    <MSH.7>
      <TS.1>20051024074506</TS.1>
    </MSH.7>
    <MSG.1>RSP</MSG.1>
    <MSG.2>Z01</MSG.2>
    <MSG.3>RSP_Z01</MSG.3>
  </MSH>
</RSP_Z01>
```
5.2 Patient Identities Query Message
A Patient Identities Query identifies a person of interest (person attributes are specified in an HL7 PID segment) and requests the NHIN server to find all of the known patient registrations for that person, across that SNO. The SOAP request message is an HL7 Query By Parameter (QBP) message with event code Z02. It contains HL7’s MSH, QPD, PID, and RCP segments, in that order. The response message will contain one PID segment for each registration found in one of the SNO’s Master Patient Index tables.

5.2.1 Patient Identities Query Conformance Statement

<table>
<thead>
<tr>
<th>Query Statement ID:</th>
<th>Z02</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type:</td>
<td>Query</td>
</tr>
<tr>
<td>Query Name:</td>
<td>Patient Identities Query</td>
</tr>
<tr>
<td>Query Trigger (= MSH-9):</td>
<td>QBP^Z02^QBP_Z02</td>
</tr>
<tr>
<td>Query Mode:</td>
<td>Both</td>
</tr>
<tr>
<td>Response Trigger (= MSH-9):</td>
<td>RSP^Z02^RSP_Z02</td>
</tr>
<tr>
<td>Query Characteristics:</td>
<td>Patient will be identified by searching the NHIN server's Master Patient Index (MPI) or MPIs based on person attributes defined in the query's PID segment. The response will contain one PID segment for each registration instance found.</td>
</tr>
<tr>
<td>Purpose:</td>
<td>Queries an NHIN server for person demographics. Input is list of known person identifiers and attributes. Output is the list of registration instances found for the target person.</td>
</tr>
<tr>
<td>Response Characteristics:</td>
<td>Demographics and identifiers are returned in standard PID segments, one per registration instance found.</td>
</tr>
<tr>
<td>Based on Segment Pattern:</td>
<td>A19</td>
</tr>
</tbody>
</table>
### Query Grammar Pattern

<table>
<thead>
<tr>
<th>QBP(^Z02^)QBP(_Z02)</th>
<th>Query Grammar:</th>
<th>Group Control</th>
<th>Comment</th>
<th>Support Indicator</th>
<th>Sec Ref</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSH</td>
<td>Message Header</td>
<td></td>
<td></td>
<td></td>
<td>2.16.9</td>
</tr>
<tr>
<td>QPD</td>
<td>Query Parameter Definition</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PID</td>
<td>Patient Identification</td>
<td></td>
<td></td>
<td></td>
<td>3.4.2</td>
</tr>
<tr>
<td>RCP</td>
<td>Response Control Parameter</td>
<td></td>
<td></td>
<td></td>
<td>5.5.5</td>
</tr>
</tbody>
</table>

### Response Grammar Pattern

<table>
<thead>
<tr>
<th>RSP(^Z02^)RSP(_Z02)</th>
<th>Response Grammar:</th>
<th>Group Control</th>
<th>Comment</th>
<th>Support Indicator</th>
<th>Sec Ref</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSH</td>
<td>Message Header</td>
<td></td>
<td></td>
<td></td>
<td>2.16.9</td>
</tr>
<tr>
<td>MSA</td>
<td>Message Acknowledgement</td>
<td></td>
<td></td>
<td></td>
<td>2.16.8</td>
</tr>
<tr>
<td>[ERR]</td>
<td>Error</td>
<td></td>
<td></td>
<td></td>
<td>2.16.5</td>
</tr>
<tr>
<td>QAK</td>
<td>QueryAcknowledgement</td>
<td></td>
<td></td>
<td></td>
<td>5.5.2</td>
</tr>
<tr>
<td>QPD</td>
<td>Query Parameter Definition</td>
<td></td>
<td></td>
<td></td>
<td>5.5.3</td>
</tr>
<tr>
<td>{</td>
<td>QUERY_RESPONSE</td>
<td>Begin PID Group</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[</td>
<td>]</td>
<td>Begin Patient Result</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PID</td>
<td>Patient Identification</td>
<td></td>
<td></td>
<td></td>
<td>3.4.2</td>
</tr>
<tr>
<td>[ PD1 ]</td>
<td>Additional Demographics</td>
<td></td>
<td></td>
<td></td>
<td>3.4.10</td>
</tr>
<tr>
<td>[ { NK1 } ]</td>
<td>Next of Kin/Associated Parties</td>
<td></td>
<td></td>
<td></td>
<td>3.3.5</td>
</tr>
<tr>
<td>[ { NTE } ]</td>
<td>Notes and comments</td>
<td></td>
<td></td>
<td></td>
<td>2.16.10</td>
</tr>
<tr>
<td>]</td>
<td>Close PID Group</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>Close Patient Result</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Only the PID segment is currently valued, but other segments might be valued in future releases.
**QPD Input Parameter Specification**

<table>
<thead>
<tr>
<th>Field Seq</th>
<th>ColName</th>
<th>Key / Sort</th>
<th>LEN</th>
<th>DT</th>
<th>Opt</th>
<th>R P / #</th>
<th>Match Op</th>
<th>TBL#</th>
<th>Segment Field Name</th>
<th>Service Identifier Code</th>
<th>Element Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>MessageQueryNa me</td>
<td></td>
<td>60</td>
<td>CE</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Message Query Name</td>
</tr>
<tr>
<td>2</td>
<td>QueryTag</td>
<td></td>
<td>32</td>
<td>ST</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Query Tag</td>
</tr>
</tbody>
</table>

**QPD Input Parameter Field Description and Commentary**

<table>
<thead>
<tr>
<th>Input Parameter</th>
<th>Component Name</th>
<th>DT</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MessageQueryName</td>
<td>CE</td>
<td>Z02^Patient Identities Query^NHIN Query Code</td>
<td></td>
</tr>
<tr>
<td>QueryTag</td>
<td>ST</td>
<td>Unique to each query message instance. This is used to relate the response back to its original query.</td>
<td></td>
</tr>
</tbody>
</table>

**RCP Response Control Parameter Field Description and Commentary**

<table>
<thead>
<tr>
<th>Field Seq</th>
<th>Name</th>
<th>Component Name</th>
<th>LEN</th>
<th>DT</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Query Priority</td>
<td></td>
<td>1</td>
<td>ID</td>
<td>(D)ferred or (I)mmediate. If the query is a “D” (deferred) query, the query client will receive an immediate ACK back from the query server. The actual query results will be returned asynchronously, in a separate SOAP conversation. If the query is an &quot;I&quot; (immediate) query, the query client will receive the actual query results back in the current SOAP conversation.</td>
</tr>
<tr>
<td>2</td>
<td>Quantity Limited Request</td>
<td></td>
<td>10</td>
<td>CQ</td>
<td>Number of units (specified by the following component) that will be returned in each increment of the response. If no value is given, there is no limit on the number of results and reports returned.</td>
</tr>
<tr>
<td></td>
<td>Units</td>
<td></td>
<td>CE</td>
<td></td>
<td>CHaracters, Lines, PaGes, or RecorDds. Should be RD, when valued.</td>
</tr>
</tbody>
</table>

No other RCP fields should be valued.
5.2.2 Patient Identities Query Message Description

<table>
<thead>
<tr>
<th>HL7 Segment</th>
<th>Repeat</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSH</td>
<td>N</td>
<td>standard HL7 message header</td>
</tr>
<tr>
<td>QPD</td>
<td>N</td>
<td>Query Parameter Definition – required by HL7 standard, but not used</td>
</tr>
<tr>
<td>PID</td>
<td>N</td>
<td>Patient identification attributes</td>
</tr>
<tr>
<td>RCP</td>
<td>N</td>
<td>Response Control Parameters – max number of reports to return and definition of “immediate” versus “deferred” query response</td>
</tr>
</tbody>
</table>

5.2.3 Patient Identities Response Message Format

This response contains a list of HL7 PID segments, one for each patient registration that matches the attributes specified in the query. In the case where no matches are found, the return message contains no PID segments. “No matches” is not considered an error condition.

The response is an HL7 ADT Response ADR message with event code A19. It contains only the HL7 MSH, MSA, and PID segments, in that order. There is one PID segment per registration match found.

<table>
<thead>
<tr>
<th>HL7 Segment</th>
<th>Repeat</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSH</td>
<td>N</td>
<td>standard HL7 message header</td>
</tr>
<tr>
<td>MSA</td>
<td>N</td>
<td>HL7 message acknowledgment. It confirms that registration search was performed without error. It echoes back the Patient Identities Query message’s MESSAGE CONTROL ID so that the response can be matched up with the request.</td>
</tr>
<tr>
<td>QAK</td>
<td>N</td>
<td>HL7 query acknowledgement</td>
</tr>
<tr>
<td>QPD</td>
<td>N</td>
<td>Query Parameter Definition – required by HL7 standard, but not used</td>
</tr>
<tr>
<td>PID</td>
<td>Y</td>
<td>One PID segment is returned per registration match. Each PID segment represents a single registration instance found within the target SNO’s database(s). The NHIN server is free to populate as much of the PID segment as it wants to; however, the required values are an institutional medical record number along with its assigning authority. The institutional medical record number must be in &lt;PID.3&gt;. The medical record number itself will be in the child node &lt;CX.1&gt;. Child Node &lt;CX.5&gt; will contain the value “MR” signifying that the identifier is a medical record number. Child Node &lt;CX.6&gt; must contain the agreed upon institutional identifier for the institution at which the patient is registered. Each PID XML node must be a child of an HL7 RSP_Z02.QUERY_RESPONSE node. In other words, each &lt;RSP_Z02.PATIENT&gt; node contains exactly one &lt;PID&gt; node, but there may be any number of &lt;RSP_Z02.PATIENT&gt; nodes.</td>
</tr>
<tr>
<td>RCP</td>
<td>N</td>
<td>Response Control Parameters – max number of reports to return and definition of “immediate” versus “deferred” query response</td>
</tr>
</tbody>
</table>
Sample Query:

```xml
<QBP_Z02 xmlns="urn:hl7-org:v2xml">
  <MSH>
    <MSH.1/>
    <MSH.2/>
    <MSH.3>
      <HD.1>Query Application Name</HD.1>
    </MSH.3>
    <MSH.4>
      <HD.1>ST ELSEWHERE HOSPITAL</HD.1>
    </MSH.4>
    <MSH.5>
      <HD.1>Target ISB</HD.1>
    </MSH.5>
    <MSH.6>
      <HD.1>Target SNO Name</HD.1>
    </MSH.6>
    <MSH.7>
      <TS.1>200506171410</TS.1>
    </MSH.7>
    <MSH.9>
      <MSG.1>QBP</MSG.1>
      <MSG.2>Z02</MSG.2>
      <MSG.3>QBP_Z02</MSG.3>
    </MSH.9>
    <MSH.10>987654321</MSH.10>
    <MSH.11>
      <PT.1>P</PT.1>
    </MSH.11>
    <MSH.12>
      <VID.1>2.4</VID.1>
    </MSH.12>
  </MSH>
  <QPD>QPD.
  </QPD>
  <PID>
    <PID.1/>
    <PID.2/>
    <PID.3/>
    <PID.5>
      <XPN.1>
        <FN.1>THOMPSON</FN.1>
      </XPN.1>
      <XPN.2>MARK</XPN.2>
      <XPN.3>Q</XPN.3>
    </PID.5>
    <PID.5>
      <XPN.1>
        <FN.1>AliasLastName</FN.1>
      </XPN.1>
      <XPN.2>AliasFirstName</XPN.2>
      <XPN.3>AliasMiddleName</XPN.3>
    </PID.5>
    <PID.7>
      <TS.1>19090630</TS.1>
    </PID.7>
    <PID.8>M</PID.8>
    <PID.11>
      <XAD.1>
        <SAD.1>28W 10TH Street</SAD.1>
      </XAD.1>
    </PID.11>
  </PID>
</QBP_Z02>
```
Sample Response:

```xml
<RSP_Z02 xmlns="urn:hl7-org:v2xml">
  <MSH>
    <MSH.1/>
    <MSH.2/>
    <MSH.3>
      <HD.1>Target ISB</HD.1>
    </MSH.3>
    <MSH.4>
      <HD.1>Target SNO Name</HD.1>
    </MSH.4>
    <MSH.5>
      <HD.1>Query Application Name</HD.1>
    </MSH.5>
    <MSH.6>
      <HD.1>ST ELSEWHERE HOSPITAL</HD.1>
    </MSH.6>
    <MSH.7>
      <TS.1>20051024074505</TS.1>
    </MSH.7>
    <MSH.9>
      <MSG.1>QBP</MSG.1>
      <MSG.2>Z02</MSG.2>
      <MSG.3>QBP_Z02</MSG.3>
    </MSH.9>
    <MSH.10>2</MSH.10>
    <MSH.11>
      <PT.1>P</PT.1>
    </MSH.11>
    <MSH.12>
      <VID.1>2.4</VID.1>
    </MSH.12>
  </MSH>
  <MSA>
    <MSA.1>AA</MSA.1>
    <MSA.2>123456789</MSA.2>
  </MSA>
  <QAK/>
  <QPD>
    <QPD.1/>
    <QPD.2/>
  </QPD>
  <RSP_Z02.QUERY_RESPONSE>
    <PID>
      <PID.1/>
    </PID>
  </RSP_Z02.QUERY_RESPONSE>
</RSP_Z02>
```
<RSP_Z02.QUERY_RESPONSE>
<PID>
  <PID.1/>
  <PID.2/>
  <PID.3/>
  <CX.1>MADEUP-8</CX.1>
  <CX.4>
    <HD.1>ST ELSEWHERE HOSPITAL Medical Record Numbers</HD.1>
    <HD.2>MEDICAL RECORD NUMBER</HD.2>
    <HD.3>ST ELSEWHERE HOSPITAL</HD.3>
  </CX.4>
  <CX.5>MR</CX.5>
  <CX.6>
    <HD.1>ST ELSEWHERE HOSPITAL</HD.1>
  </CX.6>
</PID>
</RSP_Z02.QUERY_RESPONSE>
5.3 Access History Query – Reporting NHIN Accesses Made and Attempted

Access History Query requests data from the SNO’s log of access attempts. This information could be used to obtain data about whose information a particular user has been accessing, which users have been accessing a particular person’s data, or a combination of those conditions. HL7 supports this type of query with its QBP/RTB pattern (query by parameter and tabular response). The QPD elements can also be used to limit the returned access log data by time. The RCP elements can limit the response data to a maximum number of rows.

5.3.1 Access History Query Conformance Statement

<table>
<thead>
<tr>
<th>Query Statement ID:</th>
<th>Z03</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type:</td>
<td>Query</td>
</tr>
<tr>
<td>Query Name:</td>
<td>Access History Query</td>
</tr>
<tr>
<td>Query Trigger (= MSH-9):</td>
<td>QBP^Z03^QBP_Z03</td>
</tr>
<tr>
<td>Query Mode:</td>
<td>Both</td>
</tr>
<tr>
<td>Response Trigger (= MSH-9):</td>
<td>RTB^Z03^RTB_Z03</td>
</tr>
<tr>
<td>Query Characteristics:</td>
<td>If a patient is specified, the patient will be identified by searching the NHIN server’s Master Patient Index (MPI) or MPIs based on person attributes defined in the query PID segment and only accesses to that patient’s data will be returned.</td>
</tr>
<tr>
<td>Purpose:</td>
<td>Queries an NHIN server for data from the patient data access log.</td>
</tr>
<tr>
<td>Response Characteristics:</td>
<td>Tabular data response from the patient data access log. Each logical row represents a single patient access through the NHIN.</td>
</tr>
</tbody>
</table>

### Query Grammar Pattern

<table>
<thead>
<tr>
<th>QBP^Z03^QBP_Z03</th>
<th>Query Grammar:</th>
<th>Group Control</th>
<th>Comment</th>
<th>Support Indicator</th>
<th>Sec Ref</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSH</td>
<td>Message Header</td>
<td></td>
<td></td>
<td></td>
<td>2.16.9</td>
</tr>
<tr>
<td>QPD</td>
<td>Query Parameter Definition</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PID</td>
<td>Patient Identification</td>
<td></td>
<td></td>
<td></td>
<td>3.4.2</td>
</tr>
<tr>
<td>RCP</td>
<td>Response Control Parameter</td>
<td></td>
<td></td>
<td></td>
<td>5.5.5</td>
</tr>
</tbody>
</table>

### Response Grammar Pattern

<table>
<thead>
<tr>
<th>RTB^Z03^RTB_Z03</th>
<th>Response Grammar:</th>
<th>Group Control</th>
<th>Comment</th>
<th>Support Indicator</th>
<th>Sec Ref</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSH</td>
<td>Message Header</td>
<td></td>
<td></td>
<td></td>
<td>2.16.9</td>
</tr>
<tr>
<td>MSA</td>
<td>Message Acknowledgement</td>
<td></td>
<td></td>
<td></td>
<td>2.16.8</td>
</tr>
<tr>
<td>[ERR]</td>
<td>Error</td>
<td></td>
<td></td>
<td></td>
<td>2.16.5</td>
</tr>
<tr>
<td>QAK</td>
<td>QueryAcknowledgement</td>
<td></td>
<td></td>
<td></td>
<td>5.5.2</td>
</tr>
<tr>
<td>QPD</td>
<td>Query Parameter Definition</td>
<td></td>
<td></td>
<td></td>
<td>5.5.3</td>
</tr>
<tr>
<td>[</td>
<td>ROW_DEFINITIO</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### QPD Input Parameter Specification

<table>
<thead>
<tr>
<th>Field Seq</th>
<th>ColName</th>
<th>LEN</th>
<th>DT</th>
<th>Key / Search</th>
<th>Op</th>
<th>R / #</th>
<th>Match Op</th>
<th>TBL#</th>
<th>Segment Field Name</th>
<th>Service Identifier Code</th>
<th>Element Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>MessageQueryName</td>
<td>60</td>
<td>CE</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Message Query Name</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>QueryTag</td>
<td>32</td>
<td>ST</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Query Tag</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>AccessingUser</td>
<td>100</td>
<td>XCN</td>
<td>O</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Accessing User</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>EarliestAccess</td>
<td>26</td>
<td>TS</td>
<td>O</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Earliest Access</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>LatestAccess</td>
<td>26</td>
<td>TS</td>
<td>O</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Latest Access</td>
<td></td>
</tr>
</tbody>
</table>

### QPD Input Parameter Field Description and Commentary

<table>
<thead>
<tr>
<th>Input Parameter</th>
<th>Comp. Name</th>
<th>DT</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MessageQueryName</td>
<td>CE</td>
<td>Z03^Access History Query^NHIN Query Code</td>
<td></td>
</tr>
<tr>
<td>QueryTag</td>
<td>ST</td>
<td>Unique to each query message instance. This is used to relate the response back to its original query.</td>
<td></td>
</tr>
<tr>
<td>AccessingUser</td>
<td>XCN</td>
<td>Specifies the user whose accesses are to be returned. If this is left empty, then the response is not limited to accesses made by a single user.</td>
<td></td>
</tr>
<tr>
<td>Earliest Access</td>
<td>TS</td>
<td>If specified, this indicates the date and time of the earliest access log entry of interest.</td>
<td></td>
</tr>
<tr>
<td>Latest Access</td>
<td>TS</td>
<td>If specified, this indicates the date and time of the latest access log entry of interest.</td>
<td></td>
</tr>
</tbody>
</table>
### RCP Response Control Parameter Field Description and Commentary

<table>
<thead>
<tr>
<th>Field Seq</th>
<th>Name</th>
<th>Component Name</th>
<th>LEN</th>
<th>DT</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Query Priority</td>
<td></td>
<td>1</td>
<td>ID</td>
<td>(D)ejered or (I)mediate. If the query is a &quot;D&quot; (deferred) query, the query client will receive an immediate ACK back from the query server. The actual query results will be returned asynchronously, in a separate SOAP conversation. If the query is an &quot;I&quot; (immediate) query, the query client will receive the actual query results back in the current SOAP conversation.</td>
</tr>
<tr>
<td>2</td>
<td>Quantity Limited Request</td>
<td></td>
<td>10</td>
<td>CQ</td>
<td>Number of units (specified by the following component) that will be returned in each increment of the response. If no value is given, there is no limit on the number of results and reports returned.</td>
</tr>
</tbody>
</table>

No other RCP fields should be valued.

### Input/Output Specification: Virtual Table

<table>
<thead>
<tr>
<th>ColName</th>
<th>Key/ Search</th>
<th>Sort</th>
<th>LEN</th>
<th>TYPE</th>
<th>Opt</th>
<th>Rep</th>
<th>Match Op</th>
<th>TBL</th>
<th>Segment Field Name</th>
<th>Service Identifier Code</th>
<th>Element Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>QueryUser</td>
<td>100</td>
<td></td>
<td>XCN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>QueryUser</td>
<td></td>
</tr>
<tr>
<td>QueryURL</td>
<td>100</td>
<td></td>
<td>ST</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>QueryURL</td>
<td></td>
</tr>
<tr>
<td>QueryTag</td>
<td>40</td>
<td></td>
<td>ST</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>QueryTag</td>
<td></td>
</tr>
<tr>
<td>QueryBegin</td>
<td>26</td>
<td></td>
<td>TS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>QueryBegin</td>
<td></td>
</tr>
<tr>
<td>QueryEnd</td>
<td>26</td>
<td></td>
<td>TS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>QueryEnd</td>
<td></td>
</tr>
<tr>
<td>QueryServiceCode</td>
<td>200</td>
<td></td>
<td>CE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>QueryServiceCode</td>
<td></td>
</tr>
<tr>
<td>QueryDepartmentCode</td>
<td>200</td>
<td></td>
<td>CE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>QueryDepartmentCode</td>
<td></td>
</tr>
<tr>
<td>Patient</td>
<td>200</td>
<td></td>
<td>XCN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Patient</td>
<td></td>
</tr>
</tbody>
</table>

### Virtual Table Field Description and Commentary

<table>
<thead>
<tr>
<th>ColName</th>
<th>Component Name</th>
<th>DT</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>QueryUser</td>
<td>XCN</td>
<td></td>
<td>Defines user who submitted the NHIN query.</td>
</tr>
<tr>
<td>QueryURL</td>
<td>ST</td>
<td></td>
<td>URL from which the query was submitted.</td>
</tr>
<tr>
<td>QueryTag</td>
<td>ST</td>
<td></td>
<td>HL7 query name for the submitted query.</td>
</tr>
<tr>
<td>QueryBegin</td>
<td>TS</td>
<td></td>
<td>Date and time the query was received by the NHIN server.</td>
</tr>
<tr>
<td>QueryEnd</td>
<td>TS</td>
<td></td>
<td>Date and time the query was completed by the NHIN server.</td>
</tr>
<tr>
<td>QueryServiceCode</td>
<td>CE</td>
<td></td>
<td>List of types of data the query asked for. This comes from the QPD.4 (ServiceCode) value specified in the query</td>
</tr>
<tr>
<td>QueryDepartmentCode</td>
<td>CE</td>
<td></td>
<td>List of departments from which data was being requested. This comes from QPD.5 (DepartmentCode).</td>
</tr>
</tbody>
</table>
5.3.2 Access History Query HL7 Message Segments

<table>
<thead>
<tr>
<th>HL7 Segment</th>
<th>Repeat</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSH</td>
<td>N</td>
<td>standard HL7 message header</td>
</tr>
<tr>
<td>QPD</td>
<td>N</td>
<td>Query Parameter Definition – can limit query to a range of access times and /or accesses by a specific user</td>
</tr>
<tr>
<td>PID</td>
<td>N</td>
<td>Patient identification attributes for patient of interest. Can be left empty to get all accesses by a specific user</td>
</tr>
<tr>
<td>RCP</td>
<td>N</td>
<td>Response Control Parameters – max number of reports to return and definition of “immediate” versus “deferred” query response</td>
</tr>
</tbody>
</table>

5.3.3 Access History Query Response Message Format

This response contains a list of the virtual “rows”, one per user access returned from the user access log. “No matches” is **not** considered an error condition. No rows are simply returned.

<table>
<thead>
<tr>
<th>HL7 Segment</th>
<th>Repeat</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSH</td>
<td>N</td>
<td>standard HL7 message header</td>
</tr>
<tr>
<td>MSA</td>
<td>N</td>
<td>HL7 message acknowledgment. It confirms that registration search was performed without error. It echoes back the Patient Identities Query message's MESSAGE CONTROL ID so that the response can be matched up with the request.</td>
</tr>
<tr>
<td>QAK</td>
<td>N</td>
<td>HL7 query acknowledgement</td>
</tr>
<tr>
<td>QPD</td>
<td>N</td>
<td>Query Parameter Definition – required by HL7 standard, but not used</td>
</tr>
<tr>
<td>RDF</td>
<td>N</td>
<td>Defines the list of “virtual columns” returned by this query</td>
</tr>
<tr>
<td>RDT</td>
<td>Y</td>
<td>One row data segment for each row of data returned; that is, one for each user access returned</td>
</tr>
</tbody>
</table>

5.3.4 Sample Access History Message Dialogue

**Sample Query:**

```xml
<QBP_Z03 xmlns="urn:hl7-org:v2xml">
  <MSH>
    <MSH.1/>
    <MSH.2/>
    <MSH.3>
      <HD.1>Query Application Name</HD.1>
    </MSH.3>
    <MSH.4>
      <HD.1>ST ELSEWHERE HOSPITAL</HD.1>
    </MSH.4>
    <MSH.5>
      <HD.1>Target ISB</HD.1>
    </MSH.5>
    <MSH.6>
      <HD.1>Target SNO Name</HD.1>
    </MSH.6>
    <TS.1>200506171410</TS.1>
  </MSH>
</QBP_Z03>
```
Sample Response:

<RTB_Z03 xmlns="urn:hl7-org:v2xml">
  <MSH>
    <MSH.1/>
    <MSH.2/>
    <MSH.3>
      <HD.1>Target ISB</HD.1>
    </MSH.3>
    <MSH.4>
      <HD.1>Target SNO Name</HD.1>
    </MSH.4>
    <MSH.5>
      <HD.1>Query Application Name</HD.1>
    </MSH.5>
    <MSH.6>
      <HD.1>ST ELSEWHERE HOSPITAL</HD.1>
    </MSH.6>
    <MSH.7>
      <TS.1>20051024074505</TS.1>
    </MSH.7>
    <MSH.9>
      <MSG.1>RSP</MSG.1>
      <MSG.2>Z03</MSG.2>
      <MSG.3>RSP_Z03</MSG.3>
    </MSH.9>
    <MSH.10>2</MSH.10>
  </MSH>
  <MSA>
    <MSA.1>AA</MSA.1>
    <MSA.2>123456789</MSA.2>
  </MSA>
  <QAK/>
  <QPD>
    <QPD.1>
      <CE.1>Z03</CE.1>
      <CE.2>Access History Query</CE.2>
      <CE.3>NHIN Query Code</CE.3>
    </QPD.1>
    <QPD.2>Q987654321</QPD.2>
    <QPD.4>
      <TS.1>200602241030</TS.1>
    </QPD.4>
  </QPD>
</RTB_Z03.ROW_DEFINITION>

<RTB_Z03.ROW_DEFINITION>
  <RDF>
    <RDF.1>8</RDF.1>
    <RDF.2>
      <RCD.1>QueryUser</RCD.1>
      <RCD.2>XCN</RCD.2>
      <RCD.3>100</RCD.3>
    </RDF.2>
    <RDF.2>
      <RCD.1>QueryURL</RCD.1>
      <RCD.2>ST</RCD.2>
      <RCD.3>100</RCD.3>
    </RDF.2>
    <RDF.2>
      <RCD.1>QueryTag</RCD.1>
    </RDF.2>
  </RDF>
</RTB_Z03.ROW_DEFINITION>
<RCD.2>ST</RCD.2>
<RCD.3>40</RCD.3>

<RDF.2>
<RCD.1>QueryBegin</RCD.1>
<RCD.2>DT</RCD.2>
<RCD.3>26</RCD.3>
</RDF.2>

<RDF.2>
<RCD.1>QueryEnd</RCD.1>
<RCD.2>DT</RCD.2>
<RCD.3>26</RCD.3>
</RDF.2>

<RDF.2>
<RCD.1>QueryServiceCode</RCD.1>
<RCD.2>CE</RCD.2>
<RCD.3>200</RCD.3>
</RDF.2>

<RDF.2>
<RCD.1>QueryDepartmentCode</RCD.1>
<RCD.2>CE</RCD.2>
<RCD.3>200</RCD.3>
</RDF.2>

<RDF.2>
<RCD.1>Patient</RCD.1>
<RCD.2>XCN</RCD.2>
<RCD.3>200</RCD.3>
</RDF.2>

<RDT.1>
<XCN.1>JoeUser</XCN.1>
<XCN.2>
<FN.1>Smith</FN.1>
</XCN.2>
<XCN.3>Joseph</XCN.3>
<XCN.9>
<HD.1>ST ELSEWHERE HOSPITAL Users</HD.1>
<HD.2>USERID</HD.2>
<HD.3>ST ELSEWHERE HOSPITAL</HD.3>
</XCN.9>
<XCN.13>EI</XCN.13>
<XCN.14>
<HD.1>ST ELSEWHERE HOSPITAL</HD.1>
</XCN.14>
</RDT.1>

<RDT.2>https://www.myisb.org</RDT.2>

<RDT.3>Observation Reporting Query</RDT.3>

<TS.1>200602230831</TS.1>

<TS.1>200602230832</TS.1>

<XCN.1>123456-7</XCN.1>
<XCN.2>
<FN.1>Patient</FN.1>
</XCN.2>
<XCN.3>Example</XCN.3>
<XCN.9>
<HD.1>Brigadoon Emergency Care Patients</HD.1>
<HD.2>MR</HD.2>
<HD.3>Brigadoon Emergency Care</HD.3>
</XCN.9>
<XCN.13>MR</XCN.13>
<XCN.14>
6 Using Registration Data from the *Patient Identities Query*
Response in a Subsequent *Observation Reporting Query*

An NHIN query client may choose not to obtain the results, reports, and/or medications from all registrations, only from selected ones. To support this type of query, NHIN queries recognize the `<IdentifyPatient>` attribute within the query `<EvaluationSettings>`. When `<IdentifyPatient>` is set to “no”, the query must already contain one or more fully identified patient registrations, usually from the response to a previous *Patient Identities* query. Let us define how such a combination of queries and responses might look.

First, the client makes a *Patient Identities* query, just like the one described in section 5.2. For brevity, we do not repeat that sample query here. Refer to section 5.2.4 for that example. Suppose that the NHIN client now determines that it wants the results and reports stored for the MADEUP-8 medical record number rather than the results and reports stored for all identified medical record numbers. The NHIN client constructs the *Observation Report Query* listed below. Note that the PID segment included in this query message is identical to the PID segment returned in the *Patient Identities Query* response. The response to this query is like any other *Observation Reporting Query* response.

Sample Query:

```xml
<soapEnv:Body>
<nhin:EvaluationSettings>
  <nhin:IdentifyPatient>no</nhin:IdentifyPatient>
</nhin:EvaluationSettings>
<nhin:Query>
  <QBP_Z01 xmlns="urn:hl7-org:v2xml">
    <MSH>
      <MSH.1/>
      <MSH.2/>
      <MSH.3>
        <HD.1>Query Application Name</HD.1>
      </MSH.3>
      <MSH.4>
        <HD.1>ST ELSEWHERE HOSPITAL</HD.1>
      </MSH.4>
      <MSH.5>
        <HD.1>Target ISB</HD.1>
      </MSH.5>
      <MSH.6>
        <HD.1>Target SNO Name</HD.1>
      </MSH.6>
      <MSH.7>
        <TS.1>200506171410</TS.1>
      </MSH.7>
      <MSH.9>
        <MSG.1>QBP</MSG.1>
        <MSG.2>Z01</MSG.2>
        <MSG.3>QBP_Z01</MSG.3>
      </MSH.9>
      <MSH.10>123456789</MSH.10>
      <MSH.11>
        <PT.1>P</PT.1>
      </MSH.11>
      <MSH.12>
        <VID.1>2.4</VID.1>
      </MSH.12>
    </MSH>
  </QBP_Z01>
</soapEnv:Body>
```
<QPD.1>
  <CE.1>Z01</CE.1>
  <CE.2>Observation Reporting Query</CE.2>
  <CE.3>NHIN Query Code</CE.3>
</QPD.1>

<QPD.2>Q123456</QPD.2>

<QPD.3>
  <CE.1>RES</CE.1>
  <CE.2>result</CE.2>
  <CE.3>0048</CE.3>
</QPD.3>

<QPD.5>
  <CE.1>LABORATORY</CE.1>
  <CE.2>Laboratory</CE.2>
  <CE.3>NHIN_0001</CE.3>
</QPD.5>

<QPD.6>
  <TS.1>19980810</TS.1>
</QPD.6>

<QPD.8>LATEST</QPD.8>

</QPD>

<PID>
  <PID.1></PID.1>
  <PID.2></PID.2>
  <PID.3>
    <CX.1>MADEUP-8</CX.1>
    <CX.4>
      <HD.1>ST ELSEWHERE HOSPITAL Medical Record Numbers</HD.1>
      <HD.2>MEDICAL RECORD NUMBER</HD.2>
      <HD.3>ST ELSEWHERE HOSPITAL</HD.3>
    </CX.4>
    <CX.5>MR</CX.5>
    <CX.6>
      <HD.1>ST ELSEWHERE HOSPITAL</HD.1>
    </CX.6>
  </PID.3>
  <PID.5>
    <XPN.1>
      <FN.1>THOMSON</FN.1>
    </XPN.1>
    <XPN.2>MARCUS</XPN.2>
  </PID.5>
  <PID.7>
    <TS.1>19090630</TS.1>
  </PID.7>
  <PID.8>
    <XAD.3>BOSTON</XAD.3>
    <XAD.4>MA</XAD.4>
    <XAD.5>02171</XAD.5>
  </PID.8>
  <PID.11>
</PID>

<RCP>
  <RCP.1>I</RCP.1>
  <RCP.2>10</RCP.2>
</RCP>

</QBP_Z01>

</nhin:Query>
</soapenv:Body>
7  Response Containing Non-HL7 Data

Currently, the only non-HL7 response from an NHIN PatientDataQuery is the medication dispensing history. This data is returned in NCPDP Scripts 8.1 format. Complete documentation of that format can be found at “Medication History Standards,” part of part of The Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange.

Note that there are two <Response> nodes, one for a brief HL7 response and one for the NCPDP Scripts 8.1 data. If the query had requested both LABORATORY and MEDICATIONS DISPENSED data, the HL7-style <Response> node would have also contained the LABORATORY results data.

Sample Query:

```xml
<Query>
    <QBP_Z01 xmlns="urn:hl7-org:v2xml">
        <MSH>
            <MSH.1/>
            <MSH.2/>
            <MSH.3>
                <HD.1>Query Application Name</HD.1>
                <HD.1 ST ELSEWHERE HOSPITAL</HD.1>
                <HD.1>Target ISB</HD.1>
                <HD.1>Target SNO Name</HD.1>
                <TS.1>200506171410</TS.1>
                <MSG.1>QBP</MSG.1>
                <MSG.2>Z01</MSG.2>
                <MSG.3>QBP_Z01</MSG.3>
            </MSH.3>
            <MSH.4>
                <PT.1>P</PT.1>
            </MSH.4>
            <MSH.5>
                <VID.1>2.4</VID.1>
            </MSH.5>
            <MSH.6>123456789</MSH.6>
            <MSH.7>123456789</MSH.7>
            <MSH.8>123456789</MSH.8>
            <MSH.9>123456789</MSH.9>
        </MSH>
        <QPD>
            <QPD.1>
                <CE.1>Z01</CE.1>
                <CE.2>Observation Reporting Query</CE.2>
                <CE.3>NHIN Query Code</CE.3>
            </QPD.1>
            <QPD.2>Q123456</QPD.2>
            <QPD.3>
                <CE.1>RES</CE.1>
                <CE.2>result</CE.2>
                <CE.3>0048</CE.3>
            </QPD.3>
            <QPD.5>
                <CE.1>MEDICATIONS DISPENSED</CE.1>
            </QPD.5>
        </QPD>
    </QBP_Z01>
</Query>
```
<ns0:senderIdentificationLevelOne>3</ns0:senderIdentificationLevelOne>
<ns0:levelOneIdentificationCodeQualifier>SID</ns0:levelOneIdentificationCodeQualifier>
<ns0:interchangeRecipient>
<ns0:recipientIdentificationLevelOne>57c42842-25e9-4b57-b93f-4e8e99bcfab</ns0:recipientIdentificationLevelOne>
<ns0:levelOneIdentificationCodeQualifier>SID</ns0:levelOneIdentificationCodeQualifier>
<ns0:recipientIdentificationLevelTwo>JohnD</ns0:recipientIdentificationLevelTwo>
<ns0:levelTwoIdentificationCodeQualifier>ZZZ</ns0:levelTwoIdentificationCodeQualifier>
<ns0:recipientIdentificationLevelThree>HR Staff</ns0:recipientIdentificationLevelThree>

<ns0:dateTimeOfInitiation>
<ns0:date>20051114</ns0:date>
<ns0:eventTime>013045</ns0:eventTime>
<ns0:offSet>-0700</ns0:offSet>
</ns0:dateTimeOfInitiation>

<ns0:UIB>
<ns0:UIH>
<ns0:messageType>Response</ns0:messageType>
<ns0:messageVersionNumber>008</ns0:messageVersionNumber>
<ns0:messageReleaseNumber>001</ns0:messageReleaseNumber>
<ns0:messageFunction>RxHRES</ns0:messageFunction>
<ns0:messageReferenceNumber>123</ns0:messageReferenceNumber>
<ns0:dialogueReference>
<ns0:initiatorControlReference>1</ns0:initiatorControlReference>
</ns0:dialogueReference>
</ns0:UIH>
<ns0:RES>
<ns0:responseTypeCode>A</ns0:responseTypeCode>
</ns0:RES>
<ns0:PTT>
<ns0:birthdate>19090630</ns0:birthdate>
<ns0:name>
<ns0:partyName>THOMSON</ns0:partyName>
<ns0:firstName>MARK</ns0:firstName>
</ns0:name>
<ns0:genderCode>M</ns0:genderCode>
<ns0:referenceNumber>
<ns0:referenceNumber>http://ceide4/CDX/CDX_MH.asmx</ns0:referenceNumber>
<ns0:referenceQualifier>UR</ns0:referenceQualifier>
</ns0:referenceNumber>
<ns0:communicationNumber/>
</ns0:PTT>
<ns0:PVD>
<ns0:providerCode>PC</ns0:providerCode>
<ns0:referenceNumber>
<ns0:referenceNumber>12343</ns0:referenceNumber>
<ns0:referenceQualifier>OB</ns0:referenceQualifier>
</ns0:referenceNumber>
<ns0:communicationNumber/>
<ns0:codeListQualifier>TE</ns0:codeListQualifier>
</ns0:communicationNumber>
<ns0:name/>
<ns0:middleName/>
<ns0:nameSuffix/>
<ns0:namePrefix/>
</ns0:name>
</ns0:PVD>
<ns0:DRU>
<ns0:drug>
<ns0:itemDescriptionIdentification>D</ns0:itemDescriptionIdentification>
<ns0:itemDescription>Docusate Sodium</ns0:itemDescription>
</ns0:drug>
</ns0:DRU>
<ns0:drug><ns0:itemDescriptionIdentification>D</ns0:itemDescriptionIdentification><ns0:itemDescription>Ibuprofen</ns0:itemDescription><ns0:itemNumber>51079028220</ns0:itemNumber><ns0:codeListResponsibilityAgency>ND</ns0:codeListResponsibilityAgency><ns0:measurementValue>600MG TAB</ns0:measurementValue><ns0:form>1 TAB</ns0:form></ns0:drug><ns0:quantity><ns0:quantityQualifier>EA</ns0:quantityQualifier><ns0:quantity>1.00</ns0:quantity></ns0:quantity><ns0:directions><ns0:dosage>600 mg</ns0:dosage></ns0:directions><ns0:date><ns0:dateTimePeriod>20030817200000-0400</ns0:dateTimePeriod><ns0:dateTimePeriodFormatQualifier>126</ns0:dateTimePeriodFormatQualifier><ns0:dateTimePeriodQualifier>07</ns0:dateTimePeriodQualifier></ns0:date><ns0:date><ns0:dateTimePeriod>20030815150000-0400</ns0:dateTimePeriod><ns0:dateTimePeriodFormatQualifier>126</ns0:dateTimePeriodFormatQualifier><ns0:dateTimePeriodQualifier>36</ns0:dateTimePeriodQualifier></ns0:date><ns0:date><ns0:dateTimePeriod>20030819051124-0400</ns0:dateTimePeriod><ns0:dateTimePeriodFormatQualifier>126</ns0:dateTimePeriodFormatQualifier><ns0:dateTimePeriodQualifier>LD</ns0:dateTimePeriodQualifier></ns0:date><ns0:productSubstitutionCode>0</ns0:productSubstitutionCode><ns0:refillQuantity><ns0:quantityQualifier>R</ns0:quantityQualifier><ns0:quantity>0</ns0:quantity></ns0:refillQuantity></ns0:DRU><ns0:DRU><ns0:drug><ns0:itemDescriptionIdentification>D</ns0:itemDescriptionIdentification><ns0:itemDescription>Codeine</ns0:itemDescription><ns0:itemNumber>00054815624</ns0:itemNumber><ns0:codeListResponsibilityAgency>ND</ns0:codeListResponsibilityAgency><ns0:measurementValue>30mg Tab</ns0:measurementValue><ns0:form>1-2 TAB</ns0:form></ns0:drug><ns0:quantity><ns0:quantityQualifier/>><ns0:quantity/></ns0:quantity><ns0:directions><ns0:dosage>30-60 mg</ns0:dosage></ns0:directions><ns0:date><ns0:dateTimePeriod>20030817200000-0400</ns0:dateTimePeriod><ns0:dateTimePeriodFormatQualifier>126</ns0:dateTimePeriodFormatQualifier><ns0:dateTimePeriodQualifier>07</ns0:dateTimePeriodQualifier></ns0:date><ns0:date><ns0:dateTimePeriod>20030815150000-0400</ns0:dateTimePeriod><ns0:dateTimePeriodFormatQualifier>126</ns0:dateTimePeriodFormatQualifier><ns0:dateTimePeriodQualifier>36</ns0:dateTimePeriodQualifier></ns0:date><ns0:date><ns0:dateTimePeriod>20030819051124-0400</ns0:dateTimePeriod><ns0:dateTimePeriodFormatQualifier>126</ns0:dateTimePeriodFormatQualifier><ns0:dateTimePeriodQualifier>LD</ns0:dateTimePeriodQualifier></ns0:date><ns0:productSubstitutionCode>0</ns0:productSubstitutionCode><ns0:refillQuantity><ns0:quantityQualifier>R</ns0:quantityQualifier><ns0:quantity>0</ns0:quantity></ns0:refillQuantity></ns0:DRU>
<ns0:DRU>
  <ns0:drug>
    <ns0:itemDescriptionIdentification>D</ns0:itemDescriptionIdentification>
    <ns0:itemDescription>Acetaminophen</ns0:itemDescription>
    <ns0:itemNumber>51079039620</ns0:itemNumber>
    <ns0:codeListResponsibilityAgency>ND</ns0:codeListResponsibilityAgency>
    <ns0:measurementValue>500MG TAB</ns0:measurementValue>
    <ns0:form>1-2 TAB</ns0:form>
  </ns0:drug>
  <ns0:quantity/>
  <ns0:quantityQualifier>EA</ns0:quantityQualifier>
  <ns0:quantity>2.00</ns0:quantity>
  <ns0:directions>
    <ns0:dosage>500-1000 mg</ns0:dosage>
  </ns0:directions>
  <ns0:date/>
  <ns0:date/>
  <ns0:date/>
  <ns0:productSubstitutionCode>0</ns0:productSubstitutionCode>
  <ns0:refillQuantity />
  <ns0:refillQuantity/>
</ns0:DRU>

<ns0:DRU>
  <ns0:drug>
    <ns0:itemDescriptionIdentification>D</ns0:itemDescriptionIdentification>
    <ns0:itemDescription>Bisacodyl (Rectal)</ns0:itemDescription>
    <ns0:itemNumber>51079055271</ns0:itemNumber>
    <ns0:codeListResponsibilityAgency>ND</ns0:codeListResponsibilityAgency>
    <ns0:measurementValue>10MG SUPP</ns0:measurementValue>
    <ns0:form>1 SUPP</ns0:form>
  </ns0:drug>
  <ns0:quantity/>
  <ns0:quantityQualifier/>
  <ns0:quantity>
    <ns0:quantityQualifier>R</ns0:quantityQualifier>
    <ns0:quantity>0</ns0:quantity>
  </ns0:quantity>
  <ns0:directions/>
  <ns0:date/>
  <ns0:date/>
  <ns0:date/>
  <ns0:productSubstitutionCode>0</ns0:productSubstitutionCode>
  <ns0:refillQuantity/>
  <ns0:refillQuantity/>
</ns0:DRU>
<ns0:quantityQualifier>R</ns0:quantityQualifier>
<ns0:quantity>0</ns0:quantity>
</ns0:refillQuantity>
<ns0:DRU>
<ns0:UIT>
<ns0:messageReferenceNumber>0</ns0:messageReferenceNumber>
</ns0:UIT>
<ns0:UIZ>Text</ns0:UIZ>
</ns0:RXHRES>
</Response>
APPENDIX A - HL7 Implementation Guidelines

1. Populating the PID Values for a Patient Search

The system sending an Observation Reporting Query request should populate as many of the PID segment values as it knows. Each SNO that receives the search query uses its own search algorithm and decides which of the incoming PID values it will use. The only values that are guaranteed to be used are the patient name, birth date, and gender.

2. CX Identifier Values

When HL7 messages are being sent between systems, CX values may present difficult implementation issues. CX values as used for institutional medical record numbers, ancillary system order numbers, physician order entry order numbers, insurance policy numbers, driver license numbers, credit card numbers, billing account numbers, patient visit numbers, etc. Our HL7 implementation pays attention to the CX.1 (Identifier), CX.2 (Check digit), CX.4 (Assigning authority), and CX.5 (Identifier type code) sub-component values. We generate CX.6 (Assigning facility) component values in our outgoing messages, when appropriate.

We concatenate the incoming CX.1 (Identifier) and CX.2 (Check digit) components, strip off leading zeroes, and consider the result as the CX identifier/number value. On HL7 output, we value the Identifier component with the identifier value defined above. The Check digit component is always empty in our outgoing message.

The CX.4 (Assigning authority) value defines the identifier “pool” or “namespace” in which the Identifier was generated. We require it to be valued because we represent every patient, order, account, and visit identifier (etc.) as a pair: the actual identifier/number plus the “namespace” within which that identifier is unique. In the HL7 message, the Assigning authority is an HL7 HD data type. HL7 defines two different ways in which it can be valued. A value in the first HD sub-component (Namespace ID) is a universally agreed upon label for the identifier “pool” or “namespace”. It is conceptually similar to an HL7 OID. Alternatively, the second (Universal ID) and third (Universal ID type) HD sub-components may combine to specify the identifier namespace. When we receive an HL7 CX value to be stored in our database, we look into our table of valid Assigning authority values. If we find a match for the Namespace ID sub-component value, all is well and we look no further. If Namespace ID is not valued or we do find a match for it, we try to match on the combined Universal ID and Universal ID type component values. Our database contains all three HD sub-component values for every Assigning authority. When we generate a CX value in an outgoing HL7 message, we value all three CX.4 (HD) sub-components,

The CX.5 (Identifier type code) value defines the type or category of the identifier. Across HL7 messages and fields, we place importance on “AN” to indicate a billing account number, “DN” to indicate a doctor number, “MR” to indicate a medical record number, “SS” to indicate a social security number, and “VN” to indicate a patient visit number.

3. OBR [Order] and OBX [Observation result] Service Codes

We strongly suggest that LOINC codes be used for OBR.4 (Universal Service ID) and OBX.3 (Observation identifier) CE values.
4. PID.8 [Sex] Codes

We support values of “M”, “F”, and “U”. The CE.2 (Text) and CE.3 (Name of coding system) component values can be supplied but we ignore them when performing a patient lookup.

5. CE Code Values

Each HL7 CE data value contains up to six components. The first three are Identifier, Text, and Name of coding system. When supplying a coded value, these three components should always be valued. In particular, the Text component should be valued even for well-known codes. By doing so, a system that receives a CE value will always be able to display that value, even if it does not understand the code. The fourth through sixth CE components should likewise either all be valued or all be left empty. They represent an alternative code with the same meaning as the code represented in the first three components.
## Appendix B - NHIN Code Tables

### Table NHIN_0001 -- Reporting Department Codes

<table>
<thead>
<tr>
<th>Code</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MEDICATIONS DISPENSED</td>
<td>Pharmacy-dispensed medications</td>
<td>Medication dispensing transactions</td>
</tr>
<tr>
<td>LABORATORY</td>
<td>Clinical Laboratory</td>
<td>Clinical laboratory results and reports.</td>
</tr>
<tr>
<td>NURSING</td>
<td>Nursing</td>
<td>Nursing observations</td>
</tr>
<tr>
<td>RADIOLOGY</td>
<td>Radiology</td>
<td>X-Ray reports and images</td>
</tr>
<tr>
<td>VITAL SIGNS</td>
<td>Vital Signs</td>
<td>Recorded vital signs.</td>
</tr>
</tbody>
</table>

### Table NHIN_0002 -- Time Filter Direction

<table>
<thead>
<tr>
<th>Code</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EARLIEST</td>
<td>Earliest</td>
<td>When a limit is placed on the number of returned results and reports, the limit N will cause the N earliest (oldest) values to be returned by the query.</td>
</tr>
<tr>
<td>LATEST</td>
<td>Latest</td>
<td>When a limit is placed on the number of returned results and reports, the limit N will cause the N latest (most recent) values to be returned by the query.</td>
</tr>
</tbody>
</table>
### Appendix C - EvaluationSettings Elements in SOAP Header

<table>
<thead>
<tr>
<th>Element Name</th>
<th>Data Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MaxResponseInterval</td>
<td>Integer</td>
<td>unlimited</td>
<td>The server is instructed to wait no longer than this number of seconds before responding to the client query. If the server cannot respond fully with this interval, it should return whatever partial results it has gathered so far. If no query data has been gathered so far, the server should generate the SOAP fault “Server.WAIT INTERVAL EXPIRED”.</td>
</tr>
<tr>
<td>PatientIdentified</td>
<td>yes/no</td>
<td>no</td>
<td>Value of “yes” indicates patient registration information has already been resolved to a single registration instance, probably by a previous “Patient Identities” query. In the case of a “yes” value here, all PID(s) supplied in the query must already contain valid medical record numbers and institution identifiers.</td>
</tr>
</tbody>
</table>
| ResponseStyle           | String    | D       | D = deferred (asynchronous)
I = immediate (synchronous)  
This value is a copy of RCP.1 value from the HL7 query. It is duplicated in the message header for convenience. |
Appendix D - NHIN-Specific SOAP 1.1 Faults

<table>
<thead>
<tr>
<th>SOAP faultcode</th>
<th>SOAP faultstring</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client</td>
<td>INVALID QUERY DATA</td>
<td>The fault message text will describe the query data value that could not be understood.</td>
</tr>
<tr>
<td>Client</td>
<td>INVALID QUERY FORMAT</td>
<td>The format and/or version specified in the &lt;Query&gt; node is not supported by this NHIN server.</td>
</tr>
<tr>
<td>Client</td>
<td>INVALID QUERY NAME</td>
<td>The HL7 query name was not in the list of supported queries.</td>
</tr>
<tr>
<td>Server</td>
<td>WAIT INTERVAL EXPIRED</td>
<td>The NHIN server was not able to respond to the query within the specified response interval.</td>
</tr>
</tbody>
</table>

The SOAP “faultstring” specifies the type of fault/error that occurred, but does not tell one the exact data value that was responsible for the fault. Fortunately, SOAP provides a way to do so. Consider the following example. An NHIN server receives a “Patient Identities” query. No person first name is specified in the query message and the target person’s date of birth is not a valid date. The NHIN server returns the following SOAP fault:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi:schemaLocation="http://schemas.xmlsoap.org/soap/envelope/
https://connectingforhealth.regenstrief.org:8443/NHIN/services/NHINQueryEnvelope.xsd">
<soapenv:Body>
<soapenv:Fault>
    <faultcode>Client</faultcode>
    <faultstring>INVALID QUERY DATA</faultstring>
    <detail>
        <NHINFault xmlns="http://www.nhin.gov/messaging">
            <ErrorMessage>No person name was specified. Person date of birth was not a valid date.</ErrorMessage>
            <ErrorData>
                <Field>PID.5 XPN.2</Field>
                <Reason>Person first name missing</Reason>
            </ErrorData>
            <ErrorData>
                <Field>PID.7 TS.1</Field>
                <Value>19009999</Value>
                <Reason>Invalid person date of date</Reason>
            </ErrorData>
        </NHINFault>
    </detail>
</soapenv:Fault>
</soapenv:Body>
</soapenv:Envelope>
```

Any number of <ErrorData> elements can be added to the NHIN SOAP fault <detail>. Each <ErrorData> node must contain a <Reason> element defining the exact fault or error. When applicable, the <Field> node defines exactly what field in the message contained the invalid, missing, incomplete, or incompatible value. The value itself appears in the <Value> element.
Appendix E - Query Response Format and Version Identifiers

The table below describes the currently recognized contents of the format and version attributes used in the XML representation of a <nhin:Response> node.

<table>
<thead>
<tr>
<th>Format</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HL7</td>
<td>2.4</td>
<td>XML representation of HL7 2.4</td>
</tr>
<tr>
<td>HL7</td>
<td>3.0</td>
<td>HL7 3.0 (natively XML)</td>
</tr>
<tr>
<td>NCPDP Scripts</td>
<td>8.1</td>
<td>XML version of NCPDP medication dispensing information</td>
</tr>
</tbody>
</table>
Appendix F - ACK/NAK Soap Message

NHIN's asynchronous queries are implemented as two separate SOAP conversations. The NHIN client sends its query message in a SOAP message to the NHIN server, which responds with the “ACK” SOAP message defined in this Appendix. Later on, the NHIN server sends the actual query response back to the NHIN client, or its designee, in a new SOAP conversation. The NHIN client responds with a SOAP “ACK” message of its own. From the SOAP server's point of view, this “ACK” message is the response to the query SOAP message and the response to the query response SOAP message.

The ACK message is returned as an HL7 “original mode” ACK within an “NHINResponse” message. The HL7 MSH and MSA “segments” are defined in the remainder of this Appendix.

F.1  

PatientDataRequestACKNAK.MSH  [Message Header]

The message is type ACK with no event code.

F.2  

PatientDataRequestACKNAK.MSA  [Message Acknowledgement]

The MSA segment returns the Acknowledgment Code value “AA” and echoes the original query's MSH.MESSAGE CONTROL ID value in MSA.MESSAGE CONTROL ID.

F.3  

Complete Example

<ACK xmlns="urn:hl7-org:v2xml">
  <MSH>
    <MSH.1/>
    <MSH.2/>
    <MSH.3>
      <HD.1>Query Result Locator</HD.1>
    </MSH.3>
    <MSH.4>
      <HD.1>Query Facility Name</HD.1>
    </MSH.4>
    <MSH.5>
      <HD.1>Query Application Name</HD.1>
    </MSH.5>
    <MSH.6>
      <HD.1>ST ELSEWHERE HOSPITAL</HD.1>
    </MSH.6>
    <MSH.7>
      <TS.1>20051026130205</TS.1>
    </MSH.7>
    <MSH.9>
      <MSG.1>ACK</MSG.1>
    </MSH.9>
    <MSH.10>24</MSH.10>
    <MSH.11>
      <PT.1>P</PT.1>
    </MSH.11>
    <MSH.12>
      <VID.1>2.4</VID.1>
    </MSH.12>
  </MSH>
  <MSA>
    <MSA.1>AA</MSA.1>
    <MSA.2>123456789</MSA.2>
  </MSA>
</ACK>
Appendix G - Prototype Servers

In order to test the Connecting for Health Common Framework prototype, we set up a series of Record Locator Service (RLS) and Inter-SNO Bridge (ISB) test servers in the three participating communities. The RLS servers provide access to a matching algorithm for determining when an existing patient record matches a query, and to database of accurate but anonymized demographic details (names, dates of birth, and addresses were scrambled to prevent any "test" patient from having a real patient's identity), plus associated record locations for those patients. Incoming test requests were then run through the matching algorithm to determine which record locations in the database, if any, were matched. Each of the ISB servers provides access to the RLS from entities outside the SNO.

In order to make the basic workings of the prototype visible, we have left the test servers running and accessible for those who would like to experiment with formatting valid queries and parsing the results. In addition, each region is making the source code used to handle the incoming queries available for download from the same server hosting the test interface. The source code covers those functions created by each of the three regions, built on a variety of technical platforms:

**CA:**
- Operating System: Linux Red Hat Enterprise Linux ES 4
- Application Server: Apache Tomcat, 5.0
- Web Services: Apache Axis, 1.3

**IN:**
- Operating System: Red Hat Enterprise Linux AS 4
- Application Server: Apache Tomcat, 4.1.31
- Web Services: Apache Axis, 1.1

**MA:**
- Application Server: IIS 5/BizTalk 2004 as EAI tool
- Web Services: .NET framework 1.1

You can find pointers to the regional servers hosting the test interface for the prototype, plus the source code and related files, at:

Acknowledgements

The working groups in the three regions of the Connecting for Health prototype and the Technical Subcommittee have worked for over two years to create a prototype of a decentralized, standards-based, and privacy-protecting architecture for the exchange of health records. During that time, we have been fortunate to work with respected experts in the fields of health and information technology, all of whom have contributed their time, energy, and expertise to the transition from a basic set of principles to a working prototype. Our consultants and volunteers have worked long hours in meetings and conference calls to negotiate high-level questions of architectural design and low-level details of particular technical protocols. We offer them our heartfelt thanks for taking on this journey with us, and look forward to the remaining work ahead.

In addition, we would like to offer special thanks to the working groups who took the conceptual technical model and instantiated it as running code: for the Massachusetts test, John Halamka, Greg DeBor, Gail Fournier, Vinod Muralidhar, and John Calladine; for the Indiana test, J. Marc Overhage, Clement McDonald, Lonnie Blevins, and Andrew Martin; and for the California test, Will Ross and Don Grodecki.

Finally, we must note that none of this work would have been possible without the leadership and inspiration of Clay Shirky, who encouraged us to turn theory into practice, and whose unmatched skills at navigating and then capturing each progressive phase of our work over the last two years allowed us to do so.

Connecting for Health Technology Subcommittee

Clay Shirky, New York University, (Chair)

Laura Adams, Rhode Island Quality Institute

Steve Adams, RMD Networks

William Braithwaite, MD, eHealth Initiative, (Co-Chair, Policy Subcommittee)

Deleys Brandman, First Consulting Group

Bryan Breen, Cisco Systems, Inc.

Sophia Chang, MD, MPH, California HealthCare Foundation

Art Davidson, MD, MSPH, Denver Public Health

Didi Davis, Eclipsys, Healthcare Information and Management Systems Society, and Integrating the Healthcare Enterprise

Lyman Dennis, Partnership HealthPlan of California, Healthcare Information and Management Systems Society, and Integrating the Healthcare Enterprise

George Eisenberger, IBM Corporation

David A. Epstein, IBM Software Group

Linda Fischetti*, RN, MS, Veterans Health Administration
Mark Frisse, MD, MBA, MSc, Vanderbilt Center for Better Health (Co-Chair, Policy Subcommittee)

Don Grodecki, Browsersoft, Inc.

John Halamka, MD, CareGroup Healthcare System

Bob Hedgcock, Wisconsin Health Information Exchange

Noreen Hurley, Tufts Health Plan

Charles Jaffe, MD, PhD, Intel Corporation

Timothy Kenney, GE Healthcare

Josh Lemieux, Omnimedix Institute

J.P. Little, RxHub

Christopher Lindop, Eastman Kodak Company

David Lubinski, Microsoft Corporation

Janet Marchibroda, eHealth Initiative

Gregory Andre Marinkovich*, MD, FAAP LTC, Marine Corps, Office of Secretary of Defense/Health Affairs

Patrick McMahon, Microsoft Corporation

Omid Moghadam, Intel Corporation

Don Mon, PhD, American Health Information Management Association

Bruno Nardone, IBM Corporation

J. Marc Overhage, MD, PhD, Indiana Health Information Exchange; Indiana University School of Medicine, Regenstrief Institute for Healthcare

George Peredy, MD, Kaiser Permanente, HealthConnect

Nick Ragouzis, Enosis Group, LLC

Rick Ratliff, SureScripts

Jere Retzer, Oregon Health and Science University

Wes Rishel, Gartner Group

Barry Rhodes*, PhD, Center for Disease Control, United States Department of Health and Human Services

Scott Schumacher, PhD, Initiate Systems, Inc.

Raymond W. Scott, Axolotl Corporation

Don Simborg, MD, American Medical Informatics Association

Geoff Smith, Meditech

Jonathan Teich, MD, PhD, Healthvision

Micky Tripathi, Massachusetts eHealth Collaborative

Charlene Underwood, Healthcare Information and Management Systems Society, EHR Vendor Association

Karen Van Hentenryck, HL-7

Jukka Valkonen, California HealthCare Foundation

Cynthia Wark*, CAPT, United States Public Health Service Commissioned Corps, Centers for Medicare and Medicaid Services, United States Department of Health and Human Services

Jon White*, MD, Agency for Healthcare Research and Quality, United States Department of Health and Human Services

Scott Williams, MD, MPH, HealthInsight

Amy Zimmerman-Levitan, MPH, Rhode Island Department of Health

*Note: Federal employees participate in the Subcommittee but make no endorsement
Medication History Standards
Medication History Standards
Medication History Standards*

One of two use cases we tested in the Connecting for Health Common Framework prototype was the exchange of medication history. In order to do so, we adopted a format for representation in the network that had the best fit with broad adoption and potential standardization. The Medication History schema we used was derived from the National Council for Prescription Drug Programs (NCPDP) SCRIPT specification, version 8.1, as described by RxHub.2

We generated a schema for use in the prototype using the ZixCorp XML implementation. These Medication History schemae, as developed by CSC, can be located at:

https://ehr.consult.csc.com/cfh/.

There is considerable work on medication history standards, and we anticipate that there will be future changes to this standard in the near term. Because the Common Framework maintains a separation between data description and transport, updates to the medication history standard will not require re-engineering the network to accommodate the new standard.

* Connecting for Health thanks the Massachusetts prototype team, John Halamka, MD, Vinod Muralidhar, John Calladine, and Gail Fournier for their implementation efforts on this standard.

1 www.ncpdp.org.
2 www.rxhub.net.
3 www.zixcorp.com/.

©2006, Markle Foundation
This work was originally published as part of The Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange and is made available subject to the terms of a license (License) which may be viewed in its entirety at: http://www.connectingforhealth.org/license.html. You may make copies of this work; however, by copying or exercising any other rights to the work, you accept and agree to be bound by the terms of the License. All copies of this work must reproduce this copyright information and notice.
Laboratory Results Standards
The document you are reading is part of The Connecting for Health Common Framework, which is available in full and in its most current version at: http://www.connectingforhealth.org/. The Common Framework will be revised and expanded over time. As of October 2006, the Common Framework included the following published components:
Laboratory Results Standards*

One of two use cases we tested in the Connecting for Health Common Framework prototype was the exchange of laboratory results. In order to do so, we adopted a format for representation in the network that had the best fit with broad adoption and potential standardization. The Laboratory Results schema we used was derived from the ELINCS v2.0 (draft) specification, created by the California Healthcare Foundation.¹

The specification can be found at:

There is considerable work on laboratory results standards, and we anticipate that there will be future changes to this standard in the near term. Because the Common Framework maintains a separation between data description and transport, updates to the lab results standard will not require re-engineering the network to accommodate the new standard.

The ELINCS 2.0 version we used is still in draft form. The messages as we formatted them had several deviations from the ELINCS implementation guide in its draft form:

1. ELINCS prohibits populating many of the PID fields. NHIN permits any or all to be populated in query messages and returns most of those values when responding to a query. Our own implementation will return most of the contents of the PID segment in the query response (with the exception of SSN, which we will blank out).

2. The ELINCS draft requires a time zone accompanying all date-time values, while we do not. (We believe that that requirement will be relaxed in the balloted standard.)

*Connecting for Health thanks the Indiana prototype team, J. Marc Overhage, MD, PhD, Clement McDonald, MD, and Lonnie Blevins for their implementation efforts on this standard.

¹ http://www.chcf.org/.

©2006, Markle Foundation
This work was originally published as part of Connecting for Health: Resources for Implementing Private and Secure Health Information Exchange and is made available subject to the terms of a license (License) which may be viewed in its entirety at: http://www.connectingforhealth.org/license.html. You may make copies of this work; however, by copying or exercising any other rights to the work, you accept and agree to be bound by the terms of the License. All copies of this work must reproduce this copyright information and notice.
3. Only the first component of the OBR.15 (SPECIMEN SOURCE) is allowed to be valued in the ELINCS draft. We routinely get very useful specimen source information in all five components of this HL7 field, and have allowed them to be populated.

4. The draft ELINCS spec requires all units be expressed as UCUM codes. We do not expect to see all units expressed in that coding system.

5. HL7 permits OBX.14 (DATE/TIME OF OBSERVATION) when test results for some members of a test battery were performed at a time different from the other members of the test battery. ELINCS forbids this value. We support it.

6. The ELINCS draft limits the value type in OBX results segments to be of type CE (code), SN (structured numeric), ST (string), TX (text), or FT (formatted text). HL7 defines a much longer list of allowed value types. Our messages also support the longer list for those value types, such as DT (date), etc.

7. The ELINCS draft ignores OBX.4 (SUB-ID) for all but microbiology tests. Our messages include that value. It is useful for formatted reports and for other, less common types of data.

8. OBR fields for Principal Results Interpreter, Assistant Results Interpreter, Reason For Study, Technician, Diagnostic Service Sect ID, Danger Code, Relevant Clinical Info, and Priority are prohibited from being valued in the ELINCS draft. Our messages support those values.
Background Issues on Data Quality
Background Issues on Data Quality
The document you are reading is part of *The Connecting for Health Common Framework*, which is available in full and in its most current version at: [http://www.connectingforhealth.org/](http://www.connectingforhealth.org/). The Common Framework will be revised and expanded over time. As of October 2006, the Common Framework included the following published components:

![Diagram of the Common Framework](image-url)
Background Issues on Data Quality

Introduction
We live in an era of unprecedented data abundance and aggregation. The sheer variety of new information available on the Internet, in databases, and from other sources has changed the way we conduct business, undertake research, and communicate. Most of the changes are positive. Yet, increased reliance upon networked data has also introduced new challenges. One serious problem we need to address is that of “dirty data”—missing or inaccurate information that resides in (and, indeed, frequently results from) the abundance and aggregation of data in our lives today.

Dirty data can have several pernicious effects. In particular, it:

- Impacts the quality of care;
- Introduces privacy and other civil liberty concerns;
- Increases costs and inefficiencies;
- Creates liability risks; and
- Undermines the reliability and benefits of information technology (IT) investments, including the potential to streamline service delivery, accounting, and billing.

These concerns are particularly important in the medical field, where data problems represent the dark side of the tremendous potential offered by the adoption of health IT systems. In a “networked” medical setting, dirty data not only introduces economic inefficiencies; it may also cost lives. In addition, the lack of a data quality culture may be a core deterrent for many users in adopting and using health IT today.

As various regional and affinity-based information exchange networks around the country are developing and implementing strategies and architectures to link and share patients’ data, the issue of dirty data will have to be addressed. Inaccurate patient data, especially if it affects the data fields used to establish individual patient identity through a Record Locator Service (RLS), may be harmful if not mitigated from the outset. Dirty patient data has, for instance, the potential to undermine the matching capabilities of an RLS or to provide for an unacceptable level of false negatives. This document considers the growing need to develop a “data quality culture” at the network level and lists possible issues and options to consider.

* Connecting for Health thanks Stefaan Verhulst, Chief of Research, Markle Foundation, for drafting this paper.

1 For a definition and description of a Record Locator Service (RLS), see http://www.connectingforhealth.org/assets/reports/linking_report_2_2005.pdf.

© 2006, Markle Foundation
This work was originally published as part of The Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange and is made available subject to the terms of a license (License) which may be viewed in its entirety at: http://www.connectingforhealth.org/license.html. You may make copies of this work; however, by copying or exercising any other rights to the work, you accept and agree to be bound by the terms of the License. All copies of this work must reproduce this copyright information and notice.
I. The Problem

By some estimates, the problem of dirty data in industry has reached epidemic proportions. The problem is equally prevalent and potentially even more alarming in health care.

In a medical setting, dirty data has several consequences:

First and foremost, it can lead to medical errors, which can kill or cause long-term damage to the health of patients. A widely noted 2000 Institute of Medicine report estimates, for example, that between 44,000 and 98,000 lives are lost every year due to medical errors in hospitals alone, and that such errors result in an additional $17 to $29 billion in annual healthcare costs. Although not all these errors can be attributed to inaccurate data, a number of studies have shown a link between poor quality data (in databases) and medical errors and subsequent poor quality of care. Further, in a “networked” health care setting, the challenge of data accuracy becomes even more critical because a health professional immediately uses the information accessible, especially in the case of an acute illness or emergency intervention, without any built-in step or potential to review its accuracy.

Conversely, improving data quality can increase the quality of care by initiating a positive chain reaction—improving the data that clinicians see when the patient is admitted can validate the need for services to the patient, and if followed up with the provision of those identified services, may provide for better outcomes. A study on child mental health services, for instance, showed that 58 percent of the patients had improved outcomes after a data quality improvement project was instituted.

Poor data quality can also reduce the accuracy of insurance bills. A study analyzing Medicare data found that 2.7 percent of the nearly 11.9 million records in the database, approximately 321,300 records, contained coding errors. Such errors can impact the clinician’s and/or the patient’s insurance reimbursement and/or cause additional time to be spent correcting the errors. The study also identified the immediate benefits of addressing the errors. According to the Medicare study, the top 10 coding errors accounted for 70 percent of the total errors. By focusing on those 10 coding errors a high percentage of the problem can be addressed instantly, saving time and money.

Dirty data can also have serious consequences for patient privacy, especially in a networked environment. A single—and originally isolated—error in a data set can be magnified (and thus pose a
more serious privacy risk) as it is “propagated” into various other data sets, systems and warehouses, while decreasing at each step the potential to redress the error.\(^9\) On the other hand, a networked and aggregated data environment obviously undermines the “privacy by obscurity” paradigm that was often the sole privacy protection available in an off-line world.

While poor quality data can erode privacy, strong privacy protections can enhance the quality of data and subsequent health care, for example, by increasing trust and therefore increasing the amount of data that patients are willing to share with medical providers.\(^10\) “Data accuracy” is therefore one of the nine principles underpinning “The Connecting for Health Architecture for Privacy in a Networked Health Information Environment.”\(^11\)

Despite the severity of the problem, the risks posed by dirty data often go unrecognized; in many ways, the problem of inaccurate data remains a low priority for companies and organizations.\(^12\) It is critical to understand the problem and to develop strategies for minimizing data inaccuracies and the potential harm they cause.

II. Understanding Dirty Data: Definitions, Causes, and Locations

Data quality is broadly defined as “the totality of features and characteristics of a data set that bear on its ability to satisfy the needs that result from the intended use of the data.”\(^13\) Data accuracy is one of the “foundational features” that contribute to data quality\(^14\) (along with other attributes such as timeliness, relevancy, representation, and accessibility).\(^15\) In addition, data quality has two essential components: content (i.e., the information must be accurate), and form (i.e., the data must be stored and presented in a manner that makes it usable). These definitions are important to keep in mind when considering ways to minimize data inaccuracies, as they illustrate why the task of fixing dirty data requires more than merely providing “right” information.

Equally important when developing a strategy to increase data quality is identification of the underlying causes of “dirty data.” Two broad categories of errors can be distinguished: systematic and random. Among the sources of systematic errors are: programming mistakes; bad definitions for data types or models; violations of rules established for data collection; poorly defined rules; and poor training. Random errors can be caused by: keying errors; data transcription problems; illegible handwriting; hardware failure (e.g., breakdown or corruption); and mistakes or deliberately misleading statements on the part of patients (or others) providing primary data. This is obviously not an exhaustive list, but a few examples of the types of errors that may occur. It is worth noting that according to the Data Warehousing Institute, 76 percent of all errors, across sectors and setting, result from “data entry.” This suggests the critical role played by human error; many of the strategies proposed below, therefore, focus on reducing the likelihood of human error.

III. Strategies to Address Dirty Data: Towards a Data Quality Culture

To establish data quality within a health care setting and to prevent data quality errors in the system and limit their consequences, health care organizations should develop comprehensive strategies to establish...
a data quality culture. Ideally, such strategies should be developed from the outset and be embedded in the design of any networked health information exchange system.

Organizations can use a variety of tools and techniques to increase the cleanliness of data, both at the time of collection and during subsequent processing.

For the purposes of Connecting for Health, data cleanliness efforts should be concentrated on those data elements required by the RLS. As the US moves towards widespread data standardization,16 data input quality control can improve the usability and quality of data outputs. It should be noted that the documentation of a clinician cannot, by law, be changed retroactively, as this constitutes a change to the documented medical record of an individual; adding corrected information is allowed.

For cases in which data cleansing techniques17 are applicable in health care, for example, detection (not resolution) of a single patient with two records, these techniques can be automated (e.g., in the form of software packages) or involve a human component (e.g., monitoring and training).

Ultimately, a well-thought-out and comprehensive data quality program should include both automated and human strategies, such as:

- **Standardize** data entry fields and processes for entering data18;
- **Institute** real-time quality checking, including the use of validation and feedback loops19;
- **Design** data element to avoid errors (for example, through the use of check digits and checking algorithms on numeric identifiers where human entry is involved and the use of well-designed user interfaces)20;
- **Develop and adhere to** guidelines for documenting the care that was provided to the patient 21;
- **Review automated billing software**;
- **Build human capacity**, including training, awareness-building, and organizational change.

Each of these strategies will incur certain costs, but they are likely to be less expensive than addressing errors resulting from a system designed without data quality features. The US health care system has a unique window of opportunity to establish such an internal data quality culture when considering how to adopt health IT systems in the near future.

These “organizational strategies” should be complemented by external strategies, especially redress mechanisms, which encourage identification and correction of errors. Redress mechanisms are frequently built into laws and regulations, which, among other things, allow consumers to access and correct errors in personal information.

In the United States, legal systems for redress date back at least to the Fair Credit Reporting Act of 1970. In addition, redress is built into the Privacy Act of 1974, and the Health Insurance Portability and Accountability Act of 1996.

Common redress strategies include:

- Notice of a possible adverse decision using inaccurate data and the procedure for challenging it;

---


17 For a discussion, see Arts et al., op cit, and Leithesser, op cit.


21 AHIMA Coding Products and Services Team. “Managing and Improving Data Quality (Updated) (AHIMA Practice Brief).” Journal of AHIMA 74, no.7 (July/August 2003): 64A-C.
• Access to the information on which the decision is based, which is premised on the ability to trace information to its source for verification;
• Opportunity to correct erroneous information and an obligation to correct or delete information that is erroneous;
• Procedures for ensuring that erroneous information does not re-enter the system;
• Obligations on data furnishers to respond to requests for reconsideration of data and to take corrective action when justified; and
• Independent administrative or judicial review and enforcement.

IV. Creating a “Data Quality Culture”: Implementation Issues to Consider
Implementing a data quality culture, as suggested above, poses various challenges. Without specifying the operational procedures that may be unique to each network design and RLS implementation, the following set of questions will need to be addressed:

Record Locator Service
• How do data quality concerns affect the RLS and clinical data exchange? What are the particular data quality problems likely to afflict the RLS, requiring RLS-specific interventions?
• How does the network deal with the integrity of data in the RLS itself? Who is responsible for these cleaning functions in the network?

Network versus Participants
• What are the expectations or requirements for each Participant vis-à-vis the Network with regard to sustaining a data quality culture?
• Are patients’ rights to access their records, as they pertain to the RLS, provided by the Network centrally, or does each Network participant offer such a policy individually?
• Should the Network provide universal data audits on RLS fields across all participants, flag conflicts, and resolve them?
• Should Networks use common training modules and protocols across all participants to address human errors?
• What are the roles of the Network and its participants with regard to cleaning clinical data that is exchanged among participants?

Patient Empowerment
• How do patients communicate corrections through the entire system, rather than just to the first place they might identify dirty data?
• Are patients or Network participants allowed to complete partial matches by using the RLS to search across the system (on the patient’s behalf) in the interest of improving data quality?
• What are reasonable procedures for rollover and rollback corrections across the system?
Acknowledgements

The members of the Connecting for Health Policy Subcommittee have accomplished an extraordinary task in less than a year’s time—the development of an evolving piece of work that can serve as the core of nationwide health information exchange—the policy components of The Common Framework. During this time, we have been fortunate to work with respected experts in the fields of health, information technology, and privacy law, all of whom have contributed their time, energy, and expertise to a daunting enterprise. Our consultants and volunteers have worked long hours in meetings and conference calls to negotiate the intricacies of such issues as privacy, security, authentication, notification, and consent in health information exchange. We offer them our heartfelt thanks for taking on this journey with us, and look forward to the remaining work ahead.

In addition, we would like to offer special thanks to the volunteers and consultants who authored the initial drafts of this body of work—their hard work created a strong foundation upon which to focus the Subcommittee’s deliberations: Stefaan Verhulst, Clay Shirky, Peter Swire, Gerry Hinkley, Allen Briskin, Marcy Wilder, William Braithwaite, and Janlori Goldman.

Finally, we must note that none of this work would have been possible without the leadership and inspiration of our co-chairs, William Braithwaite and Mark Frisse. They have led us with steady hands and determination of spirit.

Connecting for Health Policy Subcommittee

William Braithwaite, MD, eHealth Initiative, (Co-Chair)

Mark Frisse, MD, MBA, MSc, Vanderbilt Center for Better Health, (Co-Chair)

Laura Adams, Rhode Island Quality Institute

Phyllis Borzi, JD, George Washington University Medical Center

Susan Christensen*, JD, Agency for Healthcare Research and Quality, United States Department of Health and Human Services

Art Davidson, MD, MSHP, Denver Public Health

Mary Jo Deering*, PhD, National Cancer Institute/National Institutes of Health, United States Department of Health and Human Services

Jim Dempsey, JD, Center for Democracy and Technology

Hank Fanberg, Christus Health

Linda Fischetti*, RN, MS, Veterans Health Administration

Seth Foldy, MD, City of Milwaukee Health Department

Janlori Goldman, JD, Columbia College of Physicians and Surgeons

Ken Goodman, PhD, University of Miami

John Halamka, MD, CareGroup Healthcare System

Joseph Heyman, MD, American Medical Association

Gerry Hinkley, JD, Davis, Wright, Tremaine LLP

Charles Jaffe, MD, PhD, Intel Corporation

Jim Keese, Eastman Kodak Company

Linda Kloss, RHIA, CAE, American Health Information Management Association

Gil Kuperman, MD, PhD, New York-Presbyterian Hospital

Ned McCulloch, JD, IBM Corporation

Patrick McMahon, Microsoft Corporation

Omid Moghadam, Intel Corporation
Joyce Niland, PhD, City of Hope National Medical Center

Louise Novotny, Communication Workers of America

Michele O’Connor, MPA, RHIA, MPI Services Initiate

Victoria Prescott, JD, Regenstrief Institute for Healthcare

Marc A. Rodwin, JD, PhD, Suffolk University Law School

Kristen B. Rosati, JD, Coppersmith Gordon Schermer Owens & Nelson PLC

Sara Rosenbaum, JD, George Washington University Medical Center

David A. Ross, ScD, Public Health Informatics Institute

Clay Shirky, New York University (Chair, Technical Subcommittee)

Don Simborg, MD, American Medical Informatics Association

Michael Skinner, Santa Barbara Care Data Exchange

Joel Slackman, BlueCross/BlueShield Association

Peter P. Swire, JD, Moritz College of Law, Ohio State University

Paul Tang, MD, Palo Alto Medical Foundation

Micky Tripathi, Massachusetts eHealth Collaborative

Cynthia Wark*, CAPT, United States Public Health Service Commissioned Corps, Centers for Medicare and Medicaid Services, United States Department of Health and Human Services

John C. Wiesendanger, MHS, West Virginia Medical Institute/Quality Insights of Delaware/Quality Insights of Pennsylvania

Marcy Wilder, JD, Hogan & Hartson LLP

Scott Williams, MD, MPH, HealthInsight

Robert B. Williams, MD, MIS, Deloitte

Joy Wilson, National Conference of State Legislatures

Rochelle Woolley, RxHub

Amy Zimmerman-Levitan, MPH, Rhode Island State Department of Health

*Note: Federal employees participate in the Subcommittee but make no endorsement
Record Locator Service:
Technical Background from the Massachusetts Prototype Community
Record Locator Service – Technical Background from the Massachusetts Prototype Community
The document you are reading is part of The Connecting for Health Common Framework, which is available in full and in its most current version at: http://www.connectingforhealth.org/. The Common Framework will be revised and expanded over time. As of October 2006, the Common Framework included the following published components:

- **Policy Guides: How Information is Protected**
  - P1 The Architecture for Privacy in a Networked Health Information Environment
  - P2 Model Privacy Policies and Procedures for Health Information Exchange
  - P3 Notification and Consent When Using a Record Locator Service
  - P4 Correctly Matching Patients with Their Records
  - P5 Authentication of System Users
  - P6 Patients’ Access to Their Own Health Information
  - P7 Auditing Access to and Use of a Health Information Exchange
  - P8 Breaches of Confidential Health Information
  - P9 A Common Framework for Networked Personal Health Information

- **Technical Guides: How Information is Exchanged**
  - T1 The Common Framework: Technical Issues and Requirements for Implementation
  - T2 Health Information Exchange: Architecture Implementation Guide
  - T3 Medication History Standards
  - T4 Laboratory Results Standards
  - T5 Background Issues on Data Quality
  - T6 Record Locator Service: Technical Background from the Massachusetts Prototype Community

**Future Technical Guides**

**Future Policy Guides**

**Model Contractual Language**

- M1 Key Topics in a Model Contract for Health Information Exchange
- M2 A Model Contract for Health Information Exchange
Record Locator Service – Technical Background from the Massachusetts Prototype Community

This document describes the early design process for the Record Locator Service (RLS) as implemented in Massachusetts, and is included here as background on the technical conversation around the design of the Connecting for Health prototype. It is included here as a background guide to the issues surrounding the design of the RLS as constructed in Massachusetts; as noted in “The Common Framework: Technical Issues and Requirements for Implementation,” the placement of aggregation services can vary between sub-network organizations (SNOs). In this document, aggregation takes place via a clinical data exchange service; other architectural models are possible.

In addition to the overview of the architectural design decisions included in “The Common Framework: Technical Issues and Requirements for Implementation,” the technical details surrounding message exchange in the current prototype are documented in the “Health Information Exchange: Architecture Implementation Guide.”

Connecting for Health thanks Computer Sciences Corporation (CSC) for drafting this paper.

©2006, Markle Foundation

This work was originally published as part of The Connecting for Health: Resources for Implementing Private and Secure Health Information Exchange and is made available subject to the terms of a license (License) which may be viewed in its entirety at: http://www.connectingforhealth.org/license.html. You may make copies of this work; however, by copying or exercising any other rights to the work, you accept and agree to be bound by the terms of the License. All copies of this work must reproduce this copyright information and notice.
## Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Description</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>2005-02-18</td>
<td>0.1</td>
<td>• Initial (strawman) version where architecture discussions and design to date are documented for further review</td>
<td>CSC</td>
</tr>
<tr>
<td>2005-03-01</td>
<td>0.2</td>
<td>• Revised draft based on feedback from internal review. Added content on security.</td>
<td>CSC</td>
</tr>
</tbody>
</table>
| 2005-03-23 | 0.3     | • Revised based on feedback from reviewers of 0.2  
  • Changed conceptual application architecture to explicitly support peer-to-peer messaging and support inter-RLS messaging  
  • Moved revised conceptual application architecture diagram from Implementation view to Logical view  
  • Moved process diagrams from logical to process view. Added content on message exchange patterns to process specifications |
| 2005-03-25 | 0.4     | • Revised content based on internal review.  
  • Packaged to publish to Markle Connecting for Health Technical Subcommittee  
  • Retitled document: Framework Technical Overview                                                                                     | CSC    |
| 2005-04-12 | 0.5     | • Incorporated feedback from review of 0.4 by: Markle Connecting for Health Technical Subcommittee and MA-SHARE Technical Advisory Board. Comments provided in Appendix with responses.  
  • Changed architecture diagram to depict RLS and CDX Gateway as two solutions that the RLS Prototype project will develop to be flexible collection of a loosely-coupled services. Shows separation of RLS and other components more clearly. Section 5.2  
  • Added sequence diagrams to process view (Section 6) indicating processing logic for transactions supported by RLS                                                                                   | CSC    |
| 2005-04-15 | 0.6     | • Incorporated comments from internal review  
  • Added discussion items 4.5 (patient lookup with local MRN) and 4.6 (query-time matching)                                                                                                         | CSC    |
| 2005-05-20 | 1.0     | • Language edits: cleaned up references to RLS Exchange  
  • Changed Figures: 3 and 4 to align with more precise definition of RLS scope (vis-à-vis clinical data exchange)  
  • Modified Figure 13 and added Figure 14 to provide more details of security architecture and process                                                                                     | CSC    |
| 2005-11-22 | 1.1     | • Removed implementation specifications pertinent to only Massachusetts pilot. Reoriented content to be more generic.  
  • Removed discussion items that were relevant to prototype architecture decisions.                                                                                                               | CSC    |
Table of Contents

1 INTRODUCTION .................................................................................................................. 7
  1.1 PURPOSE .......................................................................................................................... 9
  1.2 SCOPE .............................................................................................................................. 9
  1.3 REFERENCES .................................................................................................................. 9
  1.4 DOCUMENT OVERVIEW .............................................................................................. 10
  1.5 ARCHITECTURAL REPRESENTATION ...................................................................... 11

2 ARCHITECTURAL GOALS, PRINCIPLES AND CONSTRAINTS .............................................. 13
  2.1 GOALS ............................................................................................................................ 13
  2.2 PRINCIPLES .................................................................................................................... 13

3 USE-CASE VIEW .................................................................................................................. 17
  3.1 RLS FUNCTIONS ........................................................................................................... 17
  3.2 USE CASES .................................................................................................................... 18
  3.3 USE-CASE REALIZATIONS .......................................................................................... 21
  3.4 SECURITY, PATIENT PRIVACY AND CONSENT MANAGEMENT .............................. 22
    3.4.1 Identity management .............................................................................................. 23
    3.4.2 Confidentiality, Authentication, Integrity & Non-repudiation ............................. 23
    3.4.3 Patient Data Privacy ............................................................................................. 23
    3.4.4 Consent Management ......................................................................................... 24
  3.5 PATIENTS RECORDS LINKING AND MATCHING ...................................................... 24

4 LOGICAL VIEW .................................................................................................................... 26
  4.1 CONCEPTUAL RLS-SERVICES VIEW .......................................................................... 26
  4.2 RLS APPLICATION SERVICES ..................................................................................... 28
  4.3 GATEWAY SERVICES .................................................................................................... 30
  4.4 RLS-BASED NETWORKS ............................................................................................... 33
  4.5 REGIONAL AND NATIONAL NETWORK SUPPORT .................................................. 35

5 PROCESS VIEW .................................................................................................................... 36
  5.1 PATIENT LOOKUP AND PEER TO PEER MEDICAL RECORDS RETRIEVAL .......... 36
  5.2 PATIENT INDEX PUBLISH .......................................................................................... 37
  5.3 CENTRALLY MEDIATED MEDICAL RECORDS RETRIEVAL .................................... 37
  5.4 CENTRAL MEDICAL RECORDS AGGREGATION ...................................................... 38
  5.5 SECURITY PROCESSES ............................................................................................... 39
  5.6 MESSAGING PATTERNS .............................................................................................. 41

6 IMPLEMENTATION VIEW ..................................................................................................... 46
  6.1 OVERVIEW ..................................................................................................................... 46
  6.2 COMPONENTS AND LAYERS ....................................................................................... 47
  6.3 IMPLEMENTATION TOPOLOGY OPTIONS .................................................................. 52
  6.4 SECURITY MODEL ......................................................................................................... 54
  6.5 IMPLEMENTATION PLATFORMS .................................................................................... 55
  6.6 INTERCONNECTIVITY AND DATA STANDARDS ....................................................... 56
    6.6.1 Messaging and Transport Standards .................................................................. 57
    6.6.2 Domain Data Standards ..................................................................................... 60
    6.6.3 Comprehensive Standards List .......................................................................... 61

7 DEPLOYMENT VIEW .............................................................................................................. 64
  7.1 SERVICES MANAGEMENT ............................................................................................ 66
  7.2 SECURITY SERVICES ..................................................................................................... 66

8 DATA VIEW .......................................................................................................................... 67
  8.1 CMPI INFORMATION MODEL ...................................................................................... 67
  8.2 LOGICAL DATA MODEL ............................................................................................... 68
    8.2.1 Identifier Attributes .............................................................................................. 70
  8.3 PHYSICAL DATA MODEL .............................................................................................. 72
    8.3.1 Data Quality Management ................................................................................... 74
List of Figures

Figure 1: Architecture views and their contents ................................................................. 12
Figure 2: RLS Long term Concept of Operations ................................................................. 18
Figure 3: RLS Prototype Use Case Diagram ........................................................................ 19
Figure 4 Lookup Patient and Publish Patient Index Activity Diagrams ............................. 22
Figure 5 RLS Conceptual Architecture of Operation ............................................................ 26
Figure 6 Service Oriented Interoperation ........................................................................... 27
Figure 7: RLS Distribution of Components ......................................................................... 31
Figure 8: Gateway based interaction in a health information network ................................ 33
Figure 9 Network of clinical systems communicating peer-to-peer ................................... 34
Figure 10 Network of RLS-based networks (potentially used by RHIO) ......................... 35
Figure 11 Patient Lookup with RLS and Medical Records Retrieval through CDX
   Gateways ......................................................................................................................... 36
Figure 12 Patient Publish into RLS Patient Index ................................................................. 37
Figure 13 Centrally Mediated Patient Lookup and Record Retrieval (hosted gateway) ... 38
Figure 14 Patient Lookup and Records Retrieval -- In One Step ....................................... 38
Figure 15 RLS authentication service .................................................................................. 40
Figure 16: Authentication Mechanisms for Patient Lookup and Medical Records
   Retrieval ........................................................................................................................... 41
Figure 17 Patient lookup sequence diagram ...................................................................... 44
Figure 18 Publish patient index sequence diagram ............................................................ 45
Figure 19 RLS and CDX Gateway components and sample (prototype) implementation
   platforms .......................................................................................................................... 48
Figure 20 Web services stack ............................................................................................... 58
Figure 21 WS-I Basic Profile Web Services stack ............................................................... 59
Figure 22 Interoperability Network Layers ......................................................................... 61
Figure 23 Potential Production Deployment View of RLS .................................................. 65
Figure 24 Information Model View ...................................................................................... 67
Figure 25 Logical Data Model ............................................................................................. 69
Figure 26 Patient Identifier Composition in CMPI ............................................................. 73

List of Tables

Table 1 List of Architecturally Significant Use Cases ......................................................... 20
Table 2 List of Messaging Interactions supported by RLS Prototype ............................... 42
Table 3 CDX Gateway Service / Components Description ........................................... 49
Table 4 RLS Components Description .............................................................................. 51
Table 6 Prototype Platform and Options ............................................................................ 55
1 Introduction

The Record Locator Service (RLS) is envisioned as the key infrastructure component of the ‘Common Framework’, which Markle Foundation Connecting for Health (CfH)† has proposed to facilitate healthcare information networks in the USA. The common framework is a set of standards, policies, and methodologies intended to ensure secure and reliable connectivity between healthcare systems and enterprises.

The common framework includes the essential set of standards and policies that would allow healthcare information networks to interoperate with each other. This would enable communities and regional networks to connect and incrementally grow into a national healthcare information network, as a “network of networks”.

Building a national network through internetworking multiple regional and local health information networks implies a natural bias towards decentralization. A centralized national patient registry or clinical data repository is not considered a realistic objective. Adoption of common architecture and protocols across the networks and sub-networks would, similarly, suggest decentralization in sub-networks, with data stored in separate locations to be accessed when needed. Leaving patient data where they are now, in the healthcare enterprises’ clinical data sources also provides for appropriate patient data privacy safeguards and clear accountability for medical data ownership/stewardship.

This does not preclude sub-networks based on a regional data repository or a community master patient index. As long as the networks support the principles and protocols of the common framework, they would be capable of interoperation with other networks. Smaller participants may choose to use data aggregators to expose their clinical data securely and reliably. As the CfH Roadmap states, “Because many providers will not be able or perhaps willing to provide the levels of service required to participate in a federation, they may have to contract with business associates (in the HIPAA sense) to store their data in a repository that will sustain these service levels.”‡

The common framework that underlies the decentralized healthcare information network is expected to need a small set of critical technical infrastructure components to support interoperability. The RLS is one of them.

† http://www-connectingforhealth.org
‡ [CfH2004]
The RLS provides authorized users of a regional health information network with pointers to the location of patient health information across the network nodes, i.e. the clinical data sources. This would enable users to access and integrate patient healthcare information from the distributed sources without national patient identifiers or centralized databases. Such an integrated view of patient clinical data would help achieve the CfH vision of improved patient safety and quality of care, and reduced costs of healthcare delivery.

Massachusetts SHARE (Simplifying Healthcare Among Regional Entities)\(^8\), a regional collaborative initiative operated by the Massachusetts Health Data Consortium, seeks to foster improvements in community clinical connectivity, allowing appropriate sharing of inter-organizational healthcare data among the various participants in the healthcare system – including patients, doctors and other practitioners, hospitals, government, insurers, HMOs and other payers. MA-SHARE promotes the inter-organizational exchange of healthcare data using information technology, standards and administrative simplification, in order to make accurate clinical health information available wherever needed in an efficient, cost-effective and safe manner.

MA-SHARE’s vision includes the goal of building a utility service that would enable member organizations to hook up to the regional healthcare network (or “grid”) simply and cost-effectively. The RLS architecture advances the design of such a utility service that would connect the healthcare systems in a community securely over the Internet.

This document describes the proposed architecture of the RLS, and provides an overview of the technical components of the common framework. The RLS prototype project tests the architecture presented here and demonstrates the viability of direct peer-to-peer interoperability of disparate electronic health record (EHR) systems that are the ultimate source of clinical data in the network. This document serves as the primary record of all architectural design decisions made in the course of developing the RLS prototype.

\(^8\) http://www.mahealthdata.org/ma-share/index.html
1.1 Purpose

The Framework Technical Overview defines and describes the basic functional components that make up the RLS, and the interfaces between these components. The document presents the RLS architecture using a number of different architectural views to depict different aspects of the system, and outlines the data and transport standards used in accessing the services offered by RLS. RLS plays a critical role in the healthcare interoperability common framework, and the RLS service architecture is aligned with the clinical data exchange processes that the common framework also supports. This document also conveys the architecturally significant trade-offs and decisions which have been made in designing the system and the network.

Business stakeholders may use this document to validate the functionality of RLS in the patient care setting, and to gain understanding of the major services provided by the system. The RLS architecture is intended to serve as a reference for system designers to guide the detailed design of the system during the elaboration and construction phases of a system development project.

1.2 Scope

The Framework Technical Overview provides details of the technical architecture of the Record Locator Service prototype and outlines the strategy to meet the architectural (longer-term) requirements for the RLS as defined in the Markle Foundation Connecting for Health Common Framework Record Locator Service Reference Implementation Statement of Work”.

Technical architecture covers the domains of data, application and technology infrastructure. While technical architecture needs to be developed in the context of the organizational and business process architecture, these domains are out of scope of Framework Technical Overview. This document uses prior work by CfH to define the RLS business context and defines the technical architecture to fulfill the use case requirements thereof. The other important component of the common framework is the policy framework produced by the CfH Policy Sub-committee. This element of the framework was under development during the production of this technical architecture document; policy based requirements have been considered where available.

1.3 References


"[CfH2005a]"
1.4 Document Overview

The Framework Technical Overview document provides a high level overview of the software artifacts that make up the RLS. The document lays out the key business processes that the RLS is intended to support, a logical view of the components and their behavior, and the proposed deployment of the software on completion of development. The remainder of this section defines the concept of software architecture and describes the notation used to document it.

Section 2 defines the goals, principles, and constraints of the RLS architecture.

Section 3 lists the subset of use cases and scenarios that impact the architectural design of the system. Use cases represent the major business or functional requirements that the software is expected to meet.

Section 4 shows the decomposition of the solution into a set of logical elements, i.e., classes, subsystems, packages, and collaborations.

Section 5 presents the process structure of the system. The process view maps the logical view elements to the processes and threads in the solution.
Section 6 presents the implementation view of the system, i.e. the decomposition of the system into layers and packages. Alternative implementation models are presented that may be appropriate for specific scenarios.

Section 7 presents the deployment view, which maps the prototype components to a set of hardware and network nodes on which they execute. Given that this is an architecture document

Section 8 provides a view of the persistent data storage of the system to the extent that this is significant in a network with minimal central data storage.

A glossary of key terms, abbreviations, and acronyms used in this document is provided in Section 9.

1.5 Architectural Representation

The RLS software architecture defines the overall structure of the system in terms of the behavior of its components. Software architecture needs to be viewed from multiple perspectives and at different levels of abstraction to gain a full understanding of the system. In this document, the following architectural views are used:

- Use case view: outlines the functional requirements of RLS from an end-users perspective.
- Logical view: where the major subsystems and components of RLS are identified and a conceptual view of their working provided.
- Process view: describes the runtime behavior of RLS components in meeting key functional requirements.
- Implementation view: provides the organization of the RLS software artifacts in terms of layering and packaging.
- Deployment view: describes how the various RLS software packages and runtime components are deployed on hardware and network nodes.
These views are shown in Figure 1, which illustrates the central role of the use-case (or business oriented) view as the driver of the whole software architecture. This architecture representation follows the ‘Rational Unified Process’ reference architecture standards††. The system stakeholders that are primary audiences of the views are shown in the callout boxes attached to each view.

This document presents architectural views in the form of models (or diagrams) that use the Unified Modeling Language (UML) notation, where applicable.‡‡

The keywords "MUST", "REQUIRED", "SHALL", "SHOULD", "RECOMMENDED", ‘MAY” and “OPTIONAL” in this document are to be interpreted as described in IETF Network Working Group RFC2119§§.
2 Architectural Goals, Principles and Constraints

Architecture best practice calls for the definition of common principles at the outset to serve as a consistent basis for design decisions to be made downstream. Information Technology (IT) architectural principles define the fundamental rules and guidelines for the development and deployment of IT resources and assets. They reflect a level of consensus among the various stakeholders of the system, and form the basis for making coherent and consistent architecture and design decisions.

Architectural principles are, therefore, high level statements that govern the system architecture development process. Based on the CfH charter and the longer term MA-SHARE vision, the following RLS architecture goals, principles and constraints are proposed.

2.1 Goals

The guiding vision for RLS is that to provide directory and registry services for a regional health information network which supports the interoperability between disparate healthcare information systems in a community, reducing healthcare delivery costs and improving quality of care as well as patient safety.

CfH defines the primary objective of the Reference Implementation of the Record Locator Service as: to validate a set of standards that would, if implemented across communities, enable health information exchange within and between communities regardless of the hardware and software platforms used

Such standards and profiles are part of an interoperability architectural framework, which has been referred to as the ‘Common Framework’ by CfH. The technical standards would align with the other components of the common framework, which includes policies and methods.

The RLS is assumed to operate under the auspices of a Regional Health Information Organization (RHIO) that coordinates the various healthcare enterprises in the region (or community). RHIOs serve as distributed hubs of a prospective National Health Information Network.

2.2 Principles

**Patient privacy protection**: Clinical data sharing shall be subject to very stringent privacy and security constraints. All access to patient health data must be secured through strong authentication and authorization, comprehensively auditable, and subject to sanctions for policy violations.
Secure and confidential treatment of patient information shall be a fundamental property of all technological and process artifacts pertaining to RLS. This tenet shall be built into the RLS architecture.

Given the varying privacy regulations existing across states in the US, RLS should support the most stringent protection of health information, including the requirement of explicit patient consent for disclosure of data.

In some cases varying levels of protection are required for different categories of clinical information pertaining to conditions such as mental illness and AIDS.

Decentralized and federated architectures: Respecting the mandate for a de-centralized, federated architecture of healthcare information networks, RLS shall employ federated information architecture ensuring that each node in a RLS connected network retain ‘informational sovereignty’.

A central data repository of aggregated patient healthcare data creates a large target and poses an unacceptable privacy risk in the current political and network environment.

A ‘National Health Identifier’ for each person is impractical in the decentralized world of healthcare in the USA. Instead, RLS would support linking of health records that remain distributed and managed at their points of origin.

Data distribution should be biased to local control of clinical records and access to them. Personal health information should continue to reside where they do now, primarily with hospitals and healthcare providers. Decisions about disclosure of such information should be made at the source of the data, with patient consent if so required.

Users shall be authenticated and authorized to access patient information at the “edges” as well, obviating the need for centralized identity management of all authorized users.

Open Standards: All solutions / components shall be based on open standards and not be dependent on any proprietary technologies. While standards in themselves do not guarantee interoperability, emphasizing standards across the network communication stack helps mitigate most of the common problems that have impeded information sharing in the past.

- HL7 (version 2.x or 3.0) and NCPDP SCRIPT, the de facto industry messaging standards for general healthcare and prescription data respectively, should be used where applicable. The HL7 Reference Information Model offers a ready set of data standards that provide the semantic interoperability underpinning for HL7 messaging standards.
- XML 1.0 is the data message notation standard for inter-application data communication and shall be the default message serialization format.
- New or private network services shall not be required: the solution should be based on secure data transport over the public Internet.

---

"CfH2004a"

Architecture Document Page 14 Version 1.1a
Record Locator Service 2005-11-22
Confidential ©CSC. 2006
Secure Sockets Layer (SSL) protocol, the most widely adopted security protocol standard for the Internet, shall be used.

- ‘Web services’ are the industry standard for platform-neutral, distributed application interoperation over the Internet. Web services should be used to effect data sharing across the health information network.
- The Web Services-Interoperability Organization (WS-I) provides profiles to assure that web services built on disparate platforms have higher assurance of interoperability.

### Vendor and platform neutral

The RLS solution needs to be vendor-neutral to ensure wide-spread adoption of the architectural standards. As an extension of the open-standards principle, this principle stipulates that no dependence on specific vendor technology be introduced.

- Leverage commercial-off-the-shelf (COTS) master patient index solutions for the prototype, but develop the architecture in a manner that future adherents to the Common Framework can make their own build vs. buy decisions.
- Assume that comprehensive integrated application suites are potentially cost-prohibitive for wide-spread deployment across a range of healthcare systems from small family practices to large hospital networks.

### Best Practices

RLS service should be designed for agility and extensibility to meet varying regional clinical data exchange implementation requirements.

- Service-oriented architecture enables applications to be more flexible, and interface well with external facing web-services. Following the service-oriented approach, the RLS application should comprise loosely-coupled coarse-grained components that can be readily reused. However, the internal architecture of the RLS application is not itself relevant to the standards based external messaging that is the primary requirement.
- RLS should support existing regional and community health information networks as well as prescribe best practices and patterns for new networks to adopt.
- Variability across regional networks should be mediated through shared specifications based on the open standards as prescribed above.

### Promote Widespread Adoption

The following system constraints should be taken into account to enable rapid deployment of a solution that builds on the RLS prototype:

- Widespread distribution of the RLS solution demands a light-weight inexpensive solution for all new components at the edges.
- Participants have diverse vendor relationships and must not be bound / committed to any one vendor to benefit from RLS-based connectivity. RLS specifications and standards should be open to implementation by healthcare information technology vendors.
- Standards based, loosely coupled, and flexible design should be used to avoid ‘rip and replace’ implementation across the current healthcare landscape. The architecture should support an
incremental migration from current technology to future standards based interoperability.

- Participants in health information networks have significant investments in EHR and personal health record (PHR) applications. RLS should support connectivity between them, with incremental migration paths that call for moderate incremental investment.

**Flexible Implementation Models**: The RLS architecture should enable top-down and bottom-up implementation strategies, favoring local network infrastructure development to promote widespread usage and national interoperability models to promote inter-regional information sharing. From a technological standpoint, the RLS architecture should support three implementation models:

- **Gateway**: Physically deployable service that may be integrated into RLS subscriber enterprise IT environment, and allowing secure access to RLS.

- **Application Programming Interface specifications**: Allow solution providers (package vendors and custom development shops) to implement RLS components independently on platforms of their choice without detracting from interoperability.

- **Hosted**: All RLS services are hosted for subscribers unable or uninterested in owning and operating the RLS access infrastructure. Such a solution would be an attractive option for smaller physician practices and institutions that prefer to outsource their information technology services.
3 Use-Case View

The RLS system architecture is primarily driven by the functional requirements of the health information network. Functional requirements are captured in use case models or requirements definition documents, as well as vision and mission statements describing the longer term strategy. In addition, architectures have technology drivers and need to be cognizant of constraints of the information processing environment in which the system operates and the technology platforms used to implement the architecture.

The Use Case view represents the end users view of the system, and provides insight into the business goals of the system. Use cases represent the interactions that take place between the system and its users. Use case diagrams provide a schematic view of the end-user requirements that the system expects to satisfy. Use cases do not capture all the functionality of a system, only the users’ activities with respect to the system. Also note that use case specification diagrams need to be supplemented by textual descriptions that provide details of the requirements, which are not provided in this document.

3.1 RLS Functions

RLS is intended to serve as a key infrastructure element in a regional health information network. RLS primarily maintains an index of pointers to the network location of patient information, but not the personal health information itself. The index of pointers is akin to a ‘master patient index’ as deployed in integrated healthcare delivery networks with multiple independent clinical systems maintaining patient records.

RLS serves as a coordinating service that obviates the need for a national health identifier, by linking diverse patient records across distributed clinical data sources through probabilistic demographic matching techniques. Such a service can facilitate a federation of diverse clinical data sources to enable a consolidated view of a patient’s electronic health care records. The clinical data nomenclature includes a range of information from medical records in provider systems, dispensed drug information at pharmacy systems, to administrative and financial information in payer systems.

Various institutional models have been discussed for ownership and operation of an RLS. In the current environment, the logical organizational framework for an RLS would seem to be a regional health information organization (RHIO). RHIOs are considered key elements of the strategy for constructing an interconnected and
interoperable network of networks that forms the national health information network (NHIN).

Massachusetts SHARE (Simplifying Healthcare Among Regional Entities), a regional collaborative initiative operated by the Massachusetts Health Data Consortium, may play the role of a RHIO. One of MA-SHARE’s goals is to create a sustainable community utility for clinical connectivity and data exchange. The future extension of RLS to serve as such a utility is a consideration in its architecture.

While RLS primarily supports individual caregivers by facilitating access to aggregated patient information, it may facilitate information sharing across other authorized stakeholders as well, including the patient. A longer term ‘concept of operations’ view of RLS is shown in Figure 2.

3.2 Use Cases

The architecturally significant use cases of RLS are shown in Figure 3. The primary end user function of RLS is to provide healthcare practitioners with pointers to clinical data stored at distributed network nodes. To establish context it useful to understand the complete usage scenario from a healthcare practitioner’s perspective, which would include subsequent retrieval of patient records. Patient records retrieval is not an RLS function, and is
shown as a separate ‘clinical data exchange’ service in the use case diagram.

Actors are entities (both human and system) that interact directly with the RLS. RLS actors include:

1. Healthcare practitioners: Individual care providers who have been assigned rights to access a patient's clinical record. This category includes providers, payers, diagnostic services etc., as well as the patient.
2. Clinical Data Source: The information systems in use by a healthcare provider or payer to maintain patient related information. Data sources encompass systems at physician offices, hospitals, laboratories, imaging centers, pharmacies and other health care service entities.
3. RLS Administrator: Persons (or entities) authorized to administer the Record Locator Service and the community

---

*Figure 3: RLS Prototype Use Case Diagram*
patient index as may be required. Note: this role is expected to be progressively automated as the RLS implementation matures.

Note that the core RLS function is only to locate patient records. This essentially implies providing indexing services for distributed clinical data sources, which publish patient registry events into the RLS. This separation of services is a key aspect of the CfH strategy which seeks to decouple the standards and policies relating to separate functions of the network\textsuperscript{11}.

The following use cases are architecturally significant to the RLS, in that they exercise critical aspects of the system architecture:

\textit{Table 1 List of Architecturally Significant Use Cases}

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lookup patients</td>
<td>On entry of search criteria by authenticated and authorized users, system shall retrieve a list of patients matching the search criteria entered. System shall return the list of patient records with 'locations' (or web addresses) where these records may be accessed.</td>
</tr>
<tr>
<td>Publish patient index</td>
<td>On entry of new patient records in the clinical data source (e.g. after a registration or ADT event), or upon changes to existing patient records, the clinical data source node shall transmit a set of demographic attributes and a pointer to the patient record (typically in the form of a Medical Record Number) to the patient index maintained centrally at the RLS (the community Master Patient Index, or CMPI) The RLS acknowledges receipt of the changed record information.</td>
</tr>
<tr>
<td>Authenticate authorized users</td>
<td>RLS users are authenticated as authorized network users by the clinical system to which the user is affiliated.</td>
</tr>
<tr>
<td>Communicate securely</td>
<td>RLS and the clinical system communicate securely over the internet. Senders and receivers of messages are mutually authenticated before exchange of messages; message confidentiality and integrity are assured; and message non-repudiation is enabled for both sender and receiver.</td>
</tr>
<tr>
<td>Log messages</td>
<td>All messages are logged with name of user / organization initiating the operation. Logs can be audited for information on all access to RLS patient index.</td>
</tr>
</tbody>
</table>

\textsuperscript{11} CfH2005b
3.3 Use-Case Realizations

The patient lookup and patient publish use cases are both realized through messages sent securely from nodes in the health information network to the RLS requesting lookup and publish services respectively. The ‘lookup patient’ and ‘publish patient index’ use cases are realized in the manner shown in the activity diagram in Figure 4.

The swimlanes in the activity diagrams correspond to the actors shown in the use case diagram. Healthcare practitioners and clinical data sources are roles played by entities such as hospitals, physician practices, diagnostic services, payers, public health agencies etc. Thus, a provider system at a network node could play the role of a clinical data source, and also be the channel through which healthcare practitioners access the RLS.

While the core functionality of RLS is to support publishing into, and searching the CMPI, the RLS-based network would require information processing in each of the nodes interacting with the patient index to support secure, reliable and standards based communication between them. This communication function is the core of the common framework that enables the various network nodes to exchange information with the RLS and with each other. The communication functionality at these nodes share many common processing capabilities which may be encapsulated into a common technology artifact as shown in Section 4.
Other functional aspects that influence the RLS architecture include:

### 3.4 Security, Patient Privacy and Consent Management

Protection of patient privacy is a legal and regulatory requirement that is realized through system security as well as policies implemented by the RLS and the various participants in the healthcare information network. Patient and healthcare practitioner trust in the security and privacy protection features of the RLS-based network is a critical pre-requisite to its success.

Privacy protection is based on restricting network access to the data to only authorized personnel, monitoring all access to patient data to audit the operational use of the network, and implementing architectural safeguards to manage the risk of accidental or malicious spillage of data in the course of network operation.
3.4.1 Identity management

The RLS is intended for use by large networks of healthcare enterprises, each of which may have large user end user populations. RLS must not be required to manage the network identities of all individual users. End users (healthcare practitioners) are authenticated by the enterprise to which they are affiliated and referred to RLS as authenticated principals. Identity management is a local function. Patients who use hospital / IDN patient web sites are referred to RLS as authenticated principals by the clinical systems at the hospital / IDN. RLS and all participating entities have the ability to mutually authenticate each other before exchanging data.

3.4.2 Confidentiality, Authentication, Integrity & Non-repudiation

The RLS network architecture uses the following high level security requirements in implementing messaging as well as application data management:

- **Confidentiality:** Information shall only be disclosed to authorized users who need it for healthcare treatment, payment, or operations.

- **Authentication:** Receivers of requests for information shall be able to verify the identity of the requester. A network participant shall not be able to masquerade as anybody else.

- **Integrity:** Communication between network entities shall be protected against unauthorized alteration, and all alterations shall be logged. Receiver shall be able to verify that the message has not been altered.

- **Non-repudiation:** Transactions cannot be unilaterally revoked or altered by either party. A sender cannot falsely deny sending a message and a receiver cannot falsely deny receipt of a message.

3.4.3 Patient Data Privacy

The health information network is architected on the presumption that data privacy is easier to protect locally, i.e. on the edges of the network where data are stored. Release of information from the clinical data source to healthcare practitioners is governed by policies established and maintained by the data source.

RLS, being a directory of patient record locations, is itself a source of protected health information. RLS shall publish and maintain a clear policy governing discovery of patient information in the directory. The specific rules governing sharing of RLS directory information pertaining to individual patients are created by the patient and provider at the time of the encounter and communicated to the RLS along with the message of that encounter event.

Healthcare information networks need to pay special heed to ‘sensitive’ data disclosure:
There are categories of medical information that need additional safeguards which RLS should be cognizant of. These include mental health, AIDS, and substance abuse related care data.

While RLS does not itself retain patient care data, the availability of patient records at a mental health facility is itself disclosing. RLS access control policies should be informed by such considerations.

The patient consent process should be capable of allowing the patient to set varying restrictions on the different categories of sensitive data.

A 'break-the-glass' function should allow authorized providers to override patient privacy constraints in emergency situations that require access to sensitive data.

3.4.4 Consent Management

Some states require that explicit patient consent be obtained to share their medical records across the network. There are varying degrees of restrictions of privacy / consent requirement and RLS must be capable of handling this variability. The following policies have been proposed for the RLS-based health information network to manage the consent process:

- Require that patients be fully informed in writing of a provider’s or health plan’s participation in the RLS before their information is exchanged through the network;
- Mandate that the written notice given to patients contain certain disclosures about how information is used and exchanged through the RLS;
- Permit providers and health plans to include the disclosures about the RLS in their HIPAA privacy notices;
- Give each patient the right to decline to have their information exchanged through the RLS (“opt-out”); and
- Prohibit providers and health plans from withholding treatment or benefits to patients who have opted out.

3.5 Patients Records Linking and Matching

The key function of the CMPI is to link patient records across different institutions, each of which maintains patient data independently and, often, inconsistently. Various algorithms are available for matching person records based on limited sets of demographic attributes, for which software implementations exist. The algorithms should match the patient attributes used as search criteria with those in the CMPI records using NYSIIS matching, digit transposition checks, etc. RLS should be capable of using integrating with a variety of patient matching software.

Two models exist for implementing the linking / matching process:

- Patient records may be linked when they are loaded based on running a matching algorithm with the rest of the patient records in the database. An online query would then be matched using the same algorithm to the pre-linked records. This process is typically supported with some level of human disambiguation of data. For
example a data administrator may examine records that match marginally and manually ascertain a positive or negative match. Note: this function could potentially grow into a large data maintenance organization.

Matching is done during a RLS patient lookup query, but no explicit linking of records is done in the CMPI database. Very fast database matching speeds have been achieved using probabilistic algorithms that also provide high assurance of no false positives. A disadvantage is that this completely automated process could potentially result in higher false negatives. Patient privacy considerations (no false positives) imply high thresholds for probabilistic matching, which would miss patient records that match marginally.

Human disambiguation of patient matching results is considered undesirable. While an interactive narrowing down of patient matches may be appropriate within a hospital setting where the degree of trust is high, this is considered unacceptable when RLS is serving as a CMPI to multiple institutions. Therefore, probabilistic matching algorithms should have their positive match threshold set high enough to reduce the percentage likelihood of false positives to negligible levels.

RLS patient lookup service shall not support wild-card matching. This could open the door to database fishing which would be an egregious violation of patient privacy principles.

RLS should support the retrieval of record locations using a local patient ID.
- There could be situations where a patient is well-identified locally (e.g. has a long-established MRN). It should be possible to get the linked records from RLS rather than do a demographics attributes based search
- This may technically be considered a subset of the demographics based search. RLS maintains both patient source institution and institution local MRN.
4 Logical View

The architecturally significant subsystems / components that make up the RLS are identified and their interactions that provide the required services are described in this section. A top-down approach is taken starting with the high level functional component view, and decomposing this into more granular components that can be translated into system components and services.

4.1 Conceptual RLS-Services View

Based on the activity diagram that defines the RLS patient lookup process it is clear that functionality is required at three processing nodes. These are the healthcare practitioners, the clinical data sources, and a patient index.

A conceptual view of the interaction between RLS and its ‘subscribers’ may be viewed as shown in Figure 5.

By maintaining the patient index pointers to patient record locations in multiple clinical data sources systems, RLS serves as a directory of patient records in clinical systems. Besides the patient index, the RLS also maintains the registry of all members of the network, and their network addresses.

This model is seen to very similar to the classic service-oriented invocation paradigm where the service consumer, provider, and broker interact in the ‘publish / bind / find’ pattern, as shown in Figure 6. This similarity suggests that RLS should play the role of a patient record registry and that clinical data sources should be
exposed as services that are accessible via open standards based messaging interfaces.

Service oriented architecture (SOA) is an architectural style that promotes system agility and extensibility through loosely-coupled software components interoperating through generic messaging interfaces. Interfaces may be separated from implementation by expressing application semantics through XML messaging interfaces. Extensibility should allow new versions of the service to be published and consumed without breaking the existing service, which is facilitated through XML Schema versioning.

Web services are implementations of SOA across enterprise boundaries where interfaces use Internet transport protocols (HTTP, SMTP, and FTP). Web service communications commonly use SOAP protocols for message packaging and WSDL for service description. Service brokers and registries are also accessed through SOAP messages. Thus, in keeping with the architectural principles set out in Section 2, RLS should be implemented as an Internet accessible service using standard protocols such as SOAP and WSDL.

In addition, RLS should use healthcare domain data standards that support semantic interoperability with the various clinical systems. This would expose the resources managed by RLS (i.e. patient index) to consumers in the network through a standard representation based an industry standard information model, such as the HL7 RIM. HL7 v3 messages are derived from the RIM and, therefore, have intrinsically better semantic interoperability characteristics than earlier versions.

There are practical difficulties in implementing the above open-standards messaging interface based interaction pattern in a healthcare information exchange setting:

- While a large number of clinical systems support HL7 2.x messaging and interface with other systems within enterprise networks, message implementations are not consistent and inter-enterprise data sharing

![Figure 6 Service Oriented Interoperation](image-url)
is difficult. Use of HL7 RIM is not widespread in the industry and HL7 v3 implementations are extremely scant.

- Most clinical data sources do not conform to inter-enterprise interoperability messaging standards, and very few are ‘Web service enabled’ to consume or provide Web services.
- Canonical message formats are essential to support practical peer-to-peer information sharing. Otherwise, in a network with n nodes sharing data, it is likely that the number of distinct translations for each message exchange (request/response) is of the order of: n x (n-1).

RLS provides the master patient index service to locate patient records at distributed clinical data sources, components to interface with each of the clinical data sources, and canonical data formats for the patient index publish and lookup messages.

4.2 RLS Application Services

The common framework does not place any requirements of the RLS internal application architecture. As long as the external RLS interfaces conform to the proposed messaging standards, interoperability does not depend on the implementation details of the service. Nevertheless, the following discussion provides guidelines based on the experiences with RLS prototype development that are expected to be useful for other RLS implementation projects. As the discussion below shows, the use of SOA principles enables flexible implementation models, and network topologies while conforming to essential interoperation standards, which is a primary requirement of the common framework.

As discussed in Section 4.1, services are application components that expose their functionality through standard interfaces. In addition, the service model is fractal in that services may be created by combining other services to expose new, aggregated capabilities. Such an aggregation is also called an ‘orchestration’ or ‘composition’ of services. The ‘composability’ of services is important to the agility of SOA applications, and to understanding the RLS application architecture.

Following the service-oriented approach, the RLS application is logically structured as an aggregation of coarse-grained loosely-coupled services. In systems architectures it is useful to classify services as business services or infrastructure services. Infrastructure services are reused across multiple business services, enabling cost effective systems development and operations. The RLS is composed of multiple services, both business and infrastructure. The core business service provided by RLS is:

- Patient index service
  - Responds to patient lookup queries with a list of patient record locations
- Accepts patient index (record location) updates from clinical data sources.

RLS business services are supported by common infrastructure services such as:

- Security: Services that handle user identity management, authentication and authorization, protection of patient privacy, and consent management.
- Systems management: Covering automated administration, installation, configuration, and operational monitoring, control and optimization of systems.
- Logging: To meet auditing and system maintenance requirements
- Data services: Provide persistent storage and management of data, as well as common data access mechanisms for application components.
- Message transport: Enables reliable, synchronous, message based communication between system components.
- Message transformation: Overcomes the real-world problem of disparate data format standards supported by different systems.
- Web-services interface: Leverages the numerous WS-* standards to expose RLS services through XML based messaging API accessible over HTTP transport networks.

Web service interface services may be categorized as belonging to certain standard architectural patterns, called ‘service gateway’ and ‘service interface’††††. The service gateway is an agent, encapsulating the details of communicating with remote web services, and enabling legacy applications to consume web services. The ‘service interface’ is a façade, encapsulating the legacy application by overlaying a web services wrapper, and enabling remote systems to communicate to it.

Technically, RLS can be implemented as a composition of the above services to provide services to remote applications over the globally available Internet. But in recognition of the practical constraints of legacy clinical systems, the architecture also provides guidance on connecting clinical systems to RLS. This may be accomplished through a web service interface as listed above and:

- Adaptors: Facilitate connections to clinical systems and databases through database interfaces or custom API.

The message transformation, web services interface and adaptor components are the key infrastructural service for the interoperation of disparate clinical systems. Essentially, these infrastructure services expose the RLS patient index as well as clinical systems as web services, and enable them to consume web services. Thus connectivity in the network is established using platform and payload agnostic, open standards.

4.3 Gateway Services

Following the principle of deploying applications as aggregations of loosely coupled services, the infrastructure services listed above could be bundled to form a composite ‘Clinical Data Exchange (CDX) Gateway’ for the clinical systems to interoperate with each other. By designing the CDX Gateway to support general purpose, secure, and reliable messaging between clinical systems, it serves as the standards-based on-ramp to a health information network.

The RLS may be realized as the orchestration of the following two service compositions, which may be considered as the business service and infrastructure service respectively:

- Patient Index: Central service that maintains the community patient index, and a registry of clinical systems with routing information to direct service requests and responses to appropriate end-points.
- CDX Gateway: Distributed service that interfaces to each network node, converts from the legacy data messaging format to the standard message (if needed), and communicates to other gateways in the network through Web services.

The CDX Gateway needs to be a small footprint, low-cost service that can be deployed in participant institutions with minimal customization to interface with disparate clinical systems on one side, and to other Gateways via the public Internet on the other. A CDX Gateway is also deployed at the RLS to support messaging with the other network nodes, exposing the Patient Index to external systems through this common utility component.

Such a gateway serves as a general purpose utility to support medical records retrieval as well as RLS communication services. Users acquire patient record locations (pointers) from the RLS and access data from multiple clinical data sources as shown in Figure 7. Note the parallels with the conceptual architectural vision in Figure 5.
As may be seen from Figure 7, communication between all network nodes is through the CDX Gateway at that node. In addition, presentation and business services would be required for the user interface functionality of the RLS (patient search criteria entry, and selection of patient record locations to query). Online users would log into the CDX Gateway co-located with the clinical system to which they are affiliated and access RLS services.

The collection of clinical systems that hold patient medical information at each network node is called the Electronic Health Record (EHR) in the figure, and in the following discussions. In the figure an online interaction is shown at the CDX Gateway at EHR-1, whence the patient lookup request is made to the RLS. The other nodes EHR-2 and EHR-3 serve as clinical data sources. Data retrieval from backend systems at the clinical data sources is done through the adaptor services in the CDX Gateway. The data sources publish patient index updates to the RLS also via the CDX Gateway services at those nodes. Although not shown in the figure, online users at EHR-2 and EHR-3 can also access patient lookup services at RLS (and other clinical data exchange services).
RLS receives service requests through a CDX Gateway at its location. RLS needs an administrative user interface to manage the application, which would be the responsibility of the presentation and business services in the gateway at the RLS.

The gateway based architecture provides significant flexibility and scalability. More clinical data sources could be added by deploying a CDX Gateway at that location and customizing adaptors to connect with the clinical system there. The Gateway transforms local message formats into standard ones and manages their secure, reliable communication to other Gateways.

In general, the expectation is that CDX Gateways that are approximate clones of each other would simplify deployment, configuration and administration of this distributed service. The CDX Gateway, thus, serves as a general utility service that may be plugged in at different EHR locations. In addition the CDX Gateway serves as an infrastructure component which realizes the common framework standards in a packaged form.

CDX Gateway application architecture is based on a multi-tiered pattern of presentation, business, and data and integration tiers. The integration tier is the service that interfaces with clinical systems / data sources at the backend, and communicates with remote Gateways through orchestrated web services at the other. Gateways also include capability to serve as messaging intermediaries. This is a side-effect of implementation of WS-* standards which include WS-Security and WS-Addressing in the CDX Gateway that enables secure, reliable SOAP intermediary functionality.

A more detailed view of the CDX Gateway and its interaction with other gateways is shown in Figure 8. The distribution of functionality between a pair of communicating Gateways is flexible, dependent on the capabilities available at the clinical systems at each network node. The architecture shown in Figure 8 depicts the two EHR nodes playing distinct roles: healthcare practitioner and clinical data source. There are no backend clinical systems at the healthcare practitioner node and the presentation and business services are not deployed at the clinical data source. Within the gateway, the message handling, clinical system adaptors and web service interfaces are shown encapsulated in an Integration Broker service.

It is expected that each CDX Gateway deployment initially requires significant custom localization of the Integration Broker service to cater to EHRs that do not conform to prescribed standards. Over time clinical systems are expected to develop standard Web service interfaces. This would reduce the processing requirements of CDX Gateway, and would enable lighter weight Gateways to be directly pluggable into the data sources.
CDX Gateways communicate with each other using Web services protocol (WSDL and SOAP) over the standard HTTP/SSL transport protocol. Gateways could extend in future to adopt alternate transport protocol such as Secure FTP for batch file transfer, and SMTP using industry standard S/MIME encryption for email.

4.4 RLS-Based Networks

The RLS-based network strategy may be summarized as: Web-service enabling clinical systems. Nodes communicate with each other through HL7 (or other domain-specific standard format) messages wrapped in SOAP envelopes over HTTPS transport. Such a peer-to-peer clinical information network is shown in Figure 9.
Figure 9 Network of clinical systems communicating peer-to-peer

The diagram shows diverse ways of deploying CDX Gateway to connect health information network participants to RLS. While clinical systems routinely send patient index updates to the RLS, users connect to RLS, via their local clinical system, to query patient record locations (patient lookup). Patient lookup can also be done in a non-interactive manner through request / response messages exchanged between gateways at EHR locations and the RLS. In addition a user can query RLS from anywhere on the Internet using only a thin viewer. This mode requires the CDX Gateway at the RLS location to serve up the user interface and business logic much as a gateway at an EHR location would. Since CDX Gateways are clones of each other, this can be achieved by configuring the services in the RLS gateway appropriately.

In addition, it should be noted that the gateway service could play the role of a data cache. The data storage layer in the CDX Gateway (see Figure 8) could potentially hold a data repository into which clinical data is replicated from the EHR and made available to network access. Indeed, it is thought that clinical enterprises would likely prefer to have database queries be directed at such a proxy cache rather than exposing operational systems to remote queries over a health information network.
4.5 Regional and National Network Support

Current thinking on national health information network envisages interconnected exchanges hosted by Regional Health Information Organizations (RHIOs). Such a network of networks is shown in Figure 10.

Figure 10 Network of RLS-based networks (potentially used by RHIO)

The RLS architecture itself presumes no regional dimension; the scoping function of the RLS is the community master patient index that maintains pointers to patient records in distributed EHRs in the community. However, RLS clearly is a candidate for the central coordinating service of a RHIO network. In regards to inter-RHIO communication, it is easy to see that the RLS could also play a key role in routing and coordination of services across RHIOs.

Some RHIOs may be based upon a centralized data repository as determined by regional policy considerations (as well as legacy architectural considerations); others are decentralized. Both models, as well as intermediate ones, are supported by the proposed NHIN architecture. Using a common framework based on open standards and common policies allows a RHIO to be agnostic about the architecture of another RHIO. The service oriented CDX Gateway architecture also enables a degree of flexibility in implementation styles and operational configuration as discussed further in the following section.
5 Process View

The RLS application is a collection of loosely-coupled interoperable services, and is itself a service that can be invoked by external consumers. Components that are distributed across network nodes communicate via XML messages using Web service standards, primarily SOAP and WSDL. Additional Web service standards may be used to support reliable messaging, error handling, and security.

The essential RLS functions to fulfill the patient lookup and publish patient index use cases are realized through distributed processing of the RLS services as described below.

5.1 Patient Lookup and Peer to Peer Medical Records Retrieval

The patient lookup process may be visualized as shown in the simplified communication diagram in Figure 11, where the flow of information and messages between the distributed processing components may be tracked through the sequence numbers provided.

![Diagram of Patient Lookup with RLS and Medical Records Retrieval through CDX Gateways](image)

Figure 11: Patient Lookup with RLS and Medical Records Retrieval through CDX Gateways

The interaction diagram illustrates the use of gateways to manage all communications between network nodes. Gateways also encapsulate presentation, business, and data access services thereby providing a full application stack for flexible implementation of RLS services. For example, while the patient lookup is shown as an interactive process it could as well be transacted offline, in batch mode.
5.2 Patient Index Publish

The patient publish process is simpler in that it is a notification-type background interaction. The initiating message is triggered by a registration event at the clinical data source and essentially serves to update the patient index with details of the patient whose record has been updated, i.e. added, revised, cancelled, or merged with another patient record in the clinical data source. This interaction is shown in Figure 12.

![Patient Publish into RLS Patient Index](image)

Typically, patient registrations are maintained in ADT systems in hospital environments. An ADT event message is broadcast to the other ancillary systems in the hospital such as laboratory, radiology, transcription, etc. The RLS patient publish message is generated by tapping off the same broadcast ADT message, requiring minimal changes to existing hospital systems. While this message is notification only, a basic exception handling capability needs to be built, where errors in posting the update to the RLS patient index are communicated to the data source. If the error does not require reentry of the ADT transaction, a mechanism to fix the data problem and resend the message to RLS needs to be built in the clinical system or interface engine.

5.3 Centrally Mediated Medical Records Retrieval

The scenario shown in Figure 11 represents a federated architecture, supporting peer-to-peer clinical data exchange. Alternate scenarios exist, such as a hub and spoke model where patient medical requests are mediated by a central gateway service. The collaboration diagram below demonstrates how a user could log in directly to a central CDX Gateway (in this case, co-located with RLS) and perform the same function.
Note that the healthcare practitioner is shown as logging directly into the gateway at the RLS location and executing the patient lookup query directly on RLS. This is another variation of the use of the CDX Gateway, and demonstrates the implementation flexibility a standard gateway utility based network architecture allows.

### 5.4 Central Medical Records Aggregation

Yet another processing model would remove the need for a two step process altogether and have the patient lookup request be combined with a medical records request which the CDX Gateway at the RLS would orchestrate. Such a scenario is shown in Figure 14.
This interaction pattern is more appropriate for unattended RLS usage where a clinical system collects remote patient records and has them ready for review by a healthcare practitioner at later time. The orchestration process in the CDX Gateway is now more complex and should implement workflow processes of the healthcare practitioner, including selection of appropriate medical records to retrieve from various sources.

Other supplementary processes include the need for secure information sharing, and the establishment of contracts between the RLS and the various clinical data sources that would share patient medical records with each other. In both of these situations RLS, serves as a trusted intermediary, and reduces the need for the many-to-many relationships between the various clinical data sources. The secure messaging process is described below.

5.5 Security Processes

RLS needs a security framework to authenticate users, authorize access to specific services, and ensure confidentiality and integrity of messages. The implementation of security across a disparate, distributed computing network is optimally effected through a federated identity management architecture, where each user is authenticated by an assigned node that vouches for the user to other nodes. Federated security architecture is complex and considered beyond the scope of the current release of RLS. RLS uses a simpler model that can be extended to a federated architecture in later releases.

A distributed authentication/authorization architecture that is based on overlapping trust relationships is shown in Figure 15. Users’ identity and credentials are maintained at the gateway that they log in to. Gateways are within the clinical enterprise domain, and may be integrated with the enterprise security infrastructure to support single sign-on for users. Gateways are in a trust relationship with other gateways and authenticate each other through server-side certificates. An authentication / authorization assertion is communicated in the SOAP message along with the user identifier string for audit purposes.

Secure Socket Layer (SSL) is a session layer protocol for sending encrypted information over HTTP. SSL provides an encrypted channel with confidentiality, integrity and one-way or two-way authentication. SSL is used to secure messages between gateways in the RLS-based network. Gateway authentication may be provided by server-side digital certificates.
Over the longer term, CDX Gateways should leverage WS-Security, the emerging security standard for SOAP messaging, where different security tokens are embedded in SOAP Headers. The XML Signature and XML Encryption standard provides a platform neutral approach to message-level authentication, confidentiality, integrity, and non-repudiation.

Security Assertion Markup Language (SAML) provides a technology neutral way to exchange security information using XML to communicate authentication, authorization and other user attribute information. SAML also allows interoperability across different platforms such as J2EE, .NET and CORBA. WS-Security supports the use of a SAML token in the SOAP header.

The distributed authentication process implemented in the RLS prototype is shown in more detail in Figure 16.
5.6 Messaging Patterns

RLS defines contracts to govern message exchanges that implement services. These message exchange patterns, or message scenarios, are the basic transactions that Web services are designed around. The logical components and services described in the previous section may be considered as the ‘plumbing’ (or the Common Framework) for the health information exchange. The framework is capable of supporting various message scenarios that support multiple use cases.

There are four common messaging interaction patterns that characterize service oriented scenarios:

**Patient Lookup**
1. User logs in / enters patient lookup query (demographics)
   a. authenticated against directory
   b. access logged
2. Request for patient record locations in SOAP envelope with user identity / roles over
   c. sender-side certificate used to sign message and receiver certificate used to establish SSL / TLS connection
3. Matching patient record locations looked up
   d. remote system authenticated against registry
   b. access logged
4. Matching records from CMPI returned
   c. sender-side certificate used to sign message and receiver certificate used to establish SSL / TLS connection
5. Patient record locations displayed for user selection

**Medical Records Retrieval**
6. Patient clinical records query entered
7. Request for patient medical records request in SOAP envelope with user identity / roles, and server key
   d. remote system authenticated against registry
   b. access logged
8. Patient clinical records retrieved
9. Clinical records returned to user
   c. sender-side certificate used to sign message and receiver certificate used to establish SSL / TLS connection
10. Clinical records aggregated and displayed to user

*Figure 16: Authentication Mechanisms for Patient Lookup and Medical Records Retrieval*
* One-way: or fire-and-forget messaging, involves the sending of a message from requester to provider with no acknowledgement expected

* Request / Response: implies that a response message is generated for every request received by the provider

* Notification: may be considered a mirror image of the one-way pattern, where the provider sends a one-way message to the requester

* Solicit response: is the reverse of request / response in that the service provider sends a solicitation for a request to a requester

The contract between service provider and requestor is defined using a standard XML based language called Web Services Description Language (WSDL). Note that the WSDL 1.1 messaging terminology above have been superseded in the WSDL 2.0 specifications with more precise names; these do not have a material impact on the RLS specifications and are not used.[1]

The message scenarios supported by RLS prototype are listed below:

<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Triggering Event</th>
<th>Interaction Type</th>
<th>Sender</th>
<th>Receiver</th>
<th>Receiver Responsibility</th>
</tr>
</thead>
</table>
| 1  | Lookup patient locations      | Practitioner receives consent from patient to retrieve medical history         | Request / Response     | Practitioner (via CDX Gateway) | RLS      | Search master patient index
Match patients using linking algorithm
Return list of patient locations (clinical systems) and MRN |
| 2  | Publish patient index         | Registration of new patient into Clinical System
Patient consent is pre-requisite | Notification           | Clinical System (via CDX Gateway) | RLS      | Patient basic demographics and MRN (as maintained in the Clinical System) used to update CMPI. |
| 3  | Message logging               | Passing of message through gateway                                             | One way                | CDX Gateway              | RLS      | Insert log message into standard format logging database                                  |

<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Triggering Event</th>
<th>Interaction Type</th>
<th>Sender</th>
<th>Receiver</th>
<th>Receiver Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Exception logging</td>
<td>Error condition in message processing</td>
<td>One way</td>
<td>CDX Gateway</td>
<td>RLS</td>
<td>Insert error message into standard format logging database and notify Administrator</td>
</tr>
<tr>
<td>5</td>
<td>Retrieve medication history records:</td>
<td>Authorized practitioner submits request. Patient consent is pre-requisite</td>
<td>Request / Response</td>
<td>Practitioner (via CDX Gateway)</td>
<td>Clinical System via CDX Gateway</td>
<td>Return requested medication history list in a standard message format</td>
</tr>
</tbody>
</table>

Each message scenario assumes that an error message (SOAP Fault) is returned by the receiver to the sender if the message results cannot be parsed or results in any application error.

The flow of logic across the different service layers in the RLS / CDX Gateway solution architectures is shown as sequence diagrams in Figure 17 and Figure 18 where the application process logic may be visualized as a series of messages exchanged between application services. The services oriented architecture is realized through implementation of messaging between application components, as shown here. Figure 17 depicts the interactions between RLS application components to provide the patient lookup service to users logging in to remote gateways.
Figure 17 Patient lookup sequence diagram

As can be see in the figure, the Gateway services communicate with each other through the integration broker services.

The other core RLS service is that of accepting updates to patient indices from clinical data sources and applying them to the RLS CMPI. This may be visualized in the sequence diagram in Figure 18.
Figure 18 Publish patient index sequence diagram
6 Implementation View

This section describes how the relevant components of the RLS logical architecture are implemented. While the logical and process views provide more conceptual models of RLS, the implementation and deployment views relate more to the physical artifacts that make up the RLS-based interoperability framework. The implementation view presents a more detailed view of the organization of the static software elements of the RLS prototype than was presented in the logical view.

Note that implementation of systems based on the RLS architecture is to be undertaken by individual RHIOs, which have significant latitude of action. Each RHIO may choose implementation strategies based on their internal development methods and platform preferences. This section provides only generic implementation related information, and refers to the RLS prototype implementation architecture and platform for purely illustrative purposes.

RLS architecture is generic and platform agnostic, with interoperability based on open connectivity standards such as Web services, and semantic data standards such as the HL7 Reference Information Model. This section also outlines the relevant standards prescribed for an RLS implementation. Given that interoperability is critically dependent on the communication and data standards adopted, the expectation is that each implementation adheres closely to the recommended standards and specifications. More detailed guidance on implementing message format standards and specifications is provided in a separate document: RLS Messaging Communication Implementation Guide.

6.1 Overview

RLS is a classic n-tiered database application with a web-browser based user interface, and capability to interoperate with remote systems using open standard messaging over the Internet. The key interoperability function is realized through implementing a gateway service at each node in the network that provides essential presentation, business and data services and the ability to communicate with other gateways using web services and domain specific data standards. The RLS application may be viewed as comprising two large grained components (or service compositions).

- Patient Index service maintains and enables access to the community Master Patient Index (CMPI) and maintains a community directory / registry for the various clinical data sources, data and message standards, etc.
CDX Gateways provides a ‘web-service’ wrapper and other utility services to support message based interoperation for the RLS as well as for each clinical data source in the network.

The patient index service architecture essentially comprises components that provide Patient Record Linking / Matching and Patient Record Search services. The CMPI database contains basic patient demographic information and patient identifiers as maintained in the various clinical data sources that publish into the CMPI. Each patient record is tagged with the network resolvable address of its source.

The unified patient view is achieved through linking / matching of patient records based on demographic attributes. Record matching may use deterministic (exact) matching of patient demographic attributes or a probabilistic algorithm which takes into account the variations in source data due to data entry anomalies. The architecture implementation supports the swapping of matching algorithms by change of run-time parameters.

CDX Gateways enable the interoperation of backend legacy clinical systems with each other and with the RLS through exchange of messages (of various formats) with other gateways using Web services protocols over HTTP transport secured with SSL/TLS (or HTTPS).

6.2 Components and Layers

A logical view of the RLS application architecture was presented in Section 4.
A more detailed breakdown of the components of the RLS, their logical groupings (layers), and implementation platforms used in the prototype project is shown in Figure 19.

Figure 19 RLS and CDX Gateway components and sample (prototype) implementation platforms
The diagram shows one EHR node (comprising a clinical system and a gateway) connected to the RLS. One may imagine many such nodes also communicating to the RLS through the Web service interface component in the Integration Broker service of the gateway. CDX Gateways interface with the local clinical systems through the EHR adaptor. A design objective would be to isolate and layer services such that only the adaptor components in the Integration Broker service layer would need to be customized for each site where the Gateway is deployed.

The service layers are independently deployable units, which are orchestrated by a service broker or bus. For example, the security and systems management layers are shared across multiple business application services. Thus, all the service layers are loosely-coupled and reusable. Implementations of RLS may vary based on the specific needs of the site, with the potential for sites to tighten coupling as necessary. They may also use alternate infrastructure services (e.g. security) that conform to local standards as long as they also honor the interface standards used for RLS.

More details of the functionality of each of the components that comprise the service layers are provided in Table 3.

<table>
<thead>
<tr>
<th>Service / Components</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Presentation Services</td>
<td>Formats data display to meet end user interaction and display device requirements</td>
</tr>
<tr>
<td>Login</td>
<td>Enter username and password to gain access to RLS</td>
</tr>
<tr>
<td>Lookup Patient</td>
<td>Patient demographics data entry</td>
</tr>
<tr>
<td>Review / Select from Patient Index list</td>
<td>Present list of potential matches of patients to demographics data entered, to be selected from</td>
</tr>
<tr>
<td>Request Patient Records</td>
<td>Selection of specific patient medical records to be retrieved from source</td>
</tr>
<tr>
<td>View Aggregate Records</td>
<td>Present patient medical records received from multiple sources in common format</td>
</tr>
<tr>
<td>Monitor Messages</td>
<td>View log of messages passing through RLS</td>
</tr>
<tr>
<td>Manage Access Control Policies</td>
<td>Create and maintain access control policies</td>
</tr>
<tr>
<td>Manage User Identities</td>
<td>Create and maintain user identity information and roles to which assigned</td>
</tr>
<tr>
<td>Business Application Services</td>
<td>Key functional components that house business rules and execute business logic on clinical data to render it comprehensible to the healthcare practitioner</td>
</tr>
<tr>
<td>Patient index</td>
<td>Patient index business object</td>
</tr>
<tr>
<td>Medical records aggregation</td>
<td>Application object that merges medical records received from multiple clinical data sources</td>
</tr>
<tr>
<td>Medical records request</td>
<td>Standard application object that mediates the data request entered by users on a screen and the data access services</td>
</tr>
<tr>
<td>Auditing Services</td>
<td>Support the auditing of access to medical data using logs of all significant events in gateway operations</td>
</tr>
<tr>
<td>Medication list</td>
<td>Meds administered business object</td>
</tr>
<tr>
<td>Lab / Micro / Radiology</td>
<td>Laboratory, microbiology, radiology results business object</td>
</tr>
<tr>
<td>Images and Waveforms</td>
<td>ECG/EEG graphs, Radiology imaging etc.</td>
</tr>
<tr>
<td>Service / Components</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Notes / Reports</td>
<td>Clinical documentation business object</td>
</tr>
<tr>
<td>Visit History</td>
<td>Patient encounters business object</td>
</tr>
<tr>
<td>Problem list</td>
<td>List of current diagnoses business object</td>
</tr>
<tr>
<td>Data Management Services</td>
<td>Manage application access to data storage and processing of data in data storage layer.  Isolates the business layer from the details of the data storage service.  Supports management of metadata about data stores and repositories in system</td>
</tr>
<tr>
<td>Persistence / Data Access</td>
<td>Provide standard data access to business application services that is independent of the underlying data storage technology or database management systems</td>
</tr>
<tr>
<td>Code sets and Key management</td>
<td>Manage disparate code sets and generated keys for data imported from multiple systems</td>
</tr>
<tr>
<td>Replication, backup, data cache management</td>
<td>Technical data management services. Support data aggregation and asynchronous data streams management.  Data cache for clinical data (where required).</td>
</tr>
<tr>
<td>Data Storage Services</td>
<td>Provide reliable, secure data storage for efficient access by data management services</td>
</tr>
<tr>
<td>Data Cache</td>
<td>For storing temporary copies of data retrieved from clinical data sources for faster response to user queries.  This could be a significant component for pilot / production implementation since it buffers the clinical data sources from external queries.  However, there are significant business and technical issues to be resolved for clinical data caching.</td>
</tr>
<tr>
<td>Message store, Logs and Audit</td>
<td>Persistence mechanism for reliable messaging and for monitoring of message flow (may be part of System Management Services)</td>
</tr>
<tr>
<td>User directory, Certificates store</td>
<td>Data store for security services layer  (may be part of Security Services)</td>
</tr>
<tr>
<td>XML Schema and metadata services</td>
<td>Repository of message and data standards for reference – both run time and design time</td>
</tr>
<tr>
<td>Integration Broker Services</td>
<td>Manages flow of messages through the Gateway that serves RLS and the clinical systems that communicate with RLS</td>
</tr>
<tr>
<td>Message Queuing and Transport</td>
<td>Provides store-and-forward capability and manages connection to messaging infrastructure.  Supports asynchronous messaging between loosely coupled services</td>
</tr>
<tr>
<td>Message translation</td>
<td>Transform message formats based on mappings</td>
</tr>
<tr>
<td>Routing / Orchestration</td>
<td>Routes messages to the appropriate destination channels</td>
</tr>
<tr>
<td>Web Services Interface</td>
<td>SOAP and WSDL processing along with other WS-* service implementations, e.g. reliable messaging, error handling, security</td>
</tr>
<tr>
<td>XML Processing</td>
<td>Serialization/deserialization of messages, validation of messages against XML schema, and translation from one schema to another using XSLT</td>
</tr>
<tr>
<td>HL7 Mapping</td>
<td>Conversion from HL 2.x messages to RLS standard formats (HL7 v3)</td>
</tr>
<tr>
<td>EHR Adaptor</td>
<td>EHR system specific component with ability to extract required medical records from EHR system</td>
</tr>
<tr>
<td>MPI Adaptor</td>
<td>Component to interface with Master Patient Indexes (including CMPI)</td>
</tr>
<tr>
<td>SQL / Replication / ETL Adaptor</td>
<td>Data movement from one data store to another, includes transformation as needed and typically executed in batch (bulk) mode</td>
</tr>
<tr>
<td>Systems Management</td>
<td>Besides application management functions shown below, extends over the long term to cover remote deployment</td>
</tr>
<tr>
<td>Service / Components</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Services</td>
<td>extends over the long term to cover remote deployment, configuration, administration and patch application of distributed Gateway from central location</td>
</tr>
<tr>
<td>Logging services</td>
<td>Interface for application to log processing events</td>
</tr>
<tr>
<td>Exception Handling Services</td>
<td>Interface to raise and manage errors in application processing</td>
</tr>
<tr>
<td>Configuration</td>
<td>Interface to manage the configuration of the RLS application. E.g. setting record linking /matching algorithm, logging levels etc.</td>
</tr>
<tr>
<td>Security Services</td>
<td>Manage the implementation of security to control access to the system and protect confidentiality and integrity of data in the system</td>
</tr>
<tr>
<td>User / Roles Management</td>
<td>Manage the creation, updates, and deletion of actors authorized to use RLS</td>
</tr>
<tr>
<td>Authentication / Authorization / Personalization</td>
<td>Validate that actors (user or system) is who/what they claim to be</td>
</tr>
<tr>
<td>Consent Management</td>
<td>Manage individual patients consent to let healthcare practitioners view their medical records</td>
</tr>
<tr>
<td>Policy Management</td>
<td>Provide interface to configure and manage rules for access to healthcare data, auditing, and secure operation of RLS</td>
</tr>
</tbody>
</table>

The services that make up the Patient Index Service of RLS are described in Table 4.

<table>
<thead>
<tr>
<th>Service / Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient Index Services</td>
<td>Maintain patient records sourced from multiple clinical systems and provide access to data</td>
</tr>
<tr>
<td>Community Master Patient Index</td>
<td>Multi-enterprise Patient Index data store maintained in the RLS</td>
</tr>
<tr>
<td>Patient Records Linking / Indexing</td>
<td>Identify multiple patient records pertaining to the same individual, but created with potentially different attributes</td>
</tr>
<tr>
<td>Patient Record Search</td>
<td>Search for index for patients matching the demographic attributes entered by healthcare practitioner</td>
</tr>
</tbody>
</table>

The interfaces between the application components shown are the subject of local implementation decisions. The general bias of SOA-based applications is to use XML messaging interfaces between components. The CDX Gateway integration broker service may be used as a ‘service bus’ that mediates connections between the coarse grained services that make up the SOA-based application. It should be recognized that a messaging interface often has a system performance overhead and that this penalty may not, in some implementations, be fully offset by the benefits of true loose coupling of application components. In such cases, implementations may choose to start with tighter RPC-style interfaces between application components, and migrate to SOA as performance management allows.
6.3 Implementation Topology Options

As shown in Section 5 there are several processing models that can be implemented with the gateway based network architecture. Each gateway is an n-tier application with distinct presentation, application, data storage and integration services. This allows the functionality and data storage at each gateway service to be varied based on the degree of centralization or decentralization desired.

Being based on the Internet, the health information network has a fully connected mesh topology at the transport (and connectivity) level. The application and data distribution across the network nodes determine whether an interaction between nodes is server-based or peer-to-peer. In server-based networks some computers (clients) consume services provided by others (servers). In a peer-to-peer network, the computers on the network can act both as clients and servers, and are referred to as peers. The RLS-based health information network is a hybrid, with some key services (record location) being provided centrally, while others (clinical data exchange) are consumed on a peer-to-peer basis.

RLS’ service oriented application architecture (SOA) and the Web service based network supports multiple application and network configurations with varying degrees of data and application distribution. This derives from the fact that a loosely coupled, peer-to-peer model offers the ability to ‘tighten’ the coupling or centralize the architecture as needed by local implementations, whereas a priori centralization does not offer such flexibility. In effect the RLS-based network leverages the strengths of the Internet where a fully connected network allows varying service topologies to be used based on requirements.

The RLS-based network architecture seeks to find the right balance between being a potential single point of failure in the middle and reducing the processing footprint at the nodes. The proposed SOA model enables the intra-RLS service distribution to be adjusted and tuned for optimal performance at local, regional and national scale.

A case for data decentralization can also be built on patient privacy protection grounds. Recent security episodes and public perception suggest that the likelihood of data spills is reduced by not creating a large centralized repository of patient health information. Leaving protected health information in local clinical systems, and using a federated peer-to-peer clinical data exchange model reduces the likelihood of catastrophic data spills. Where local clinical systems are accessible from the network, the architecture anticipates data being cached by a hosted gateway service, which would serve as a proxy for the legacy clinical system (similar to an application service provider (ASP) model – a hybrid variation on centralized services).
An additional consideration is the messaging architecture for inter-RLS communication. Given that the health information network nodes are all Web-addressable each RLS sub-network node could connect to a remote RLS sub-network node on a peer-to-peer basis. However, as the security discussion indicates the need for each node to authenticate to each other impacts the scalability of such connectivity. An intermediary bridging service is required that can also be provided by the CDX Gateway at the RLS.

The different implementation options are listed in Table 5 below.

<table>
<thead>
<tr>
<th>Implementation Topology</th>
<th>Description</th>
<th>Decision Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer-to-peer using gateways for transport mediation and aggregation</td>
<td>Clinical data are distributed and managed within their clinical systems&lt;br&gt;Central patient registry for record location&lt;br&gt;Gateways translate messages from local to network standard format&lt;br&gt;Message and data aggregation at each gateway node</td>
<td>Service oriented architecture provides maximum flexibility in linking disparate systems&lt;br&gt;No single point of failure (SPOF)&lt;br&gt;No centralized command and control&lt;br&gt;Increased mediation/ aggregation functionality at Gateway ... complex distributed administration</td>
</tr>
<tr>
<td>Peer-to-peer with gateways maintaining clinical data caches</td>
<td>Gateways in addition to facilitating interconnectivity also serve as proxies for clinical data stores</td>
<td>Clinical data sources maintain autonomy&lt;br&gt;Operational clinical systems are not subject to unpredictable query loads from network users&lt;br&gt;Data replication needs to be set up and maintained between clinical database and proxy cache</td>
</tr>
<tr>
<td>Hub and spoke with distributed data sources using central mediation service for message routing</td>
<td>While clinical data remains at network nodes, messages are all routed through a central service&lt;br&gt;Central service handles message and data aggregation</td>
<td>The gateway at the RLS could serve as the central routing and mediation service&lt;br&gt;Lighter weight gateways at the edges minimize network joining overhead</td>
</tr>
<tr>
<td>Hub and spoke with central data repository</td>
<td>Variation of the distributed proxy data cache wherein data from clinical data sources are moved to central data repository&lt;br&gt;Gateway function is purely transport mediation</td>
<td>Increased central data management and security overhead&lt;br&gt;Reduced participation rates from clinical enterprises&lt;br&gt;Very light-weight distributed gateway&lt;br&gt;High degree of data conformity required</td>
</tr>
<tr>
<td>Implementation Topology</td>
<td>Description</td>
<td>Decision Criteria</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Inter-RLS data sharing on a peer-to-peer basis</td>
<td>Use Gateway service at each clinical system to communicate across RLS sub-networks</td>
<td>Sharing of information across communities needs to be independent of data distribution with the RLS sub-networks. Trust relationships need to be built on very large scale across all nodes in all sub-networks.</td>
</tr>
<tr>
<td>Inter-RLS data sharing using a ‘central’ intermediary service</td>
<td>Use the RLS Gateway to provide intermediary services to mediate patient lookup and clinical data exchange between different sub-networks</td>
<td>Trust relationships need exist only within an RLS sub-network and between RLSs.</td>
</tr>
</tbody>
</table>

Centralization and distribution are relative concepts and network topologies typically exist somewhere on a continuum between the two. The RLS architecture principle of federated data and centralized directories is currently considered best practice, but may well need to adapt to different models as technologies evolve. The above list of possible implementation options shows that the proposed architecture is flexible and adaptive.

6.4 Security Model

The RLS architecture principles recommend a delegated authentication model as the most practical approach to achieving the rigorous security and privacy demands on a health information network. Users are authenticated at the gateway service that they use to connect to RLS. Each gateway service is a full member of the clinical enterprise trust domain where it is deployed. Users wishing to access the health information network have their identity and authorization verified by enterprise security processes integrated with the gateway service.

Delegated enterprise security processes are expected to fully conform to HIPAA regulations and other clinical system and local, regional and national security requirements. Once authenticated, the user’s identity is embedded in each message flowing through the network, and is logged for comprehensive audit-ability. In addition, the RLS security model calls for authentication of sender and receiver systems using SSL/TLS (or HTTPS) for all messaging interactions. The digital certificates required for SSL/TLS based client and server authentication should be issued by trusted third parties. X.509 certificate life cycle management is recognized as a significant overhead, and automated support is essential as the network expands.
This basic security model that all network nodes must adopt to use RLS is considered adequate for point-to-point (SOAP server to SOAP server) message confidentiality, authentication and integrity. More comprehensive network security covering intermediaries, application-to-application encryption, etc. would need to use message level security.

The RLS security model foresees the migration to WS-Security based authentication across gateway services using XML Digital Signatures and XML Encryption to address confidentiality, authentication, integrity and non-repudiation requirements. WS-Security standards are available for X.509 digital certificate based message signatures and encryption, but implementations are relatively immature. After stabilization of the RLS basic transport level security, implementations should migrate to message level security using WS-Security.

A fully federated architecture would require individual user credentials to be managed at each node, which would pose a significant identity management problem. While federated security standards have been proposed, these are currently not proven in large scale inter-enterprise networks of disparate systems. RLS architecture should, over time, evolve to federated authentication and authorization models using Liberty Identity Federation Framework (ID-FF) and the Secure Assertion Markup Language (SAML) as mature implementations become available.

6.5 Implementation Platforms

There are several platform options available to implement the open standards based RLS architecture. Following the principle of no proprietary technologies, this technical overview does not recommend any specific platform for RLS. As guidance for identifying the appropriate platform-specific tools for the various components of RLS, the discussion below covers the experiences of the prototype development project.

The RLS prototype is developed on the Microsoft .NET platform for local reasons relating to skills and resource availability. The platform choice is based on practical considerations that apply to only RLS prototype development. Other technologies could as well be used, and it is expected that future implementations of RLS are based on other platforms. The choices made for the prototype components and possible alternatives are provided in Table 6.

<table>
<thead>
<tr>
<th>Service Layer</th>
<th>Prototype Platform</th>
<th>Alternatives</th>
</tr>
</thead>
<tbody>
<tr>
<td>Presentation Services</td>
<td>ASP.NET</td>
<td>* JSP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>* PHP</td>
</tr>
</tbody>
</table>

Table 6 Prototype Platform and Options
<table>
<thead>
<tr>
<th>Service Layer</th>
<th>Prototype Platform</th>
<th>Alternatives</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Application Services</td>
<td>.NET components</td>
<td>* Java Servlets&lt;br&gt; * EJB Session Beans&lt;br&gt; * PHP / Python / Perl</td>
</tr>
<tr>
<td>Data Management Services</td>
<td>ADO.NET using .NET framework services</td>
<td>* EJB Entity Beans&lt;br&gt; * Java Servlets&lt;br&gt; * PHP / Python / Perl</td>
</tr>
<tr>
<td>Data Storage Services</td>
<td>Microsoft SQL Server 2000</td>
<td>* Oracle DBMS&lt;br&gt; * IBM DB2&lt;br&gt; * MySQL&lt;br&gt; * PostgreSQL</td>
</tr>
<tr>
<td>Integration Broker Services</td>
<td>Microsoft BizTalk Server 2004</td>
<td>* BEA WebLogic Integrator&lt;br&gt; * IBM WebSphere / Mercator&lt;br&gt; * InterSystems Ensemble&lt;br&gt; * Orion Symphonia&lt;br&gt; * SeeBeyond eGate&lt;br&gt; * Combination of Enterprise Service Bus (Sonic MQ) and XML utilities (Altova XML Suite)</td>
</tr>
<tr>
<td>Adaptor Services</td>
<td>Custom components built on BizTalk framework</td>
<td>* Packaged adaptors from Integration broker vendors above</td>
</tr>
<tr>
<td>Messaging Services</td>
<td>Microsoft BizTalk Server 2004, which uses MSMQ</td>
<td>* IBM WebSphere MQ</td>
</tr>
<tr>
<td>Systems Management Services</td>
<td>Custom .NET components using .NET framework</td>
<td>* CA Unicenter&lt;br&gt; * IBM Tivoli&lt;br&gt; * Microsoft Management Services</td>
</tr>
<tr>
<td>Security Services</td>
<td>Custom .NET components using simple database table for user identities / credentials</td>
<td>* Novell Odyssey&lt;br&gt; * Sun ONE&lt;br&gt; * CA eTrust</td>
</tr>
</tbody>
</table>

### 6.6 Interconnectivity and Data Standards

Standards play a central role in the interoperability framework that RLS is part of. Policies and data standards may be considered the two pillars of the healthcare information network interoperability architecture. Technical standards that underpin the RLS-based common framework are described here.

While the healthcare industry in the US has no shortage of data exchange standards, clinical systems interoperability remains a major challenge. The problem is more one of choosing from several candidate offerings from various standards development organizations, and specifying coherent interoperability profiles that are easy to implement.
Interoperability standards can be specified across technology, data, application and organizational domains. Given the restricted problem domain of RLS, the common framework focuses on standards that are directly relevant to the use cases within RLS’ immediate scope. To advance decoupled development of interoperable systems and rapid adoption of the data sharing architectures, the RLS specification seeks to cover a minimum set of standards rather than make “all or nothing” recommendations.

At a high level, system interoperability standards may classified under the following categories:

- **Domain Data Content and Structure Standards:** includes information models, data naming standards, and controlled vocabularies. These represent semantic specifications that support business process level interoperability

- **Messaging and Transport Standards:** covering message packaging, transport and network protocols. These may be considered more in the realm of syntactic standards that support technical interoperability

As implied by its name various domain standards exist for the different clinical domains of data to be shared. However, it is possible to standardize on a common messaging and transport protocol that can be used across all the business domains. The technical standards decision is seen as relatively less contentious and will be discussed first.

### 6.6.1 Messaging and Transport Standards

Given the architectural principle to use open standards and the Internet for connectivity, the RLS uses Web services as the transport layer standard. This determination drives a range of other standards, which may be represented in the form of a technology stack. A common view of the ‘Web services stack’ is shown in Figure 20.

---

Figure 20 Web services stack

At the base of the stack are the HTTP and URI standards. The World Wide Web is evidence of the massive scale interoperability engendered by just these two enabling standards. Web services, based on SOAP (message packaging) and WSDL (message exchange contract) format standards, which in turn use XML and XML Schema as message notation and description standards, leverage transport layer interconnectivity to connect the data and application layers. Other technologies that are in wide-spread use and integrated in XML based messaging are XML Namespaces, XPath, and XSL. The other functional boxes in the stack have associated standards as well, but these do not have as high a degree of industry consensus about them.

Given the varying stages of approval and acceptance of the various standards in the stack, RLS needs to focus on the essential protocols that support interconnectivity while presenting the lowest adoption overhead to network participants. The Web Services Interoperability (WS-I) Organization provides a profile that focuses on the core Web services specs such as WSDL and SOAP, and addresses known interoperability issues. More specifically, the 'Basic Profile' provides specific implementation guidance on the core Web services standards that should be used together to develop interoperable Web services. Implementers thereby have higher confidence on achieving interoperability using Web services products from different vendors. The WS-I Basic Profile 1.1 offers the best choice for a candidate stack that RLS should adopt, and track as it evolves with the national (and global) technology environment.

-----

In addition, WS-I has published a draft Basic Security Profile that should be used in implementing WS-Security based services. The advantages of using the WS-I profiles include reuse of tools, implementation guides, and reduced costs, complexity and risks. A more restricted Web services stack with specifications that conform to the WS-I Basic Profile, is shown in Figure 21.

![WS-I Basic Profile Web Services stack](image)

Figure 21 WS-I Basic Profile Web Services stack

RLS uses the WS-I Basic Profile as its core messaging and transport services standards suite. Web services specifications providing standard XML grammars for the other functions in the technology stack are growing and some (e.g. BPEL for process orchestration) are strong candidates to become mainstream standards in the near term.

As RLS grows functionally the appropriate specifications should be reviewed and incorporated into the standards stack. Ideally, this evolution of RLS standards should leverage profiles developed by WS-I, or other interoperability standards organizations. WS-I is currently engaged in updating the Basic Profile to include SOAP v1.2 and WSDL v2.0 which offer significant functionality improvements over the current versions in the profile. RLS implementations should develop migration strategies to SOAP v1.2 and WSDL v2.0, so that the added benefits from the new features can be availed.

---

An alternate XML based business to business messaging frameworks with strong claims to being ‘industry standard’ is OASYS’ Electronic Business using eXtensible Markup Language (ebXML) framework. ebXML has been adopted by, among other, the U.S. Department of Defense for EMall, Center for Disease Control and Prevention (CDC) Public Health Information Network (PHIN), and NHS (UK) National Program for Information Technology (NPfIT). While the corresponding WS-* standards are maturing, as of this writing ebXML is clearly ahead in terms of stable specifications for reliable messaging, security, and exception handling. However, the rate of uptake of WS-* across the US market is higher than ebXML, particularly among applications and tools vendors. The perception that ebXML carries major implementation overhead has inhibited its use particularly among smaller organizations.

There are significant commonalities between the standards suggested for RLS and the PHIN ebXML stack. ebXML wraps another envelope on a SOAP message, and there is overlap between WSDL and ebXML’s CPPA, as well as between UDDI and the ebXML registry. The RLS architecture is extensible to support ebXML based messaging, through extension of the Gateway Integration Services layer to include an ebMS type messaging adaptor.

6.6.2 Domain Data Standards

Having fixed on the Web services stack as its data transport standards RLS offers significant flexibility in choice of domain data standards. The primary use cases that RLS supports deal with publishing and looking up patient demographic information. The leading information model standard for patient information is the HL7 Reference Information Model (RIM), which is the basis for the new HL7 v3 message formats definition. RLS uses the HL7 RIM as the basis for data standards. RLS adopts a HL7 v3 message format for the various interactions it supports. Given the prevalence of HL7 v2.x messaging in the healthcare industry in the US, RLS also supports a 2.4 (XML) based message format. Details are provided in the RLS Communication Messaging Implementation Guide.

In general information exchange between nodes in the healthcare network may be visualized as occurring over a multi-layered set of standards, as shown in Figure 22.
EHR information in the RLS context refers specifically to patient demographic and identifier information. The same stack is applicable to general clinical data exchange in the healthcare information network. The domain data standards would be mostly drawn from the available HL7 format standards. However, legacy data formats need to be catered to such as NCPDP Script for prescription medication data, and DICOM for radiology imaging.

The interoperability framework is focused on messaging and data standards. This is in keeping with the SOA principle that interfaces trump implementation. The internal implementation details of the RLS Patient Index service or Gateway service are not relevant to the interoperability of the different network nodes. The two interfaces internal to a network node are:

1. User access to the RLS is from standard Web-browser clients that invoke presentation services from the CDX Gateway servers. The user interface is generated in strict XHTML so that enterprises can use CSS and XSL style sheets to customize the user experience as necessary.
2. Gateway services interface with the local clinical data systems through standards interfaces such as HL7 messaging, or SQL database queries. If the Gateway is to serve as a clinical data cache to offload queries from the transaction clinical system, then data feeds need to be built to move clinical data into the Gateway data cache.

### 6.6.3 Comprehensive Standards List

The full suite of standards covering support functions for RLS implementation and use in the healthcare information network is listed in Table 7.

<table>
<thead>
<tr>
<th>Component</th>
<th>Specification</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hypertext Transport</td>
<td>HTTP/1.1: RFC 3818</td>
<td>Base message transport layered on TCP/IP</td>
</tr>
<tr>
<td>Directory access</td>
<td>LDAP v3</td>
<td></td>
</tr>
<tr>
<td>Domain name services</td>
<td>RFC 1035</td>
<td></td>
</tr>
<tr>
<td>Transport security</td>
<td>SSL v3 / TLS 1.0</td>
<td></td>
</tr>
<tr>
<td>Component</td>
<td>Specification</td>
<td>Comments</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>--------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Encryption algorithm</td>
<td>3DES</td>
<td></td>
</tr>
<tr>
<td>Message Hashing</td>
<td>SHA256</td>
<td></td>
</tr>
<tr>
<td>Message Signing</td>
<td>RSA FIPS 186-2</td>
<td></td>
</tr>
<tr>
<td>Web service message</td>
<td>SOAP v1.1</td>
<td>Upgrade to SOAP v1.2</td>
</tr>
<tr>
<td>Web services description</td>
<td>WSDL 1.1</td>
<td>Upgrade to WSDL 1.2</td>
</tr>
<tr>
<td>Web services basic interoperability profile</td>
<td>WS-I Basic Profile 1.1</td>
<td></td>
</tr>
<tr>
<td>Web services choreography</td>
<td>BPEL4WS</td>
<td></td>
</tr>
<tr>
<td>Web services security</td>
<td>WS-Security</td>
<td></td>
</tr>
<tr>
<td>Web services addressing</td>
<td>WS-Addressing</td>
<td></td>
</tr>
<tr>
<td>Data integration metadata /</td>
<td>XML 1.0</td>
<td>Legacy formats (e.g. HL7 v2.x, NCPDP) do not all use XML.</td>
</tr>
<tr>
<td>metalanguage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data integration metadata definition</td>
<td>XML Schema 1.0</td>
<td>Non-XML based messages do not have a standard schema notation</td>
</tr>
<tr>
<td>Data transformation</td>
<td>XSL: Extensible Stylesheet language, <a href="http://www.w3.org/TR/xsl">http://www.w3.org/TR/xsl</a></td>
<td></td>
</tr>
<tr>
<td>Data modeling language</td>
<td>UML</td>
<td></td>
</tr>
<tr>
<td>Data model exchange</td>
<td>XMI</td>
<td>XML based metadata interchange</td>
</tr>
<tr>
<td>Message signatures</td>
<td>XML Signature</td>
<td>Signatures are embedded in the SOAP Header</td>
</tr>
<tr>
<td>Message encryption</td>
<td>XML Encryption</td>
<td>Encryption information is provided in SOAP Header</td>
</tr>
<tr>
<td>Registered namespaces</td>
<td>URI (Uniform Resource Identifier) <a href="http://www.w3.org/TR/2001/NOT">http://www.w3.org/TR/2001/NOT</a> E-uri-clarification-20010921/</td>
<td>URN: form of URI which uses a namespace for persistent object names</td>
</tr>
<tr>
<td>Scheme for site identification on the WWW</td>
<td>URL (Uniform Resource Locator): address of a resource which is retrievable using the Internet. <a href="http://www.w3.org/TR/2001/NOT">http://www.w3.org/TR/2001/NOT</a> E-uri-clarification-20010921/</td>
<td></td>
</tr>
<tr>
<td>Identifiers using ASN.1</td>
<td>Object Identifier (OIDS) <a href="http://www.iso.ch/iso/en/ISOOnlinefrontpage">http://www.iso.ch/iso/en/ISOOnlinefrontpage</a></td>
<td></td>
</tr>
<tr>
<td>Scripting</td>
<td>ECMA 262 Script</td>
<td></td>
</tr>
<tr>
<td>Domain data</td>
<td>Health Level Seven (HL7) v3</td>
<td></td>
</tr>
<tr>
<td>Component</td>
<td>Specification</td>
<td>Comments</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Clinical Terminology</td>
<td>SNOMED</td>
<td>Clinical Terms creates a single unified terminology to underpin the development of the integrated electronic patient record by providing an essential building block for a common computerized language for use across the world</td>
</tr>
<tr>
<td></td>
<td>Sponsor: NLM (sourced from College of American Pathologists)</td>
<td></td>
</tr>
</tbody>
</table>
7 Deployment View

This section describes how the major components of the RLS logical architecture are distributed across hardware nodes in a health information network. Given that only the interface (inter-node messaging) specifications are expected to be consistent, deployment of systems based on the RLS architecture could vary widely based on local technology policies and preferences. This section provides deployment related information, for general guidance.

RLS components and services are designed to be flexible and highly configurable to enable deployment across a wide variety of sites. RLS requires the deployment of software on the following two types of server nodes:

- RLS Patient Index server which hosts the database of pointers to records in the clinical data sources, and routing information for each of the Gateways.
- CDX Gateway server which hosts the middleware that mediates data transfer from clinical data sources maintained at distributed locations (e.g. provider clinical systems, payer claims databases) and the Internet.

The RLS Patient Index is deployed at a central facility that provides robust data center management capabilities. This represents the one new patient data location that the health information network introduces. It is essential that HIPAA rules be observed at the RLS data center, much as they would in a covered entity.

Gateway servers are located within the circle of trust of the clinical system, and are typically deployed at the edge of the enterprise IT infrastructure zone in what is popularly known as the “DMZ”. An application firewall separates the Internet accessible gateway server from the internal network resources of the clinical enterprise. Only specific and authorized messages from the gateway are allowed past this application firewall.

Depending on volume of message traffic and throughput requirements, consideration may be given to deploying an ‘XML firewall’ that protects against malicious XML content based attacks. Such devices also feature XML processing capabilities, including XML Encryption and XML Digital Signatures using X.509 digital certificates based public keys. Typically, XML processing in hardware would provide significantly higher message handling performance. However, XML-aware network infrastructure is an emerging product category, and organizations should ensure that lock-in to proprietary features is avoided by insisting on conformance to open standards and verifying interoperability with XML software solutions.
Gateways can also invoke Web services on each other, enabling server processes to query the RLS. Such ‘batch’ mode queries and response processing will require additional functionality including the services of a job scheduler on the gateway server. The systems management services layer of the gateway is expected to manage these processes, which may be integrated with enterprise standard utilities as needed.

In a production network, deployment is expected to span a large number of CDX Gateway nodes that communicate with RLS and with each other. Sample production deployment topology is shown in Figure 23. Hardware sizing at each node is done based on production deployment requirements, which would be driven by network characteristics such as clinical transactions and patient registry volumes.

![Figure 23 Potential Production Deployment View of RLS](image)
7.1 Services Management

Systems management is critical to RLS-based network operations. The CDX Gateway architecture provides for comprehensive message logging and auditing capability. The same logs could be readily extended to support monitoring and reporting using simple scripting and system utilities. Several enterprise and network systems management tools exist that can be deployed to manage the CDX Gateway within the enterprise network context. Gateways need to be instrumented with the appropriate Simple Network Management Protocol (SNMP) agents for this purpose.

A Web services systems management standard: OASIS Web Services Distributed Management is expected to gain ground in the near future and advance SOA management using Web services. WSDM is based on SNMP and the Common Information Model and would represent a natural evolution from current distributed management standards to Web services based ones. The advantage of WSDM is that it uses Web service methods to manage distributed services such as those proposed for the RLS-based health information network, and therefore aligns well with the RLS architecture. Additional system management services would need to be added to the CDX Gateways to monitor and control message traffic using the WSDM protocol.

One of the key features of WSDM is SOAP based deployment of Web services. This would allow the Gateways to be deployed and configured from a central location (such as from RLS). This would further the goal of a utility service that can be cloned and deployed at the distributed network nodes with minimal disruption to the EHR systems at the node.

7.2 Security Services

Since RLS’ major communication security functionality is embedded in the gateway, this offers a convenient approach to localizing the deployment and management of security services. The major security infrastructure that needs to be deployed with the RLS and CDX Gateways are the Digital Certificates required to support SSL and, in future, WS-Security.

Directory services (LDAP or Active Directory) are often used as certificate stores, and as the user identity and roles repository. Enterprises directories should be used if this shared service is available on the EHR network. Gateways should be interfaced with the enterprise directory using LDAP interfaces.

The reader is referred to directory and PKI documentation for detailed guidance on the deployment and management of public key certificates.
8 Data View

Following the federated data architecture principle, RLS persists minimal patient data centrally. The core of the RLS data store is a community Master Patient Index (CMPI) that supports lookup of patient electronic health record locations based on basic demographic attributes.

A canonical information model is used to develop reference XML schema that CDX Gateways use to send and receive messages based on the HL7 Reference Information Model (RIM). A logical data model using standard Entity-Relationship diagramming notation is derived from the information model. All messaging services that RLS supports are integrated with the physical implementation of the logical model in the form of a relational database.

8.1 CMPI Information Model

The RLS information model view derived from the HL7 RIM is shown in Figure 24 for reference.

Figure 24 Information Model View

---


Architecture Document Page 67 Version 1.1a
Record Locator Service 2005-11-22
Confidential ©CSC. 2006
The community Master Patient Index follows the traditional MPI structure storing only ‘pointers’ to providers systems and patient identifiers therein, in addition to essential demographics attributes that can be searched on. The pointer to patient records is the id attribute of the communityMasterPatientIndex (CMPI) class. The list of attributes shown in the model view represents a set of all possible patient demographics. An RLS implementation would choose a specific subset of demographic attributes for the CMPI based on the specific community policies and requirements.

As can be seen from the information model, the patient EHR that the RLS index points to is a hierarchical abstraction of the RIM classes. With the patient index provided by the CMPI users can retrieve and select from visits or patient encounters at the provider facility. Users may then navigate from encounters to individual care records represented by the generalized clinical act class that may refer to procedures, observations (covering laboratory results, diagnostic images, etc.) and substanceAdministration (medication) lists.

8.2 Logical Data Model

The classes and attributes in the RLS information model are translated into entities and attributes of a logical data model that can be implemented physically in a relational (SQL) DBMS. The logical data model derived from the information model is shown in Figure 25.

The Entity-Relationship (ER) modeling notation used here is directly translatable to physical SQL databases. Entities have attributes corresponding to the class attributes of the information model. Attributes above the dividing line form the ‘primary key’ of the entity. Relationships between entities are denoted with lines that have a crows-foot notation to symbolize the ‘many’ end of a one-to-many relationship. These relationships result in the entity at the ‘many’ end inheriting the primary key of the entity at the ‘one’ end, as a foreign key marked as (FK).

The identifiedPerson entity represents the person as maintained in the source (EHR) system. The attributes of the CMPI entity shown do not signify the norm in any way. Select attributes from the identifiedPerson entity are replicated into the CMPI entity, based on community requirements for patient record matching. The identifying information (primary key) of patients in the communityMasterPatientIndex (CMPI) is formed by concatenating the identifiers of the assigningOrganization and the identifiedPerson. This combination of identifiers provides a unique key for the CMPI record.
Figure 25 Logical Data Model
Within a clinical data source, patients are usually assigned local identifiers (e.g. MRN, chart number, etc.). In some instances alternate standard identifiers (e.g. Social Security Number, Medicaid numbers etc.) are used. Given the expected variability in data quality in diverse clinical systems, and the privacy constraints around some of the standard identifiers used (such as SSN) RLS does not distinguish between these two types of identifiers. Each is treated as a non-intelligent key to the patient record in the clinical data source.

The gatewayDevice entity is used to store the network address of the clinical data source managed by the assigningOrganization. Thus, along with the patient pointer information the CMPI returns the network address (of the Gateway) to which queries for patient medical records should be sent. When an EHR Gateway receives a patient medical data request it resolves the medical record location using the personIDRoot (assigningOrganization's ID) part of the patient index, and redirects the query to the appropriate clinical data source.

The RLS supports use of multiple other identifiers for a patient such as identifiers used by ancillary systems. These additional identifiers are used more as attributes than identifiers, and may be used to search for the patient in the RLS. Standard identifiers, e.g. SSN, may be explicitly used as otherIDs, if the RLS implementation policy and regulations permit. The otherIDRoot attribute entity represents organizations such as the Social Security Administration (for SSN) or state Registry of Motor Vehicles (for driver’s licenses).

The assignedPerson entity represents the user who has access to the gatewayDevice. The user role that determines access rights of the user is carried in the ‘code’ attribute (following the HL7 v3 implementation guide).

In addition to the business domain entities, messages and message logs are represented in the model. Messages are not stored physically in the RLS database except as XML strings in the message logs. Message logs are generic entities that may be used to store all messages that flow through the RLS/Gateway. This entity also carries patient and user attributes related to the message, which supports auditing of the logs.

### 8.2.1 Identifier Attributes

Translation from the object-oriented information model to classic relational data structures requires that the HL7 v3 data types be converted to SQL data types. The conversion is for the most part straightforward where the components of the object attribute types such as II, EN, AD, etc. are flattened out to sequences of SQL data types.
Identifiers in the logical data model are formed from HL7 v3 instance identifiers (type II), and are worth examining in more detail since they are critical to understanding of the data returned by RLS. The II data type is defined as:

An identifier that uniquely identifies a thing or object. Examples are object identifier for HL7 RIM objects, medical record number, order id, service catalog item id, Vehicle Identification Number (VIN), etc. Instance identifiers are defined based on ISO object identifiers.

Instance identifiers are used for patient, organizations, devices etc. The HL7 v3 data type II has the following structure:

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>root</td>
<td>A unique identifier that guarantees the global uniqueness of the instance identifier. The root alone may be the entire instance identifier. This is a number sequence that matches a pattern corresponding to DCE UUID, ISO OID, or strings consisting only of (US-ASCII) letters, digits and hyphens, where the first character must be a letter.</td>
</tr>
<tr>
<td>extension</td>
<td>A character string as a unique identifier within the scope of the identifier root. If the root is used as a unique identifier, the extension is null.</td>
</tr>
<tr>
<td>assigningAuthority</td>
<td>A human readable name or mnemonic for the assigning authority. Note: no automated processing must depend on the assigning authority name to be present in any form.</td>
</tr>
<tr>
<td>displayable</td>
<td>Specifies if the identifier is intended for human display and data entry (displayable = true) as opposed to pure machine interoperation (displayable = false).</td>
</tr>
</tbody>
</table>

The extension, assigningAuthority, and displayable attributes are all optional. The root may itself be used as a unique identifier, such as when it contains a UUID. In the RLS data model, the convention is to use UUIDs for transactional entities such as messages. Entities such as organizations and devices have fixed identifiers set up by the RLS, which may use OIDs or UUIDs. Patients have two part identifiers, where the root maps to the assigningOrganization’s id and the extension to the specific person id (e.g. MRN).

The root attribute of the patient identifier is set to the OID or UUID of the ‘assigningOrganization’ that defines the id namespace (within which the id is unique). The personIDRoot of the CMPI is a foreign key mapping to the assigningOrganization primary key idRoot and the personIDExtension maps to the identifiedPerson primary key idExtension. The personIDRoot may be considered the prefix that RLS attaches to make the pointer unique in the CMPI.
The primary key of the CMPI is not used for searching as the demographics attributes are. Searchable identifiers are stored in the otherIDs entity. For example, when a user specifies, where permitted, the SSN of the patient as a query criterion, the RLS derives the OID of the SSA using a lookup table of standard OIDs, which is then used to match the patientIDRoot of the otherIDs table and the given SSN is matched to the patientIDExtension.

8.3 Physical Data Model

The physical data model maps very closely to the logical model shown above. However, the physical tables are not all implemented in the same database instance since the architecture posits the RLS as a combination of a Patient Index service and a distributed Gateway service. The distribution of tables across the Patient Index and the Gateway is worth further discussion. The problem of OIDs management is also relevant to this design discussion.

The tables generated from the CMPI, patientConsent, otherIDs and otherNames entities reside in the Patient Index database. In addition the patient matching algorithm may create persistent secondary indexes to increase the performance of lookup queries. For example a probabilistic matching method may need to maintain a secondary index of Soundex transformed names. Since the RLS architecture needs to work with multiple matching algorithms, the patient matching component is treated as a separate service that maintains all the secondary indexes it needs. Optionally, the record matching algorithm may also generate a linking identifier that would be persisted along with the index. However, this would lead to increased maintenance overheads.

The remaining tables in the logical data model are created in the Gateway service data storage layer. Authorized user identity (assignedPerson) and messageLog tables are used for the purposes described above at Gateway services at each node in the healthcare information network, including the RLS node.

Organization and gateway information is maintained at each node based on the message processing requirements at the node. The RLS maintains the master list of Gateway services at all the network nodes. The Gateway service at the participating nodes maintains information on the various clinical data sources that it supports. The RLS does not require to know the details of the individual clinical data sources at each node. That information is abstracted by the Gateway service at that node. The RLS maintains a local copy of the OIDs for standard identifier assigning authorities as replicated from centrally maintained registries, e.g. the HL7 OID registry.
RLS accepts patient index data from the distributed sources with patient identifiers qualified with the `assigningOrganization` id. If these `assigningOrganizations` are not stored in the RLS Gateway, then the patient record in the CMPI is provided an additional prefix: the `gatewayDevice.idRoot`. The sequence of actions to build up the patient index in the CMPI is shown in Figure 26.

![Diagram showing patient identifier composition in CMPI](image)

Figure 26 Patient Identifier Composition in CMPI

The patient record location provided by RLS in response to patient index lookup requests will contain the composite patient index made up of: `personIDRoot`, `personIDExtension` and the `gatewayDevice.telecomURI`. The recipient of this patient record location sends a query to the `gatewayDevice.telecomURI` with the composite `patientID` information. Since the remote Gateway maintains the `assigningOrganization` IDs it is able to resolve the composite patient identifier and retrieve the requested medical data.
As the above discussion shows, the division of labor between the Gateways at the clinical data source and the RLS requires that the appropriate cross-reference tables be maintained accordingly. At the RLS the various remote Gateways are assigned OIDs and maintained in the gatewayDevice table. The Gateway at the clinical data source, in turn, assigns OIDs to each clinical data source and maintains the cross-reference in the assigningOrg table. The use of OIDs is not mandatory; any local identifier system may be used as long as the patient identifier composition process described above is followed.

8.3.1 Data Quality Management

A general principle is that the CMPI database be a read-only version of patient records as they exist on source systems. The CMPI is intended purely for record matching and is not to be considered a patient registry. Data quality issues are expected to be resolved on the source systems, and cleansed data would replicate to the CMPI. The CMPI is therefore different from an Enterprise MPI in that no central data management organization is envisaged for an RLS. Data cleansing and quality services are not thought to be viable in a community of disparate, autonomous enterprises contributing data into the CMPI.

8.3.2 Data Cache

Message caching (logging) is likely to be required (over and beyond the persistence service offered by the MQ engine).

The data services layer in the CDX Gateway could serve as a cache for patient EHR data. Alternate architectures use clinical data repositories at the edge to serve the data requests received via information exchanges, so that core clinical data sources are not hit by these queries that could potentially impact the core clinical system performance. This aspect is discussed in more detail in Section 6.3. Some nodes may not want to push their EHR directly to the CMPI, instead may choose to expose their EMPI, or replicate their MPIs to the CMPI. Replicated MPI should have a ‘time-to-live’ based expiry, after which it must be refreshed.
## 9 Definitions, Acronyms, and Abbreviations

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.NET Framework</td>
<td>The core programming model for using Windows as an application server. Offers native support for database connectivity and Web Services</td>
</tr>
<tr>
<td>Bus</td>
<td>Common conduit for message based communication between services</td>
</tr>
<tr>
<td>CDX</td>
<td>Clinical Data Exchange: A community utility that allows interchange of healthcare information between diverse medical systems</td>
</tr>
<tr>
<td>EHR</td>
<td>Electronic Health Record: Clinical data collected in the course of delivering patient care, available in discrete digital form allowing access to individual data elements</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol: Protocol for exchanging files over the Internet</td>
</tr>
<tr>
<td>HL7</td>
<td>‘Health Level 7’ (Refers to the seven layer network model popularized by ISO): Message format standards used for exchange of data between healthcare systems</td>
</tr>
<tr>
<td>HL7 RIM</td>
<td>HL7 Reference Information Model: Object model used in deriving new HL7 (Version 3) message formats</td>
</tr>
<tr>
<td>Interoperability</td>
<td>The ability of two or more systems (or components) to exchange information and to use the information that has been exchanged</td>
</tr>
<tr>
<td>LOINC</td>
<td>‘Logical Observation Identifier Name Codes’: Standard code set covering medical terms, procedures and diagnoses maintained by Regenstrief</td>
</tr>
<tr>
<td>Metadata</td>
<td>Data about data. Technical metadata describes how and when the data was collected, transformed and should be used. Business metadata provides the business meanings of the data</td>
</tr>
<tr>
<td>MIME</td>
<td>Multi-purpose Internet Mail Extensions: Standard format for non ASCII content sent over the Internet mail system</td>
</tr>
<tr>
<td>MPI</td>
<td>Master Patient Index (also called Master Person Index by some vendors): An electronic index that enables lookup of patient data distributed across multiple systems, to provide an aggregated view of patient's EHR</td>
</tr>
<tr>
<td>Prototype</td>
<td>A visual, functional model of the proposed software system. A prototype is developed for various reasons. The primary purposes of the RLS prototype are to validate software architecture concepts and to demonstrate the working of a software product to stakeholders.</td>
</tr>
<tr>
<td>Reference</td>
<td>A tool to demonstrate the practical feasibility of software standard specifications, or application programming interfaces (API).</td>
</tr>
<tr>
<td>Implementation</td>
<td></td>
</tr>
<tr>
<td>RLS</td>
<td>Record Locator Service: An information service that locates patient records across systems that subscribe to the service</td>
</tr>
<tr>
<td>RxNORM</td>
<td>Clinical drug nomenclature produced by NLM, in consultation with FDA, VA, and the HL7 standards development organization. RxNorm provides standard names for clinical drugs and for dose forms as administered.</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SAML</td>
<td>Security Assertions Markup Language: An XML framework for communicating security information (authentication, authorization, other attributes) between systems. SAML is independent of the security protocol used (e.g. PKI, LDAP, Kerberos, etc.) and promotes interoperability between disparate systems</td>
</tr>
<tr>
<td>Semantic Interoperability</td>
<td>Property of data exchange that ensures that the receiver of data understands what the sender 'meant' (contrast with mere 'syntactic' interoperability)</td>
</tr>
<tr>
<td>Service Oriented Architecture</td>
<td>An application architecture comprising components, whose interface descriptions can be published, discovered and invoked. Components are said to be loosely coupled in that they have no knowledge of each other except for their respective interfaces and communicate with each other through messages. W3C definition: A set of components which can be invoked, and whose interface descriptions can be published and discovered</td>
</tr>
<tr>
<td>S/MIME</td>
<td>Secure MIME: Version of the basic MIME protocol that supports encrypted messages based on RSA's public key encryption technology</td>
</tr>
<tr>
<td>SNOMED-CT</td>
<td>Systematized Nomenclature of Medicine – Clinical Terms: Standard code set covering medical terms, procedures and diagnoses maintained by College of American Pathologists</td>
</tr>
<tr>
<td>SOAP</td>
<td>Acronym, originally, for Simple Object Access Protocol; no longer considered an acronym. Lightweight XML based protocol for exchanging information in Web service based implementations. Primarily specifies the XML 'envelope' for a message.</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer: Protocol used to communicate private (encrypted) data over the Internet</td>
</tr>
<tr>
<td>UDDI</td>
<td>Universal Description, Discovery and Integration: Mechanism for web service providers to advertise services and consumers of services to locate them.</td>
</tr>
<tr>
<td>UML</td>
<td>Unified Modeling Language: general purpose language for specifying and visualizing software systems. Favored for object-oriented software development</td>
</tr>
<tr>
<td>URI</td>
<td>Universal Resource Identifier: The standard for naming and addressing resources on the Internet. The commonly known URL (Universal Resource Locator) is a form of URI</td>
</tr>
<tr>
<td>Vocabulary Domain</td>
<td>HL7 term for standardized set of values for coded attributes used in healthcare information messages; e.g. ObservationMethod, Race, VaccineType</td>
</tr>
<tr>
<td>Web Services</td>
<td>An application that is identified by an URI, and invoked via the Internet, using data exchange notations based on XML. By emphasizing simplicity and open standards, disparate applications can securely interoperate without knowing internal details of each other. W3C definition: “A Web service is a software system identified by a URI [RFC 2396], whose public interfaces and bindings are defined and described using XML. Its definition can be discovered by other software systems. These systems may then interact with the Web service in a manner prescribed by its definition, using XML based messages conveyed by Internet protocols”</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>WSDL</td>
<td>Web Services Description Language: standard XML based specification to describe the interface to a Web Service. Machine-interpretable standard form for describing the operation of a web service, represents the ‘contract’ that the Web Service honors with any requestor.</td>
</tr>
<tr>
<td>WS-Security</td>
<td>Specification that encompasses all XML security standards related to SOAP messaging. Covers how security tokens are to be generated for SOAP message headers, how XML messages are signed and encrypted, etc.</td>
</tr>
<tr>
<td>XML</td>
<td>eXtensible Markup Language: Common notation used to represent data sent from one system to another. XML data files (or messages) use clear text and are ‘self-describing’ enabling human as well as machine understanding. E.g. HTML notation is based (loosely) on XML.</td>
</tr>
</tbody>
</table>
Connecting Americans to their Health Care:

Consumer Authentication for Networked Personal Health Information
Connecting Americans to Their Health Care: Consumer Authentication for Networked Personal Health Information
The document you are reading is part of *The Connecting for Health Common Framework*, which is available in full and in its most current version at: [http://www.connectingforhealth.org/](http://www.connectingforhealth.org/). The Common Framework will be revised and expanded over time. As of December 2007, the Common Framework included the following published components:
Connecting Americans to Their Health Care: Consumer Authentication for Networked Personal Health Information*

INTRODUCTION

This paper stems from the Connecting for Health document Connecting Americans to Their Health Care: A Common Framework for Networked Personal Health Information.\(^1\) The key goal described: Consumers have a choice of trustworthy “networked” personal health records (PHRs) to acquire electronic copies\(^2\) of their personal health data captured at various points on a network (e.g., doctor’s offices, hospital systems, pharmacies and pharmacy benefit managers, labs, diagnostic imaging services, etc.). Key points include:

- We see a networked environment for PHRs as a foundation for Americans to improve the quality and safety of the care they receive, to communicate better with their health care providers, to manage their own health, and to take care of loved ones.

- To establish a chain of trust, the participating entities must have common understandings and information policy expectations, such as how to authenticate and authorize clinicians to use the network and how to protect sensitive personal information.

- Consumers also need a chain of trust to interconnect across networks. Yet they represent a greater challenge than clinicians for authentication, authorization, liability, and security by virtue of the fact that they do not have organizational or business relationships that can serve as a vehicle for common policies and their enforcement. There is no commonly accepted set of practices today to provide credentials to consumers for health information exchange across different systems and data repositories. It is reasonable to expect that consumer applications could become more easily “networked” if such a set of common practices existed — that is, if some type of enforceable arrangement required all participants to operate under a common set of policies and agreements to mitigate risks such as misidentification or identity theft.

Trust on an electronic network depends on several factors, including assurances to consumers and participating entities that the information they access and share will be kept confidential, i.e., only shared with authorized actors. One key policy for achieving this trust, which is the focus of this paper, is to make sure that consumers are properly authenticated.

This work is the product of the Connecting for Health Work Group on Consumer Authentication Policies for Networked Personal Health Information. The Work Group charge

---

* Connecting for Health thanks Clay Shirky of New York University, Josh Lemieux of the Markle Foundation, and Dan Combs, an independent contractor, for drafting this paper. See Appendix A for acknowledgements and the Work Group roster.

1 Available online at: http://www.connectingforhealth.org/commonframework/docs/P9_NetworkedPHRs.pdf.

2 We emphasize the word “copies.” PHR applications may store copies of an individual’s health data along with original information contributed by the consumer. A consumer may control those copies of information stored in her own PHR application. This does not equate to her having a similar level of control over the data about her that is captured and held by health-related organizations, such as clinics, hospitals, pharmacy services, labs, health plans, etc. It is within our scope to find solutions to enable the individual to collect and control copies of health data captured initially by health-related institutions. It is not within our scope or intent to enable individuals to be able to directly alter or delete original data held by health-related institutions, although it is important (and required by HIPAA) for consumers to have clear mechanisms to notify and request corrections of erroneous or incomplete data about them.
stems from the *Connecting Americans to Their Health Care: A Common Framework for Networked Personal Health Information* paper. The group was asked to address the specific challenges of authentication. A second Work Group, the **Connecting for Health** Work Group on Consumer Access Policies for Networked Personal Health Information, was also assembled to address critical policies such as privacy, consent, secondary uses, breach notification, etc.

**A CRITICAL PROBLEM OF THE DIGITAL AGE**

At birth, a baby’s hospital nametag is the first of several tokens that society will use to assert “identity” throughout the rest of life. For a child born into this Digital Age, countless electronic transactions will be based on assertions of identity. There is no practical or affordable technology — at least, not yet — to flawlessly identify each person for each transaction. So we use a variety of imperfect tokens (driver’s licenses, passports, PINs, passwords, etc.) to validate an individual’s claim to a particular identity. And that identity will be created over and over again in electronic systems throughout a person’s life.

All business sectors and all individuals are challenged — and to some extent threatened — by this burden of proving identity, and of issuing and using authentication tokens. The increasing scattering of personally identifiable information makes identity management critical for business and consumer activities, yet at the same time problematic, costly, and sometimes risky. In the health care sector today, many important transactions occur daily with little rigor to confirm the identity of individual consumers.

This paper addresses the problem of authenticating consumers in electronic health information exchanges involving PHRs. These include concerns such as the growing public anxiety regarding privacy and security of personal health information, the fear by primary sources of data of increased risk to the information they hold, and loss of provenance of data, resulting from extensive sharing and duplication that could affect the trustworthiness of the system.

Because PHRs store sensitive personal health data, it is critical to develop reliable and trustworthy mechanisms to ascertain the identity of anyone accessing the information. Health information has several characteristics that make it even more sensitive than similar access to bank accounts and lines of credit, because someone who loses money through inappropriate access can be made financially whole. Someone who loses control of sensitive health data, by contrast, can never arrange to have that information returned to a purely private sphere. As part of handling this sensitive data, accurately identifying and authenticating consumers is an important hurdle to be overcome in enabling institutional health data sources to share electronic personal health information with consumer-accessible applications.

This paper offers a framework for processes by which participants in electronic health information networks can be assured that an individual consumer is who she claims to be. The framework includes these four components:

**Identity Proofing:** This is our umbrella term for the steps by which a person’s identity is verified. Specifically, it is the validation of independent evidence and/or credentials of “identity.” It happens several times throughout life at various institutions. For example, to receive a driver’s license, a person must present required documents in person at a state motor vehicle department.

**Identifiers or tokens:** Once identity proofing is performed, organizations issue or require users to use tokens or identifiers, which could be physical documents (e.g., driver’s license), biological markers (e.g., fingerprint), or be based on knowledge (e.g., passwords), or some combination (e.g., ATM card plus PIN).

---

3 Available online at: [http://www.connectingforhealth.org/commonframework/docs/P9_NetworkedPHRs.pdf](http://www.connectingforhealth.org/commonframework/docs/P9_NetworkedPHRs.pdf).
Ongoing monitoring: After tokens have been issued or identifiers linked to an identity, systems are put in place to establish behavior patterns of individuals and alert authorized parties if behavior changes suspiciously.

Ongoing auditing and enforcement: If an organization relies upon third parties for identity proofing or the issuing of identifiers or tokens, then it must have mechanisms to audit those third parties and redress bad actions.

Note: The word “authentication” is sometimes used as an umbrella term for all of the above components to manage identity in an electronic environment.
BACKGROUND

The Connecting for Health Work Group on Consumer Authentication Policies for Networked Personal Health Information focused on the authentication policies for private and secure consumer access to their health information routinely over the Internet to support important aims of consumer empowerment and improved health care quality and safety. Any framework for authentication in this environment must guard against opening up new vulnerabilities at a time in which medical identity theft already is a growing and serious problem. Our Work Group’s recommendations are consistent with principles articulated in the Connecting for Health Architecture for Privacy in a Networked Health Information Environment.

See Appendix A for the membership of the Connecting for Health Work Group on Consumer Authentication Policies for Networked Personal Health Information.
See Appendix B for more detail on the scope and charge of this Work Group.
See Appendix C for the background and principles of Connecting for Health.
See Appendix D for a partial list of other groups working on the consumer authentication problem.

We use the following definitions in this paper:

**Personal Health Records (PHRs):**
PHRs encompass a wide variety of applications that enable people to collect, view, manage, or share their health information or health-related transactions electronically. Although there are many variants, PHRs are intended to facilitate an individual’s ability to compile personal health information into an application that the individual (or a designee) controls. PHRs may contain copies of data held by health-related institutions as well as information contributed by the consumer or health monitoring devices. We do not envision PHRs as a substitute for the professional and legal obligation for recordkeeping by health care professionals and entities.

- **Consumer Access Services:** This is a set of functions that enable an individual consumer to securely access copies of their health data from multiple sources in an electronic environment. Consumers may be offered such services by a variety of organizations, ranging from existing health care entities to new entrants. Some will be covered under the Health Insurance Portability and Accountability Act (HIPAA), others will not. Consumer Access Services may combine both authentication services as well as data management services.

- **Health Data Sources:** For the purposes of this paper, a health data source is any entity that serves as custodian of the individual’s personal health data. This may include health care providers and clinics, hospitals and health care systems, health insurance plans, clearinghouses, pharmacies and pharmacy benefit managers, laboratory networks, disease management companies, and others that hold data related to the personal health of individuals.

The diagram below depicts a highly simplified data flow. In the center are Consumer Access Services, which include a mechanism to authenticate the individual consumer to the satisfaction of both ends of the exchange. (Appendix F contains a more detailed discussion of alternate models for conducting this authentication.)

---

5 Available online at: http://www.connectingforhealth.org/commonframework/docs/P1_CFH_Architecture.pdf.
The simplicity of the diagram obscures a few important points about our vision for Consumer Access Services:

First, PHRs (i.e., consumer-facing applications) could be offered by entities at either end of the diagram. For example, an independent technology company (left side of diagram) could supply a PHR, and so could one or both of the health data sources (right side of diagram). The site of the application is not relevant. The aggregation of copies of data that the consumer collects could be stored at either end of the diagram, or by an intermediary. For any of the entities to exchange data, however, there needs to be what we call Consumer Access Services (including authentication and the provision of access to records).

Secondly and similarly, Consumer Access Services may be performed by a third-party intermediary, but they also could be performed by the PHR applications or the Health Data Sources, or both. In fact, the Consumer Access Services and the PHR may be offered by the same entity and therefore indistinguishable to the end user. Our concern is with getting the process of authentication right, without regard to what sort of entity is doing the authenticating.

Third, our recommendations are designed to be compatible with existing networks — health care providers forming electronic health information exchanges, pharmacy networks, or large non-geographic networks. As the Networked Personal Health Information paper points out, there is a great deal of electronically available personal health information in existing databases today. Existing networks (e.g., large scale pharmacy chains, the VA, Kaiser Permanente), Regional Health Information Organizations (RHIOs), or other new services (monitoring devices, disease management programs, etc.) emerging from continued innovation in the PHR space — all may eventually provide multiple avenues for consumers to receive copies of their health data.

Throughout its deliberations, our Work Group was fully cognizant that other issues — revenue models, business relationships and contracts, limitations of liabilities, enforcement mechanisms — are bigger hurdles to PHR development than consumer authentication, which is the narrow focus of this paper.
WORKING PRINCIPLES AND ASSUMPTIONS OF THE WORK GROUP

In addition to the Connecting for Health principles (see Appendix C), our Work Group agreed to the following guiding principles for solutions to the authentication problem:

Principle 1

Authentication systems should, as a whole, cover as much of the population currently using the U.S. health care sector as possible. Authentication processes that are ineffective or unavailable for particular groups of people (due to disability, expense to the user, lack of available credentials such as driver’s licenses, etc.) should be balanced with alternatives appropriate for those groups, to the extent that such alternatives are available.

Principle 2

Consumers should have a choice in Consumer Access Services. Consumers should be entitled to a reasonable expectation of a choice of entities conforming to a published set of authentication standards. It’s optimal, when feasible, to let informed consumers play a role in determining their Consumer Access Service provider and authentication stringency level of choice. However, given a widespread lack of consumer awareness about authentication techniques and identity threats, minimum consumer authentication standards for health information should provide relatively high security.

Principle 3

To be both effective and trustworthy, a distributed system of authentication needs oversight, accountability, and mechanisms of redress. The policies of the authentication system should be transparent. Systems should allow the consumer to understand who has potential access to her data as well as when it has been accessed and by whom, ideally on demand and in real-time.

We prefaced our deliberations by stating that:

- Our recommendations must be reasonably affordable and workable in today’s environment.
- Our recommendations must not be tied to existing practices and technologies that may preclude future innovations.
- Our recommendations should not depend on the promise of future innovations in order for organizations to act on them now.
- Our recommendations must not favor any one technology or vendor, or any business model or business relationships.
- Our recommendations must be fully cognizant of any non-proprietary frameworks that are broadly accepted by at least large segments of the health sector.

6 On this final point, one key reference point for identity proofing and authentication stringency levels are those adopted by the E-Authentication Federation (EAF) among U.S. government agencies and its private sector companion organization, the E-Authentication Partnership (EAP). The National Institute for Standards and Technology (NIST) created a technical implementation guide for EAF based on industry standard Security Assertion Markup Language (SAML). The policies of the EAF have been licensed to the EAP.
A NEED FOR A NEW APPROACH

Frameworks that address the authentication problem typically do so based on a model of increasing stringency of identity proofing and authentication, corresponding with increased sensitivity of the data being accessed and the related risk. Requirements that are too low or loose create an unacceptable risk of the wrong person getting someone's information, compromising a consumer's accounts, defrauding providers or otherwise engaging in criminal acts. Requirements that are too stringent create unacceptable difficulties for the right person to get to his information, and may erect unacceptable barriers to adoption and implementation.

The development of networked PHRs is in its infancy, so there is no broad ecosystem to observe. Yet the problems of authentication are primarily ecosystem problems. If every organization dealing with a consumer managed its own authentication process from start to finish, there would be no systemic risk, and thus no need for a systemic solution. However, making every organization responsible for every one of its users pushes significant costs onto both the individual (who needs to manage multiple passwords) and the organizations that hold the consumer's data (each of which needs to be able to maintain a proofing and authentication infrastructure.)

A Consumer Access Service with insufficient proofing or authentication standards creates a risk for the security of the consumer's records. It also creates a risk to any clinical organizations and other entities that hold the consumer's data, to the degree that those organizations trust a Consumer Access Service to correctly validate a consumer's identity. If there is a race to the bottom for convenience to the customer, then there may be a high level of abuse (which could in turn inspire a draconian legislative or regulatory post-hoc remedy).

Therefore, it would be helpful to define an acceptable baseline identity proofing and authentication standard to which all Consumer Access Services should conform. Ideally, the standard would have an understood and generally accepted threshold for reliability, so that new methods for authentication can be evaluated against the effectiveness of existing methods. We aspire to a situation where an affordable and accepted industry standard is based on a measurable reliability of performance. However, as we discuss below, such a standard is not quantifiable today.

Given the constraints of the environment today, we make the following recommendations as an appropriate approach to the four key components of authentication: identity proofing, the issuing of identifiers or tokens, ongoing monitoring, and ongoing auditing and enforcement.

COMPONENT 1: RECOMMENDATIONS FOR IDENTITY PROOFING

The first step — verifying the identity of an individual consumer to an acceptable level of certainty — is typically the most difficult, expensive, and important.

Recommendation 1A: Consider in-person proofing as appropriate in some, but not all, cases: By in-person proofing, we generally mean requiring a face-to-face encounter in which the consumer presents a verified current primary government ID that contains a picture and either address of record or nationality (e.g., driver's license or passport). This option is an acceptable industry practice that is particularly appropriate when the organization performing the identity proofing:

a. Has no prior relationship with the consumer, and/or,

b. Has the infrastructure and budget necessary to conduct face-to-face encounters with consumers.
**Discussion:**
A key presumed advantage of requiring face-to-face identity proofing encounters is that it lowers the risk of mass or automatic attacks to obtain false credentials. In the virtual world, in which people can easily pose as others online, a requirement for in-person proofing has a strong appeal: It seems like the best way to establish a baseline identity of an individual. It raises the presumed commitment of the individual submitting to the proofing process. It raises the cost of a conducting a fraudulent “attack” on an individual identity, and it reduces the likelihood of remote, automated attacks from many sources or on many identities at once. Requiring presentation of commonly used documents (e.g., birth certificates, driver’s licenses, and passports) sets a hurdle for registrants and brings into play a variety of laws that may be useful at a later time for enforcement or prosecution, if necessary.

**Caveats:**
However, this option comes with three critical caveats:
- First, although dissuading misuse is a key goal for any such system, these same hurdles dissuade legitimate use as well. In-person proofing carries a cost and inconvenience burden for consumers, particularly those who face mobility or transportation barriers. Given the potential utility of providing consumers with electronic access to their health information and services, this outcome is not ideal and risks systematic underuse of PHRs. In-person proofing may be in tension with Principle 1, above, that the authentication process be available to as much of the population as possible.
- Secondly, in-person identity proofing is a significantly costly and labor-intensive process, which many organizations are not well-positioned to perform. If in-person identity proofing were required of all organizations on the network, it would keep organizations that could offer potentially useful data or services from participating. This affects both large and small organizations. For example, the Centers for Medicare & Medicaid Services (CMS) — the nation’s largest payer — has no direct way currently to conduct face-to-face identity proofing of its beneficiaries. Nor do most technology companies or web portals ever conduct in-person encounters with their customers.
- The third — and most critical — caveat is that, although in-person processes are a widely accepted starting point for identity proofing, we could not find (much less validate) any measurement of their effectiveness. If there were such a measurement (in the manner of “errors per 100,000” or similar), it would enable useful comparisons between various forms of in-person proofing, and between in-person and remote forms of proofing. Our Work Group found a dearth of publicly available research backing up the accuracy of in-person proofing. The assumption that in-person proofing is acceptably accurate is not based on empirical understanding. And certainly, the stringency of methods for in-person proofing varies from one organization to another. In fact, the existence of an in-person proofing process may create a false sense of security if those checking credentials are not well-trained or audited.

Recommendations 1B, 1C and 1D below attempt to address this problem.

**Approach 1B: Consider ‘bootstrapping’ of in-person proofing by other organizations:** We recommend that entities in the health sector consider “bootstrapping” other in-person encounters by third-parties to establish the consumer’s identity at acceptable levels of accuracy. We recommend that both current and potential holders of clinical data consider partnering with institutions that have effective authentication processes.

**Discussion:**
For many reasons, individual doctors’ offices are not well-equipped to authenticate 300 million Americans. (Their main authentication procedures relate to
confirming eligibility for health benefits.) However, there are other common places where in-person proofing can occur, including post offices, retail pharmacies, notary publics, and financial institutions. In the bootstrapping model, a laboratory could accept the authenticated identity of a consumer who had first been authenticated by another one of these parties. The entity would pass on the assertion about the patient’s identity, along with enough demographic details for the clinical data holder to match the consumer’s identity with her records, which could then be returned in any channel that could guarantee delivery. Note that such a system should never re-use existing identifiers. It would be potentially catastrophic, for example, to bind a consumer’s PHR directly to a bank account number, as publication of the number would then compromise both categories of data.

This is not a general-purpose solution, as the issues of transparency and liability will have to be worked out as business relationships between the authenticator and the relying party that holds the consumer’s health data. However, it would allow new interfaces to be offered to consumers for access to their records, and would do so without creating new proofing hurdles.

(These kinds of relationships will probably form as point-to-point business agreements, rather than multilateral networks, at least at first.)

**Approach 1c: Consider alternatives to in-person proofing:** Because there are no metrics to evaluate the quality of existing proofing systems, the data holder is, de facto, left to judge the acceptability of various methods. We recommend that data sources consider adopting remote proofing on their own, or rely on remote proofing from acceptable third parties (see Component 4 section below), when such proofing methods:

a. Rely on combinations of at least two alternative methods or sources for validating identity that use separate data (i.e., don’t use two different sources relying on Social Security Number or the same account number).

b. Are optimized to minimize the rate of false positives (i.e., when the wrong person is granted access based on an identity not his own).

c. Provide an alternative identity-proofing protocol to mitigate false negatives (i.e., when the right person using his correct identity is denied access nonetheless). In such cases, the person denied access in a remote-proofing protocol should be given an alternative means, such as in-person, to establish that he really is who he says he is.

d. Take precautions to minimize risk to the consumer, including but not limited to:

   - Not requiring consumers to use existing account numbers as identifiers. After the initial proofing step, nothing should be communicated from the consumer to the identity proofer that could provide access to the consumer’s account if intercepted by a third party.

   - Securely storing and limiting the number of parties privy to any “shared secrets” to the absolute minimum necessary.

   - Refreshing interrogation questions and “shared secrets” so as to avoid overuse.

This is not meant to be a list but a guide. Security practices change, and the underlying concern should be to adopt practices that create the necessary security while minimizing the privacy risks of the security methods themselves.

**Discussion:**

Knowing when remote proofing is acceptable suffers from a Catch-22. The obvious threshold for remote proofing should be, at a minimum, “as good as or better than current practice.” However, since there are no convincing metrics for current practice, it is impossible to say how any remote proofing system compares. With fake IDs readily available and with harried clerks often doing the checking, in-person
identity proofing does not guarantee that any particular individual is who he claims to be. In some cases it is possible that remote proofing actually works better in defending against a determined attacker than current in-person proofing practices.

There are examples, as with PayPal, where user-proofing is transactional (i.e., based on past or present transactions of information or money that serve to tie a person’s identity to a location or service, such as a U.S. Mail box or a bank account), and requires no face-to-face encounter. This method is one of a subset of “Knowledge-based Authentication” (KBA) methods in which a consumer is identified by answering a set of questions only she could reasonably be assumed to know. Sometimes these questions involve historical information (past addresses, use of credit cards for certain transactions) and sometimes they involve information generated as part of the KBA process itself, as with the PayPal technique of generating specific deposits.

The ideal situation would be to measure effectiveness of proofing by a numerical target, such as: “Wrongful issuance of credentials must be kept to an error rate below one in X,” where X would be at least a thousand patients. (This metric would be a 99.9% deflection of false positives, in other words.) In the absence of such precision, for either in-person or remote proofing (see 1D, below), the decision about when and how to use remote proofing will necessarily be in the hands of the person responsible for the security of patient data, to be undertaken with two principles in mind: Minimize false positives, and don’t rely on a single method.

Our recommendation is that at least two methods or sources be used in remote proofing processes. (For example, the consumer presents authentication credentials issued to him by another institution and successfully responds to an online interrogation about information acquired through his relationship with a separate independent service.) This is because two methods are likely to have different strengths and weaknesses, thus raising the cost of an attack while lowering its chance of success. This is true for both defense (i.e., it’s less likely that a criminal could fraudulently obtain knowledge or credentials in two places than in one) and for sustainability (i.e., if one method becomes compromised, the system would still have at least one untainted method still running, to which it could add new methods without starting from scratch).

**Approach 1D: Begin Federal research on identity proofing quality:** This is not a recommendation to data holders, but to the federal government. We recommend that the National Institute of Standards and Technology (NIST), in collaboration with other interested agencies, study current identity proofing practice wherever consumers are given access to their records remotely to provide or create metrics expressing the effectiveness of those various methods.

**Discussion:**

The current administration has made increasing accessibility of electronic health records to providers and citizens a national goal, and the lack of well-understood and generally agreed-to authentication methods for consumers is clearly a hurdle. This recommendation is intended to lead to a benchmark for future proposed systems to meet or exceed, thus moving us out of the current situation of identity proofing ratified by habit, but uninformed by measurement.

**Recommendation 1E: Do not use clinical data in the proofing process:** As a matter of privacy policy, we recommend against using clinical data as validation data in a proofing process. The reasons for this are articulated in the Connecting for Health paper Linking Health Care Information: Proposed Methods for Improving Care and Protecting Privacy.7

---

COMPONENT 2: RECOMMENDATIONS FOR ISSUING TOKENS OR IDENTIFIERS

Upon successful completion of identity proofing, it is necessary to issue acceptable tokens or identifiers to the consumer.

Recommendation 2A: Bind the consumer’s identity in such a way as to facilitate later authentication: At the time of initial proofing, the capture and retention of copies of the documents allows for re-verification if needed at a future time. If in-person visits are used in identity proofing, they present an opportunity to capture a biometric indicator, such as photographs or fingerprints.

Discussion: This process of connecting or binding of particular information or attributes to a particular physical person, when combined with system monitoring, can provide improved ability to discover certain types of fraud attempts in which attributes are used by multiple registrants. However, it is important to note that improved information collection, of any sort, also raises the requirements for securing the database where the records are stored. Improvements in knowledge-based authentication methods generate, as an inevitable side effect, more stored knowledge about the consumer — knowledge that must be held securely to prevent near-term defeat of the authentication system itself and to prevent identity theft. Although database security is not in the scope of this paper, we note that care must be taken to evaluate the security of the data held in aggregate, as well as the security of person-by-person authentication.

Less reliable, although at times more economically practical, are password reminders as “shared secrets” that can be used to support later authentication, or password reset requests. A common example is for the consumer to be forced to answer questions such as pet names or mother’s maiden name. Care must be taken that these not be based on common questions that can be easily guessed or snooped. Another possible source of shared secrets are questions the service asks of the consumer. For example, PayPal makes two small deposits in a new user’s account, then asks that the user report those amounts back to PayPal. This removes the risk of trivial guessability, though it requires a higher degree of integration with the financial system.

Interesting work is being done on “zero-knowledge” authentication systems, which reduce or eliminate the need for knowledge-based secrets to be held by the authenticating party. In a zero-knowledge system, the consumer proves who he is by using a secret that only he knows to perform a task that he could only perform with that secret. (Imagine that you see someone unlock a door that you know can open with only one key. You could conclude that the person has that particular key without you needing to see a copy of the key yourself.) “Zero-knowledge”-based systems have not yet been widely deployed, and have significant management issues in their current implementations. Still, they should be watched closely, as they may provide a way to increase authentication security without also increasing the privacy risk to consumers that comes with knowledge being held about them in various authentication databases.

Recommendation 2B: Choose an appropriate token or identifier: There are a variety of credentials available. PINs, cards, tokens, fobs with RF chips, antennas, and fingerprints are a few examples of a rapidly growing array of tokens.

Discussion: Many different types of tokens or identifiers can be used to good effect in authentication processes. Much depends on the budget and infrastructure of the token-issuer and the tolerance of consumers to remember and use the token appropriately.
Recommendation 2C: If using passwords as tokens, enforce ‘strong’ passwords: Requiring and enforcing rules to create strong passwords⁸ — i.e., passwords that are not easily guessable — is one of the first relatively easy steps that will dramatically increase the security of the username and password token.

Discussion:

The username and password combination is the most commonly used token. Extremely valuable and potentially risky transactions are conducted millions of times each day employing the protection of username and password. Many of the tokens and identifiers listed in Recommendation 2B are essentially variations on the concept of username and password, incorporating a variety of technologies to improve on the basic concept. Used appropriately, the username and password combination provides significant protection at very moderate cost and user inconvenience. However, if unguided by a set of guidelines or password requirements, many consumers tend to create easily guessable passwords and otherwise create the opportunities for compromise of their identity.

Many systems now prevent the use of dictionary terms as passwords, or consecutive or repeating strings of numbers or letters or other easily guessable phrases. Some require the use of at least one number, a letter and another keyboard character. Some systems will provide a rating of the strength of the password as it is created by the user. The fundamental challenge with strong password requirements is that they not only make it harder for illegitimate users to guess a password, they can make it harder for the legitimate user to remember it. If strong password requirements are too onerous, they may encourage legitimate users to compensate through insecure practices, such as writing down a password and leaving it next to an unattended computer.

It is increasingly common to supplement the username and password combination with monitoring of the requesting machine (e.g., source IP address, machine and browser characteristics). Such monitoring, which we discuss further below, requires no additional issuing of tokens to the user.

Recommendation 2D: Limit attempts on passwords: Given sufficient time, access, and attempts, any password will eventually succumb to attempts to guess it. Limiting the number of consecutive and total attempts to enter a password, requiring periodic changes to the password, and other relatively low-cost, relatively low-inconvenience requirements for use of passwords make password guessing an unacceptably difficult approach to compromising tokens.

Recommendation 2E: Establish a clear policy on requirements for password changes: Although an inconvenience to end users, it may be reasonable to require consumers to create new passwords at regular intervals. Each system should decide locally whether to enforce a policy requiring that consumers change their passwords over time. However, if such policies are enforced, it’s critical that consumers be given clear

---

⁸ The following documents contain useful information about the issuing of tokens, including strong passwords:


explanations on the methods and reasons for resetting their passwords.

**Discussion:**

The value of tokens can diminish over time. For example, many private and government organizations still use Social Security numbers not only as identifiers but also as tokens\(^9\), and it is precisely because of this ubiquity of uses that Social Security numbers have been a boon to identity thieves. Similarly, if a consumer uses the same password and password reminder at every site visited, it is much less secure than if the consumer uses different secret codes at each site’s login. On the other hand, consumers may have trouble coming up with strong passwords that they can remember, and the burden of having to do so frequently could drive down utilization. The value of forcing consumers to change passwords is hotly debated, and our work group did not feel strongly about making a recommendation one way or the other.

\(^9\) The principal reason Social Security Numbers (SSNs) should not be used as tokens is that, if this approach is taken, then one number is used to provide the public and secret parts of authentication (i.e., you have an SSN that points uniquely to you, but you must reveal it as proof that you have it.) Without being accompanied by a second, secret token such as a PIN, the SSN is damaged in regard to authentication by the very use that makes it otherwise worthwhile. In addition, no one token should be relied on too heavily, as such ubiquitous use will increase the focus of malevolent actors on compromising that token, and any compromising of such a token will have disproportionately negative effects.
COMPONENT 3:
RECOMMENDATIONS FOR ONGOING MONITORING

It is important to perform periodic or ongoing processes to continually improve upon the initial proofing and to weed out compromised identities.

Recommendation 3A: Conduct appropriate ongoing monitoring:
Ongoing monitoring is an essential third component of appropriate authentication because of inherent weaknesses in the first two components (i.e., identity proofing and issuing of tokens). Given the widespread compromise of documents used for initial identity proofing and the large and growing incidence of identity crimes, the function of authentication should be thought of as an ongoing process rather than a gateway to be passed through one time. Once the consumer’s identity is proofed and the token is issued, systems should establish the behavior patterns of individuals and alert authorized parties when behavior falls out of the established pattern. For example, credit card companies have algorithms to detect sudden changes in charging behavior, triggering a telephone call to the consumer to investigate possible fraud.

Discussion:
Identity proofing is often used as a “gateway” process. It is merely a perimeter defense, performed once and not revisited. Once identity proofing is completed, a registrant is an “insider” of the system. And there is often much secondary reliance on this initial proofing, such as airport security relying on a state-issued driver’s license. In the Digital Age, the outside/inside relationships change continually. Allowing network access to partners, customers, users, and some unintended participants quickly renders perimeter defenses insufficient. Additionally, much of the fraud and abuse comes from people accurately identified or from identities that were compromised after the initial proofing process, as well as from “inside” authorized users.

There is a robust and active population that continually probes and prods for opportunities to compromise systems and almost immediately shares with others any new intelligence gained. The risks and threats to systems change continuously. The practices and processes to respond to these threats must likewise change.

The automated ability to monitor individual behavior for fraud varies significantly from organization to organization, depending in part on the type of organization, what data it captures, and what it is permitted to do with the data. Valuable techniques include analysis of transaction history and location, keystroke patterns, and others. Detailed recommendations would rapidly become dated and ineffective. Decisions about an ongoing monitoring process must be made locally. The U.S. government provides some guidance for ongoing monitoring as an integral part of an authentication process in the NIST Special Publication 800-100, Information Security Handbook: A Guide for Managers.¹⁰

Behavior pattern monitoring can include information about the method of login (e.g., consumer’s usual IP address, machine and browser type, etc.), or information about the types of resources or data that the consumer typically accesses.

Recommendation 3B: Enable consumers to view an immutable audit trail: Consumers can become powerful allies in detecting identity fraud when they have access to the transaction history of their accounts. We recommend that Consumer Access Services and PHR offerers provide authenticated consumers with online access to an immutable audit log displaying all accesses and data transactions involving their account.

Discussion:

Consumers now are able to review their own credit reports online, providing an important and highly invested check on potential fraud or errors. This recommendation is in keeping with Principle No. 3 of this document. The Connecting for Health Common Framework document, Auditing Access to and Use of Health Information Exchange, provides some guidance in this area of immutable audit.\footnote{Available online at: \url{http://www.connectingforhealth.org/commonframework/docs/P7_Auditing_Access.pdf}.}
COMPONENT 4: RECOMMENDATIONS FOR EXTERNAL AUDIT AND ENFORCEMENT

When relying on a third party to perform proofing or issuing of tokens, or both, some mechanism of audit and redress is essential to establishing a chain of trust.

Recommendation 4A: Ensure that third parties are “observable” in how and how well they are performing identity proofing, token-issuing, and ongoing monitoring or any related services to authenticate consumers. One recommended practice is to have a contractual commitment for the parties to notify each other if either detects system compromise above a certain threshold or fails to comply with agreed procedures.

Discussion:
A fundamental premise of the Common Framework for Networked Personal Health Information paper is that Consumer Access Services will emerge to help consumers “network” their PHRs with connections to multiple sources of health data and services. In order to facilitate the consumer’s requests for digital copies of his information from Health Data Sources, all parties must be assured of the individual’s identity and bona fide authorization to share data. Simply put, such transactions require “trust.”

It will be impossible to trust and rely on any third-party’s authentication if those third-parties’ practices are not observable either directly among contracted parties or via some industry-accepted auditing and validation mechanism.

Recommendation 4B: Ensure a mechanism for enforcement and redress for bad actions: There needs to be a commonly accepted mechanism, agreed upon in advance, to redress unacceptable practices and eject bad actors.

Discussion:
Audit, enforcement, and redress are general issues for Consumer Access Services, not just with the task of authentication. All this is framed against the larger issues of binding Consumer Access Services to policies and accountability generally, and against the general fragmentation of the health care industry (a fragmentation that may increase as Consumer Access Services enter the picture).

Recommendation 4C: Consider federation and/or other contractual means to address Recommendations 4A and 4B: If the Health Data Source is considering a request from a third party (e.g., a Consumer Access Service) to pass information into the consumer’s possession, then we recommend that:

- The Consumer Access Service must be contractually bound to a group that sets and enforces shared policies, such as the E-Authentication Federation (EAF), Electronic Authentication Partnership (EAP), or similar.

- The Consumer Access Service must use at least Level 2 identity proofing as defined by EAF and adequate tokens (i.e., strong passwords, or tokens at EAF Level 2).

These recommendations are worded as a requirement on the Health Data Source, but apply equally to the Consumer Access Service.

We believe the EAF/EAP is a good framework for a discussion on finding an acceptable degree of authentication certainty and policy enforcement. Although some organizations might choose to join the EAF or the EAP, there is likely no one-size-fits-all answer. Different business relationships and different consumer populations will likely require a variety of authentication services for their transactions. Some consumers may even demand higher-level authentication stringency for certain services.

Discussion:
We emphasize that the above scenario is not the only way to approach the problem. (See Appendix G for a draft
architecture discussion.) Point-to-point trust is conceptually simplest from the point of view of any given pair of actors, but pairwise trust exposes the system as a whole to daunting complexity. Similarly, a single national actor coordinating trust on behalf of everyone is not feasible at this time, both because of the realities of fragmentation and the business context, and also because the policing problem for a single actor is acute. If these two extremes are in fact impractical, this suggests some sort of chain of trust with mutual policing, with various actors monitoring one another, possibly in contractually arranged groups.

In the absence of a federation, the following are among the most important demands that a typical health data source will make of a Consumer Access Service asserting the identity and a data request on behalf of an individual consumer:

- An authorization from the consumer to share data with the Consumer Access Service.
- A HIPAA covered entity-business associate agreement or contract with similar terms.
- A significant measure of accountability, including immutable audit logs and external audits.
- A contractual commitment to a policy of timely notification and recourse in the event of inappropriate access or breaches of personal health information.
- A cap on the Health Data Source’s liability stemming from the health data exchange.
CONCLUSION: A PATH FORWARD

This paper is driven by a desire to allow U.S. consumers to access and gain value from their own health information. Connecting for Health accepts that much of our valuable personal health data is stored and managed by numerous entities. The next key challenge is to establish the rules and techniques that establish trust among participants over a “network of networks.”

Policy rules will be needed in a number of areas — including patient consent, secondary use, and data management. Identity has quickly emerged as a primary problem in network access — particularly given the sensitivity of personal health information. A well-understood and implemented Common Framework for managing health consumers’ identity is a prerequisite to networked use of personal health records.

The recommendations in this paper are based on the technologies and practices current at a particular moment, and our desire to stimulate national progress in addressing this particular obstacle to consumers’ electronic access to their health information.

The problems of identity proofing and authentication are widely felt by all industries handling sensitive data or electronic transactions, and as a result, there is rapid evolution in the tools available for authentication. Any process of authentication for consumer access anywhere in health care must be regularly re-evaluated to factor in both new threats and new capabilities.

Many health care entities have significant interest in some form of networked personal health records. The relationships they forge could have significant impact on possible trust scenarios for consumer authentication. In addition, there is a critical need to expand consumer education about techniques to safeguard identity in the Information Age. Consumers should understand, first, that there are tradeoffs between security and convenience and, second, what the tradeoffs mean for them.

These many trends — new threats, new business relationships, emerging technologies, and consumer awareness and behavior — all warrant close monitoring. They certainly will have more impact on future health information sharing environments than the modest recommendations in this paper. We do, however, hope that this paper contributes to a growing consensus that the path forward on consumer authentication requires careful thinking, new research, and innovative approaches.
APPENDIX A: ACKNOWLEDGEMENTS

Connecting for Health thanks the following Work Group members for participating in the rich discussion that resulted in this paper.

Chair
Clay Shirky*, New York University Graduate Interactive Telecommunications Program

Work Group
Paula Arcioni*, New Jersey Office of Information Technology
Ernie Argetsinger, Omnimedix Institute
Siddharth Bajaj, VeriSign, Inc.
Dan Combs, Global Identity Solutions, LLC
Jeremy Coote, InterComponentWare, Inc.
Maureen Costello, Ingenix
Phillip D’Angio, VeriSign, Inc.
James Dempsey, JD, Center for Democracy and Technology
Carol Diamond, MD, MPH, Markle Foundation
Martin Fisher, MedicAlert Foundation International
Thomas Foth, Pitney Bowes, Inc.
Christopher Gervais, Partners Community HealthCare, Inc.
Mark Gingrich, MS, RxHub, LLC
Janlori Goldman, JD, Health Privacy Project
Philip Hagen, MD, Mayo Clinic
Jonathan Hare, Resilient
Elizabeth Holland*, Centers for Medicare & Medicaid Services

Mark Johnson, Vanderbilt University and Medical Center
Jennifer Kerber, Information Technology Association of America
David Lansky, PhD, Markle Foundation
J .P. Little, RxHub, LLC
Kathleen Mahan, MBA, SureScripts
Georgia Marsh*, United States General Services Administration, E-Authentication Initiative (former position)
Phil Marshall, MD, MPH, WebMD Health
Daniel Matthews, Lockheed Martin Corporation
Damon Miller, CapMed Corporation, A Division of Bio-Imaging Technologies, Inc.
Kim Nazi, FACHE*, United States Department of Veterans Affairs
Alison Rein**, AcademyHealth
Eric Sachs, Google Health
Charles Safran, MD, Harvard Medical School
Scott Schumacher, PhD, Initiate Systems, Inc.
Donald Simborg, MD, Independent Consultant
Michael Simko, RPH, Walgreens Pharmacy Services

Michael Stokes, Microsoft Corporation

David Temoshok*, General Services Administration, Office of Governmentwide Policy

Robert Tennant, MA, Medical Group Management Association

Jeanette Thornton, MPA, America’s Health Insurance Plans

Allison Viola, American Health Information Management Association

David Yakimischak, SureScripts

*Federal and state employees participated in the Work Group but make no endorsement.
**Participated in Work Group but makes no endorsement per employer policy.

The Connecting for Health Work Group on Consumer Authentication Policies for Networked Personal Health Information wishes to thank Josh Lemieux for his expertise and tireless help preparing this manuscript. In addition, we thank Clay Shirky for his leadership and work on this manuscript. Without his unique ability to parse very complex issues carefully and adeptly, we could not have achieved this paper. We also thank Dan Combs and Stefaan Verhulst for their help researching and drafting portions of this document.
APPENDIX B: SCOPE AND CHARGE OF THE WORK GROUP

The Work Group on Consumer Authentication and Health Information Exchange was charged with defining a framework to authenticate the identity of individual consumers consistent with Connecting for Health principles. This includes identifying a baseline of policies and technologies to assert, within acceptable thresholds of accuracy, the identity of an individual consumer requesting copies of her personal data in an electronically networked health information environment. The recommendations are intended to encourage a fresh approach to foster trust of all network participants, and specifically to protect the consumer, the health data holders, and the Consumer Access Services from the following threats:

- **Defense against illegitimate access to health records**: This is defined in this paper as externally targeted or automated attacks to gain access into an individual’s health information. The attackers in this scenario could be either known to the consumer (as with a relative or colleague looking at material inappropriately), a targeted attack by someone not known to the patient (as with a private detective trying to access records), or an indiscriminate attack (someone looking for anyone’s health records, possibly as a precursor to medical fraud).

- **Defense against identity theft**: The threat here is not to the clinical data per se, but to the consumer’s identifiers and demographics — address, date of birth, Social Security Number, health benefit eligibility number, etc. Protecting against identity theft is an obvious goal. The key complication here is that it is very difficult to protect against family members posing as one another, and it is not possible to design a system that covers all state regulations of parental access to their children’s data. Our Work Group did not focus on proxy access beyond the key principle that the identity of all proxies accessing the system be recorded, as well as the identities of people for whom they are proxies, so that, should a proxy later lose access, their authentication tokens can be revoked separately from the main account.

The following issues fell outside of the scope of this Work Group, but we list them here to acknowledge their importance in creating a trusted health information sharing environment for consumers:

**Consumer Issues:**

- **Consumer Behavior**: We are not addressing what consumers do with their copies of personal health data. We live in an age in which individuals are increasingly self-publishing on the Internet intimate details of their personal lives. It was outside the scope of this Work Group to attempt to address the complexities of individual behavior and choice. Nevertheless, these are relevant concepts. Consumers’ own experiences and individual preferences will no doubt shape this emerging area.

- **Phishing**: There is a parallel problem to consumer authentication, related to the assurances provided by the entity hosting the consumer’s data. Mechanisms need to be in place to defend the consumer against “phishing” attacks, where a consumer is directed to log into a seemingly legitimate web site or service, but which is really a copy of an existing site, with a similar URL. The risk of such phishing in medical contexts is high; however, the defenses against the phishing problem require a different set of strategies than those outlined in this document.

**Data Storage Issues:**

- **Data Security**: Methods to encrypt and secure health data repositories are beyond the scope of this paper. We focus on defense against unauthorized users defeating authentication systems, not attacks on larger data stores. For purposes of this paper, we accept as a precondition that all actors have good physical security.
practices. The digital signing of records is also outside the scope of this paper.

- **Data Policies:** Also out of scope of this paper are policies for data custodianship and data sharing other than those related to identity proofing and authentication. The parallel *Connecting for Health* Work Group on Consumer Access Policies for Networked Personal Health Information is working on recommendations for privacy policy, disclosure and consent, secondary use, etc. For purposes of this paper, we accept as a precondition that the consumer has voluntarily initiated a PHR account and authorized all uses and exchanges of personal health data consistent with *Connecting for Health* principles for privacy.  

**Business Issues:**

- **Business relationships:** This paper does not address the necessary business relationships that would provide motivations for health data sources and PHR services to share data on the consumer’s behalf, or for intermediaries to emerge between them.

In summary, this paper focuses on a framework for the authentication process when the individual wants to access or contribute personal health information electronically among health professionals or other health-related entities (HIPAA-covered or not).

---

12 Available online at:  
http://www.connectingforhealth.org/commonframework/docs/P1_CFH_Architecture.pdf.
APPENDIX C: BACKGROUND ON CONNECTING FOR HEALTH

Connecting for Health, founded and operated by the Markle Foundation, with additional support over the years from the Robert Wood Johnson Foundation, is a public-private collaborative organization with representatives from more than 100 organizations across the spectrum of health care stakeholders. Its purpose is to catalyze the widespread changes necessary to realize the full benefits of health information technology (HIT), while protecting patient privacy and the security of personal health information. Connecting for Health is continuing to tackle the key challenges to creating a networked health information environment that enables secure and private information sharing when and where it’s needed to improve health and health care.

Connecting for Health has produced the following documents that lay the groundwork for this current work product focused on consumer authentication:

• **Linking Health Care Information: Proposed Methods for Improving Care and Protecting Privacy** (February 2005) — which describes an approach to matching patient records among disparate health care institutions.\(^{13}\)

• **Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange** (April 2006) — which elaborates and defines a set of policy and technical elements necessary to enable secure exchange of health records among providers across the Internet, including a set of principles for privacy and fair information practices in a networked environment. The Connecting for Health Common Framework is composed of nine policy documents on topics such as privacy, notification, audit, and authentication of non-consumer users of the network, and six technical documents that elaborate technical specifications of a network approach based on those policies.\(^{14}\)

• **The Architecture for Privacy in a Networked Health Information Environment** (April 2006) — which describes a set of fair information practices that the Common Framework has endorsed to guide systems that support the exchange of personal health information. These principles are:

  > **Openness and transparency:** Consumers should be able to know what information exists about them, the purpose of its use, who can access and use it, and where it resides. They should also be informed about policies and laws designed to ensure transparency on how privacy is assured.

  > **Purpose specification and minimization:** The purposes for which personal data are collected should be specified at the time of collection, and the subsequent use should be limited to those purposes or others that are specified on each occasion of change of purpose.

  > **Collection limitation:** Personal health information should only be collected for specified purposes and should be obtained by lawful and fair means. Where possible, consumers should have the knowledge of or provide consent for collection of their personal health information.

  > **Use limitation:** Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified.

  > **Individual participation and control:** Consumers should be able to control access to their personal information. They should know who is storing what information on them, and how that information is being used. They should also be able to review the way their information is being used or stored.


\(^{14}\) Available online at: [http://www.connectingforhealth.org/commonframework/index.html](http://www.connectingforhealth.org/commonframework/index.html).
- **Data quality and integrity:** All personal data collected should be relevant to the purposes for which they are to be used and should be accurate, complete, and current.

- **Security safeguards and controls:** Personal data should be protected by reasonable safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure.

- **Accountability and oversight:** Entities in control of personal health information must be held accountable for implementing these principles.

- **Remedies:** Legal and financial remedies must exist to address any security breaches or privacy violations.

---

**Connecting Americans to Their Health Care: A Common Framework for Networked Personal Health Information** (December 2006) — which envisions a consumer-accessible data stream, consisting of electronic copies of personal health data that have been captured at various points on a network (e.g., doctor’s offices, hospital systems, pharmacies and pharmacy benefit managers, labs, diagnostic imaging services, etc.).

---

15 Available online at: [http://www.connectingforhealth.org/commonframework/doc/Pg_NetworkedPHRs.pdf](http://www.connectingforhealth.org/commonframework/doc/Pg_NetworkedPHRs.pdf).
APPENDIX D: OTHER GROUPS WORKING ON AUTHENTICATION

The following paragraphs list several authentication projects that currently exist. This list is based on input from Authentication Work Group members and is not comprehensive.

**Electronic Authentication Partnership (EAP)**
Building off the work of the E-Authentication Federation (see below) and other authentication federations, EAP has developed as a “multi-industry partnership working on the vital task of enabling interoperability for electronic authentication among public and private sector organizations.” It is sort of a federation of federations. This group is creating a framework for accrediting and compliance testing of participating Credential Service Providers (CSPs) and Relying Parties (RPs). EAP also addresses the issue of liability.

See: [http://eapartnership.org/](http://eapartnership.org/)


**E-Authentication Federation**
The E-Authentication E-Government Initiative is one of the President’s 24 cross-agency E-Government Initiatives. Its mission is to put in place the necessary infrastructure to support common, unified processes and systems for government-wide use. E-Authentication recently launched the E-Authentication Federation (EAF), “a public-private partnership that enables citizens, businesses, and government employees to access online government services using log-in IDs issued by trusted third parties, both within and outside the government.” Currently 13 different agency web applications are using the service. EAF has focused on the creation of policies, systems, and relationships that reuse existing credentials to meet the needs of mostly federal government-relying parties. EAF has created a framework by which a variety of Credential Service Providers — currently including federal, state, and private sector organizations — issue credentials to be trusted by Relying Parties in the federal government.

(Quotations taken from E-Authentication web site: [http://www.cio.gov/eauthentication/](http://www.cio.gov/eauthentication/))

**Privacy:**

**E-Authentication Guidance for Federal Agencies (M-04-04):**
[http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf](http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf)

**NI ST 800-63: E-Authentication Technical Guidelines:**
[http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf](http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf)

**NI ST 800-53: Recommended Security Controls for Federal Information Systems**

**Liberty Alliance Project**
In 2001, a consortium of 30 organizations formed the Liberty Alliance Project. The project’s stated mission is: “to establish an open standard for federated network identity through open technical specifications.” Over the past few years, they have published an “open framework for deploying and managing a variety of identity-enabled Web Services.” Liberty Alliance is currently working on a framework for “deploying and managing interoperable strong authentication.”

Liberty Alliance is a standards group. Liberty Alliance is represented on the EAP and involved either directly, or through efforts of members and the products and services they provide, with the other efforts.

(Quotations taken from Liberty Alliance Project web site: [http://www.projectliberty.org/](http://www.projectliberty.org/))

**eC3**
eC3 is an alliance of state and local governmental associations. Their mission is to advance the use of electronic commerce by governmental organizations. As part of this...
mission, they have published several white papers concerning identity management.

See: http://www.ec3.org/index.htm

SAFE-Biopharma Association
This identity management organization maintains and enforces the SAFE framework, which permits bio-pharmaceutical companies to digitally sign business-to-business and business-to-regulator transactions.
SAFE is a successfully operating federation which has solved a number of important cross-boundary issues including those of private-public sector and international boundaries. Based in the health industry, it is familiar with health issues and familiar to current industry participants. Representatives of SAFE participate in EAP.

See: http://www.safe-biopharma.org/

HSPD-12 / FIPS 201 / PIV
On August 17, 2004, President Bush issued Homeland Security Presidential Directive - 12 (HSPD-12). This directive called for a common identification standard for all federal employees and contractors. Given this directive, the National Institutes for Standards and Technology developed the Federal Information Processing Standards Publication 201 (FIPS 201), entitled Personal Identity Verification of Federal Employees and Contractors (PIV). This project will provide credentials to 10 to 12 million people at a relatively high level of verification and authentication and could be rolled out to many others through various extensions.

See Personal Identity Verification web site: http://csrc.nist.gov/piv-program/index.html

Real ID Act
The Real ID Act was passed in 2005 by Congress. The Act is intended to deter terrorism. Among other things, the law states that after May 11, 2008, no Federal agency may accept, for official purposes, a state driver’s license as proof of identity unless that state’s driver’s license meets certain requirements defined by the Real ID Act. There is a debate as to whether the Act creates a national ID. The debate aside, unless the law is repealed, it will likely have a significant impact on how individuals in America manage their identities.

Real ID requires issuance of a machine readable credential based upon enhanced identity verification as well as improved security practice and technology. Many people are working diligently to ensure that it becomes a widely usable component of an identity infrastructure. There will likely be many different ways to use the Real ID credentials as functions are built to extend the systems or use of the credentials and as States and/or the Federal Government extend the infrastructure. It is possible that one or more States could choose to issue further electronic credentials, PIN’s, passwords, PKI certificates, etc., in conjunction with Real ID and/or join EAF or EAP to provide a channel for citizens to use the credentials across a broader range of our society.

Shibboleth
According to its Web site, Shibboleth is “standards-based, open source middleware software which provides Web Single SignOn (SSO) across or within organizational boundaries." As part of the Internet2 project, Shibboleth “is developing architectures, policy structures, practical technologies, and an open source implementation to support inter-institutional sharing of web resources subject to access controls. In addition, Shibboleth will develop a policy framework that will allow interoperation within the higher education community." The Shibboleth federation approach is being widely adopted in this country by educational institutions and internationally by government and private sector organizations. It is working to align its policies and practices to allow interoperability with EAF, EAP and others. Examples of initiatives that have adopted Shibboleth technology include: InCommon, EduCause, and LionShare. InCommon has set up InQueue as a learning environment for participating organizations.

See: http://shibboleth.internet2.edu/
**Bylaws:**
http://www.incommonfederation.org/docs/policies/InC_SCbylaws.html

**Participant Operational Practices:**
http://www.incommonfederation.org/docs/policies/incommonfopp.html

**Federation Operating Practices and Procedures:**
http://www.incommonfederation.org/docs/policies/incommonfopp.html

**Trust Service (WebTrust/ SysTrust)**
The American Institute of Certified Public Accountants initiated the WebTrust/SysTrust project. The AICPA's Trust Services are defined as "a set of professional assurance and advisory services based on a common framework (i.e., a core set of principles and criteria) to address the risks and opportunities of IT." Essentially, the project enables CPAs to offer a new service to clients: evaluating web sites that involve data transmission (e.g., personal information such as credit card numbers, birth date, health information, etc.). Web sites that meet the WebTrust/SysTrust requirements can post a "seal of approval" logo on their web sites.


**JA-SIG Central Authentication Service (CAS)**
CAS is a single sign on service offered by JA-SIG (Java Architectures). It is an open protocol that appears to be used primarily by the academic community. (It was originally created at Yale University.)

See: [http://www.ja-sig.org/products/cas/](http://www.ja-sig.org/products/cas/)

**OATH**
As described on its web site, OATH is "an industry-wide collaboration to develop an open reference architecture by leveraging existing open standards for the universal adoption of strong authentication." Its vision is to provide "a reference architecture for universal strong authentication across all users and all devices over all networks."


**American Health Information Community (AHIC) Confidentiality, Privacy & Security Work Group**
The American Health Information Community (AHIC), a health IT advisory panel of the U.S. Department of Health and Human Services, in May 2006 established a cross-cutting work group on confidentiality, privacy and security. The Work Group's charge is to "make actionable confidentiality, privacy, and security recommendations to the Community on specific policies that best balance the needs between appropriate information protection and access to support, and accelerate the implementation of the consumer empowerment, chronic care, and electronic health record related breakthroughs."

See: [http://www.hhs.gov/healthit/ahic/confidentiality](http://www.hhs.gov/healthit/ahic/confidentiality)

**Healthcare Information Technology Standards Panel (HITSP)**
HITSP will assist in the development of the U.S. Nationwide Health Information Network (NHIN) by selecting standards and publishing specifications to support use cases developed by AHIC and the Office of the National Coordinator for Health Information Technology (ONC). The Panel is sponsored by the American National Standards Institute (ANSI) in cooperation with strategic partners such as the Healthcare Information and Management Systems Society (HIMSS), the Advanced Technology Institute (ATI), and Booz Allen Hamilton.

See: [http://www.hitsp.org](http://www.hitsp.org)

**Center for Democracy and Technology (CDT)**
In March 2007, the Center for Democracy and Technology released draft principles for identity in the Digital Age.


**PCI Security Standards Council**
The PCI Security Standards Council is an open global forum for the ongoing development, enhancement, storage, dissemination, and
implementation of security standards for account data protection. The PCI Security Standards Council’s mission is to enhance payment account data security by fostering broad adoption of the PCI Security Standards. The organization was founded by American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International.

See: https://www.pcisecuritystandards.org/

Information Technology Association of America (ITAA)
ITAA provides global public policy, business networking, and national leadership to promote the continued rapid growth of the IT industry. The Association represents over 325 information technology companies. ITAA has an Identity Management Committee that was created to provide a forum for industry to work with federal, state, and annual governments to develop best practices for the authentication and verification of identity, as well as to promote the use of technology to increase the security of our credentialing and access systems. Members include companies producing driver’s licenses, national identity credentials, and other identity cards; managing federal, state, and local smart card and identity credentialing programs; providing biometric devices, radio frequency identification technologies, and middleware solutions; as well as performing background checks and other identity proofing services.

See: http://www.itaa.org
APPENDIX E: EAF/EAP LEVELS

The following is a very brief description of the E-Authentication Federation (EAF) among U.S. government agencies and its companion organization for private sector organizations, the E-Authentication Partnership (EAP). Please refer to the EAF home page (http://www.cio.gov/eauthentication/) for comprehensive documents and updates.

The National Institute for Standards and Technology (NIST) has documented EAF policies, standards, practices, and technology. The EAF is designed to create a trust infrastructure for authenticating individuals who wish to connect to Internet-based services from federal agencies. The EAP, which licenses EAF standards, is a partnership attempting to enable interoperability for electronic authentication among public and private sector organizations. The EAF is further developed than the EAP, and for simplicity, we will refer to EAF for the rest of this discussion.

Joining the EAF requires Credential Service Providers and Relying Parties to agree to use the components of the infrastructure, and to abide by the Business Rules and Operating Rules and comply with the requirements of the appropriate documents such as NIST SP 800-53 or NIST SP 800-63.

<table>
<thead>
<tr>
<th>Credential Service Provider</th>
<th>An organization that offers one or more credential services (i.e., proofs and provides credential to individuals).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relying Party</td>
<td>A person or agency that relies on the credentials issued by a Credential Service Provider.</td>
</tr>
</tbody>
</table>

There are many technology, security, privacy, business, and operating requirements for all participating organizations covered by the suite of documents and components used to guide the implementation of the EAF. The following discussion will focus on those specific to identity proofing and credentials of individual users.

Relying parties within the EAF self-assess the risk associated with reliance upon e-

authentication credentials. Based upon this risk assessment, the relying party chooses which of four designated levels of authentication stringency will be required for accessing one or more of its online resources such as web sites, applications, or information.

Level 1 has no level-specific requirements for proofing or issuance (and thus does not have a section in the chart below). This level can be employed when the Relying Party does not have a need to ascertain the identity of the person accessing a resource. The consumer employs self-assertion, and she may employ a pseudonym. Due to the lack of identity proofing, the low level of security provided by Level 1 authentication is inappropriate for use in facilitating access to personal health information.

---

**Proofing Requirements Under EAF**

The table below\(^\text{17}\) summarizes the requirements of Levels 2-4. Both in-person and remote identity proofing methods are permitted for Levels 2 and 3. Explicit requirements are specified for each scenario in Levels 2 and 3. Only in-person initial proofing is permitted at Level 4.

<table>
<thead>
<tr>
<th>LEVEL 2</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>In-Person</td>
<td>Remote</td>
</tr>
<tr>
<td>Basis for issuing credentials</td>
<td>Possession of a valid current primary Government Photo-ID that contains applicant’s picture and either address of record or nationality (e.g., driver’s license or passport)</td>
<td>Possession of a valid Government ID (e.g., a driver’s license or passport) number and a financial account number (e.g., checking account, savings account, loan, or credit card) with confirmation via records of either number.</td>
</tr>
<tr>
<td>Registration Authority Actions (Proofing)</td>
<td>Inspects Photo-ID, compares picture to applicant, records ID number, address, and DoB. If ID appears valid and photo matches, applicant then: a) If ID confirms address of record, authorizes or issues credentials and sends notice to address of record, or; b) If ID does not confirm address of record, issues credentials in a manner that confirms the address of record.</td>
<td>Inspects both ID number and account number supplied by applicant. Verifies information provided by applicant including ID number or account number through record checks either with the applicable agency or institution, or through credit bureaus or similar databases, and confirms that: name, DoB, address, other personal information in records are on balance consistent with the application and sufficient to identify a unique individual. Address confirmation and notification: a. Sends notice to an address record confirmed in the records check or; b. Issues credentials in a manner that confirms the address of record supplied by the applicant; or c. Issues credentials in a manner that confirms the ability of the applicant to receive telephone communications or e-mail at number or e-mail address associated with the applicant in records.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>LEVEL 3</strong></th>
<th><strong>In-Person</strong></th>
<th><strong>Remote</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Basis for issuing credentials</strong></td>
<td>Possession of verified current primary Government Photo-ID that contains applicant’s picture and either address of record or nationality (e.g., driver’s license or passport)</td>
<td>Possession of a valid Government ID (e.g., a driver's license or passport) number and a financial account number (e.g., checking account, savings account, loan, or credit card) with confirmation via records of both numbers.</td>
</tr>
<tr>
<td><strong>Registration Authority Actions (Proofing)</strong></td>
<td>Inspects Photo-ID and verifies via the issuing government agency or through credit bureaus or similar databases. Confirms that: name, DoB, address, and other personal information in record are consistent with the application. Compares picture to applicant, records ID number, address, and DoB. If ID is valid and photo matches applicant then:</td>
<td>Verifies information provided by applicant including ID number and account number through record checks, either with the applicable agency or institution, or through credit bureaus or similar databases, and confirms that: name, DoB, address, and other personal information in records are consistent with the application and sufficient to identify a unique individual. Address confirmation:</td>
</tr>
<tr>
<td></td>
<td>a) If ID confirms address of record, authorizes or issues credentials and sends notice to address of record, or;</td>
<td>a. Issues credentials in a manner that confirms the address of record supplied by the applicant; or</td>
</tr>
<tr>
<td></td>
<td>b) If ID does not confirm address of record, issues credentials in a manner that confirms address of record</td>
<td>b. Issues credentials in a manner that confirms the ability of the applicant to receive telephone communications at a number associated with the applicant in records, while recording the applicant’s voice.</td>
</tr>
<tr>
<td>LEVEL 4</td>
<td>In-Person</td>
<td>Remote</td>
</tr>
<tr>
<td>---------</td>
<td>-----------</td>
<td>--------</td>
</tr>
<tr>
<td><strong>Basis for issuing credentials</strong></td>
<td>In person appearance and verification of two independent ID documents or accounts, meeting the requirements of Level 3 (in person and remote), one of which must be current primary Government Photo-ID that contains applicant’s picture and either address of record or nationality (e.g., driver’s license or passport), and a new recording of a biometric of the applicant at the time of application</td>
<td>Not applicable</td>
</tr>
<tr>
<td><strong>Registration Authority Actions (Proofing)</strong></td>
<td>• <em>Primary Photo-ID</em>: Inspects Photo-ID and verifies via the issuing government agency, compares picture to applicant, records ID number, address, and DoB.</td>
<td>Not applicable</td>
</tr>
<tr>
<td></td>
<td>• <em>Secondary Government ID or financial account</em></td>
<td></td>
</tr>
<tr>
<td></td>
<td>a. Inspects Photo-ID and if apparently valid, compares picture to applicant, record ID number, address, and DoB, or;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. Verifies financial account number supplied by applicant through record checks or through credit bureaus or similar databases, and confirms that: name, DoB, address, other personal information in records are on balance consistent with the application and sufficient to identify a unique individual.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <em>Records Current Biometric</em> Record - a current biometric (e.g., photograph or fingerprints to ensure that applicant cannot repudiate application).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <em>Confirms Address</em> - Issues credentials in a manner that confirms address of record.</td>
<td></td>
</tr>
</tbody>
</table>
Ongoing Tokens Under EAF

The following tables describe the allowable uses of tokens under EAF levels 2-4. Table 2 shows the types of tokens that may be used at each authentication assurance level. Table 3 identifies the protections that are required at each level. Protections are defined in section 8.1.2 above. Table 4 summarizes the requirements for the resistance of passwords to online password guessing attacks. Table 5 identifies the types of authentication protocols that are applicable to each assurance level. Table 6 identifies additional required protocol and system properties at each level. (NI ST 800-63; page 38, section 9.)

<table>
<thead>
<tr>
<th>Table 2. Token Types Allowed at Each Assurance Level</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Token type</strong></td>
</tr>
<tr>
<td>Hard crypto token</td>
</tr>
<tr>
<td>One-time password device</td>
</tr>
<tr>
<td>Soft crypto token</td>
</tr>
<tr>
<td>Passwords &amp; PINs</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 3. Required Protections</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Protect against</strong></td>
</tr>
<tr>
<td>Online guessing</td>
</tr>
<tr>
<td>Replay</td>
</tr>
<tr>
<td>Eavesdropper</td>
</tr>
<tr>
<td>Verifier impersonation</td>
</tr>
<tr>
<td>Man-in-the-middle</td>
</tr>
<tr>
<td>Session hijacking</td>
</tr>
</tbody>
</table>
APPENDIX F: TWO MODELS OF REMOTE AUTHENTICATION

There are at least two possible architectural solutions to the question of allowing a Health Data Source to accept a Consumer Access Services' request for copies of a consumer's health data. First, the Health Data Source could reauthenticate the consumer. Collectively, we will call this repeated authentication process a two-phase authentication (not to be confused with two-factor authentication). Second, in lieu of re-authenticating the consumer, the remote data source could accept an identity assertion from the Consumer Access Service. Collectively, we will call this scenario authentication plus assertion. The diagram, text, and table below will elaborate on the differences between these two processes.
In **authentication plus assertion** (right hand model), the consumer only authenticates to the Consumer Access Service, which then transmits an assertion to the remote source indicating that the consumer is requesting data. In addition to this assertion, the Consumer Access Service passes along its own organizational credentials. The Consumer Access Service authenticates the consumer, but asserts to the remote data source that it is acting on the consumer's behalf by presenting the demographic information necessary to match the consumer to data held by the remote data source. Therefore, authentication plus assertion assumes that a data owner trusts another entity (i.e., the local application) to authenticate the consumer.

In **two-phase authentication** (left hand model), the consumer has two separate sets of authentication credentials and procedures. Both the Consumer Access Service and the remote data source maintain separate authentication information on the consumer. Each has gone through a process that initially proofs the consumer's identity, and each has an associated method for authenticating the consumer on an ongoing basis. The role of the Consumer Access Service is to both locally authenticate the consumer and to transmit the consumer's information that is required by the remote data source to perform its authentication process. In this second step, the Consumer Access Service acts only as a proxy.

Let's consider an example that illustrates **two-phase authentication**. Programs such as Quicken allow users to download data from remote sources (banks, brokerage firms, etc.) into the local application. When a user wishes to download data from her bank into her Quicken application, she must first authenticate locally (i.e., log into the Quicken software). Then, when she requests a data download, Quicken sends the login-name/password combination that corresponds to her bank's online banking service. (For convenience, the user has already stored her login-name and password within Quicken.) Thus, Quicken acts as the user's proxy during the remote data source authentication process. In the case that the local application is a web-based service, such as the Consumer Access Service, the local application can use mechanisms such as SAML to transmit the user's credentials.

This two-phase authentication model puts the burden of authentication on the consumer and the data sources. The individual must log in to multiple data sources before accessing data through the Consumer Access Service. Data gathering and authentication choices are handled by proximate data sources. Consumer access authentication choices are handled by the Consumer Access Service. This model is the safe deposit model — the consumer's authentication with the Consumer Access Service is unrelated to her authentication with the proximate data sources. There is also nothing specific to health care governing the collection of usernames and logins for remote services, increasing the risk.

However, having established that the consumer has authenticated both at the Consumer Access Service and at a data source, the Consumer Access Service and a data source could set up a business relationship such that all subsequent logins would be treated as the same person. This would make it possible to rely on the clinical data source's proofing mechanism, but the Consumer Access Service's authentication method. The weak link in this system is the Consumer Access Service authentication mechanism. The Consumer Access Service and the clinical data source would have to agree on the stringency of the Consumer Access Service authentication requirements, and have mechanisms for audit and redress.

In **authentication plus assertion**, the consumer only authenticates to the Consumer Access Service, which then transmits an assertion to the remote source indicating that the consumer is requesting data. In addition to this assertion, the Consumer Access Service passes along its own organizational credentials. The Consumer Access Service authenticates the consumer, but asserts to the remote data source that it is acting on the consumer's behalf by presenting the demographic information necessary to match the consumer to data held by the remote data source. Therefore, authentication plus
assertion assumes that a data owner trusts another entity (i.e., the local application) to authenticate the consumer.

The table below compares these two processes based on a list of issues:

<table>
<thead>
<tr>
<th>Issue</th>
<th>Two-phase Authentication</th>
<th>Authentication plus Assertion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ease of use for consumer</td>
<td></td>
<td>Advantage</td>
</tr>
<tr>
<td>Technical work for implementing authentication</td>
<td></td>
<td>Advantage</td>
</tr>
<tr>
<td>Number of proofing/token problems per remote access</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Susceptibility to man-in-the-middle attacks</td>
<td></td>
<td>Advantage against browser hacks (but open to attacks between Consumer Access Service/data sources)</td>
</tr>
<tr>
<td>Susceptibility to error/abuse by human authorizer</td>
<td>Advantage</td>
<td></td>
</tr>
<tr>
<td>Legal risk for remote data source</td>
<td></td>
<td>Advantage</td>
</tr>
<tr>
<td>Scales well for establishing relationships from data source to Consumer Access Service</td>
<td>Advantage</td>
<td></td>
</tr>
<tr>
<td>Cost to Consumer Access Service to implement</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Cost to individual data sources</td>
<td>High</td>
<td>Low</td>
</tr>
</tbody>
</table>

Authentication plus assertion requires data owners to be willing to delegate authentication to another entity. Unless a data source has developed appropriate legal agreements that cover mistakes made by delegates (e.g., releases of data to the wrong person), the data owner (and its insurance carrier) may be unwilling to delegate its authentication process to others.

**Authentication plus assertion does not scale well from the standpoint of industry** since every local application must have agreements with all remote data sources. As the number of local applications and remote data sources increases, the total number of agreements rises exponentially. Therefore, this model is only practical if one of the following conditions is true:

1. There are a limited number of both data sources and local applications or intermediaries (i.e., if there were only a handful of Consumer Access Service providers.)
2. There are a limited number of data sources.
3. There are a limited number of local applications or intermediaries.

It is not the purpose of our Work Group to endorse one model over another. We believe it important to note that both models will likely be offered in the marketplace for some time to come.
Key Topics in a Model Contract for Health Information Exchange
Key Topics in a Model Contract for Health Information Exchange

Version 1.1
The document you are reading is part of *The Connecting for Health Common Framework*, which is available in full and in its most current version at: [http://www.connectingforhealth.org/](http://www.connectingforhealth.org/). The Common Framework will be revised and expanded over time. As of October 2006, the Common Framework included the following published components:
Key Topics in a Model Contract for Health Information Exchange, Version 1.1

Topic List

Introduction. This document (Topic List) describes the issues addressed by the Connecting for Health Model Contract for Health Information Exchange (Model).

Background. A SNO is to operate as a health information data exchange organization (both regional and affinity) that operates as a part of the National Health Information Network ("NHIN"), a nationwide environment for the electronic exchange of health information.

Use of Model. The Model is based on a number of assumptions, which are described in the following discussion. The Model is not the “answer” for all SNOs. Instead, it is intended to assist in the organization of a SNO by providing a basis upon which to begin drafting that SNO’s Terms and Conditions. All language provided in the Model is intended for informational and educational purposes only. It is not intended, nor should it be used, as a substitute for legal advice. In preparing its own terms and conditions, or other legal documents used in connection with its participation in the NHIN, an organization should consult with legal counsel. Each SNO will have to draft its Terms and Conditions based upon its own organization, operations, system and services, regulatory environment, and so on. Some of the Model’s terms will be inapplicable to some SNOs. The Model shows where some of the variations might be expected to occur.

Overview of Structure

Common Framework Policies and Procedures. The Model assumes that the NHIN will be implemented in accordance with a compilation of documents to be known as the “Common Framework Policies and Procedures.” The Common Framework Policies and Procedures will describe how the NHIN works and will include certain terms that should apply to all SNOs. The Model makes a number of assumptions about the future structure and content of the Common Framework Policies and Procedures, which are identified throughout the document. The Model should be revisited and revised as necessary to work with the Common Framework Policies and Procedures as they develop.

SNO Terms and Conditions. The Model assumes that each SNO will adopt its own “Terms and Conditions” which will be comprised of terms that apply to that SNO only, and will also incorporate the provisions of the Common Framework Policies and Procedures that apply to all SNOs.

Registration and Registration Agreements. The Model assumes that Participants will receive access to the SNO’s Services and/or access to the SNO’s System by registering with a SNO and entering into a “Registration Agreement.” The Registration Agreement will incorporate the SNO Terms and Conditions by reference and will require the Participant to comply with those parts of the Terms and Conditions that apply to the Participant, based on how the Participant uses the SNO’s Services and/or System.

©2006, Markle Foundation
This work was originally published as part of The Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange and is made available subject to the terms of a license (License) which may be viewed in its entirety at: http://www.connectingforhealth.org/license.html. You may make copies of this work; however, by copying or exercising any other rights to the work, you accept and agree to be bound by the terms of the License. All copies of this work must reproduce this copyright information and notice.
SNO Organization and Operations. The Model assumes that the SNO is a non-profit or for-profit legal entity that is organized and operated for a single purpose, i.e., to operate as a SNO. The SNO is assumed to operate with a record locator service-based, peer to peer network, and to provide, or provide access to, the software Participants require to use the SNO’s Services. SNOs may provide a different system or services, such as by acting as an application service provider (“ASP”), and the Model identifies some of the variations that are likely if the SNO is organized differently from what the Model assumes.

Defined Terms. The Model assumes that a variety of different types of entities will participate in the SNO, and that these Participants will have a variety of roles. Section 2 (Definitions) of the Model provides a framework for naming these different Participants and their respective roles.

For each section of the Model, this document provides a brief description of the contents of the section and the critical legal and policy issues raised by each. For some sections, alternative provisions are offered.

Model Terms and Conditions

Topic List

1. Introduction. A description of the Sub-Network Organization or “SNO” and how it is organized and operated, in order to provide information that may be helpful for putting the remainder of the Terms and Conditions into context.

1.1 Nature of Organization. The legal structure within which the SNO is organized, and the SNO’s essential relationships to sponsors, founders and others.

1.2 Purposes. The purposes for which the SNO is organized.

1.3 Description of Services. The facilities and services of the SNO that are subject to the SNO Terms and Conditions, and that are available to Participants.

1.4 Change or Termination of Services. The SNO’s right to change its services or to cease providing services.

2. Definitions. The definitions of certain important terms used in the Terms and Conditions. Some of these definitions may not correspond to their use in certain other contexts, and are likely to vary if the SNO’s organization, operations, system, services and/or relationships with others are different than those assumed by the Model.

“Authorized User” means an individual Participant or an individual designated to use the SNO’s Services on behalf of the Participant, including without limitation, an employee of the Participant and/or a credentialed member of the Participant’s medical staff.

“Data Provider” means a Participant that is registered to provide information to the SNO for use through the SNO’s Services.

“HIPAA” means the Health Insurance Portability and Accountability Act of 1996 and the regulations promulgated thereunder at 45 CFR Parts 160 and 164.
“Participant” means a party that registered with the SNO to act as a Data Provider and/or as a Data Recipient.

“Participant Type” means the category of Participants to which a particular Participant is assigned based upon that Participant’s role in the health care system.

“Patient Data” means information provided by a Data Provider pursuant to Section 7.2 (Provision of Data).

“Registration Agreement” means a legally-binding agreement between the SNO and a Participant pursuant to which the SNO registers the Participant in accordance with, and the Participant agrees to comply with, the SNO Terms and Conditions.

“SNO’s Services” means the information sharing and aggregation services and software described in Section 1.3 (Description of Services) for which the Participant registers as described in Section 4.1 (Registration Required).

“SNO Terms and Conditions” means the terms and conditions set forth in this document, as amended, repealed and/or replaced from time to time as described herein.

“Data Recipient” means a Participant that uses the SNO’s Services to obtain health information.

3. Terms and Conditions. The role of the SNO Terms and Conditions, and how they are developed and administered. These terms are intended to be helpful in putting the other provisions of the SNO Terms and Conditions into context.

3.1 Generally. An overview of how the SNO Terms and Conditions are developed and administered.

3.2 Development and Dissemination; Amendments. How the SNO adopts the SNO Terms and Conditions, makes changes, and informs Participants of those changes.


4. Registration Agreements. Who may be a Participant, and how the SNO will register each Participant. The Model uses the concept of “registering” Participants as the device by which the SNO will monitor and control who uses the SNO’s System and Services, and assumes that the SNO will require Participants to enter into “Registration Agreements” in order to assure that all parties with access to the SNO’s System and Services will be covered by an agreement to comply with the SNO Terms and Conditions.

4.1 Registration Required. The requirement that Participants be registered with the SNO.

4.2 Registration by Agreement. How Participants may enter into a written Registration Agreement with the SNO.

4.3 Online Registration. How Participants may register online.

4.3.1 Registration Form. How the SNO administers online registration.
4.3.2 **Participant Type.** How the SNO will categorize Participants by their respective roles in the health care system, i.e., for the purpose of determining the rights and obligations of those Participants.

4.3.3 **Review of Registration Forms.** The SNO's rights to review registration forms and decide whether or not to accept any given party's registration.

4.3.4 **Acceptance of Registration.** How registration agreements will be created for online registrants.

4.4 **Effect of Terms and Conditions Upon Registration Agreements.** How Participants will agree to comply with the Terms and Conditions.

4.5 **Changes to Terms and Conditions.** How Participants will be made aware of the SNO Terms and Conditions, and will be legally obligated to comply therewith.

4.6 **Termination Based on Objection to Change.** How a Participant may avoid being bound to a Registration Agreement if the Participant objects to a change to the SNO Terms and Conditions.

4.7 **Participant’s Other Rights to Terminate Registration Agreement.** How and under what circumstances a Participant may cease to be a Participant, generally.

4.8 **Participant’s Right to Terminate for Breach of Business Associate Agreement.** A Participant's rights to terminate a Registration Agreement if the SNO fails to perform any obligations it may have as a business associate (as defined in HIPAA) of the Participant.

4.9 **SNO’s Right to Terminate Registration Agreements.** How and under what circumstances the SNO may terminate a Participant’s Registration Agreement.

4.10 **Effect of Termination.** The consequences of terminating a Registration Agreement.

5. **Authorized Users.** Terms that govern use of the SNO Services by the Participant’s Authorized Users. The Model assumes that “user agreements” will not be required of every individual who uses the SNO’s System or Services. Instead, Participants will be responsible for designating the individuals within their organizations who would be authorized to use the SNO’s System and Services (“Authorized User”).

5.1 **Identification of Authorized Users.** How the Participant will designate individuals who will use the SNO’s Services.

5.2 **Passwords and Other Security Mechanisms.** How security mechanisms will be administered, including without limitation how log-on passwords will be provided to Authorized Users.

5.3 **No Use by Other than Authorized Users.** A requirement that the SNO’s System and Services be accessed and used only by Authorized Users.

5.4 **Responsibility for Conduct of Participant and Authorized Users.** The Participant’s responsibility for the conduct of its Authorized Users.
6. **Data Recipient's Right to Use Services.** Provisions that apply specifically to “Data Recipients” (i.e., Participants registered to use the SNO’s Services). Provisions that apply specifically to “Data Providers” (i.e., Participants registered to provide data to the SNO) appear at Section 7 (Data Provider's Obligations).

6.1 **Grant of Rights.** The nature of the Participant's right to use the System and Services.

   6.1.1. **Grant by SNO.** The rights granted by the SNO.

   6.1.2. **NHIN.** The rights granted by the NHIN.

6.2 **Permitted Uses.** The permitted uses of the SNO’s System and Services.

6.3 **Prohibited Uses.** The prohibited uses of the SNO System and the SNO Services applicable under the Common Framework Policies and Procedures, and additional prohibitions imposed by the SNO, if any.

7. **Data Provider's Obligations.** Provisions that apply specifically to “Data Providers” (i.e., Participants registered to provide data). Provisions that apply specifically to “Data Recipients” (i.e., Participants registered to use the SNO's Services) appear at Section 6 (Data Recipient's Right to Use Services).

7.1 **Grant of Rights.** The nature of the Data Provider's right to use the System.

7.2 **Provision of Data.** Terms that apply to the Data Provider's delivery of data to the Network, e.g., format, standards, etc.

7.3 **Measures to Assure Accuracy of Data.** The Data Provider's obligations to provide accurate, complete, and timely information.

7.4 **License.** The Data Provider's agreement that the data it provides will be available for use through the Network.

7.5 **Limitations on Use of Patient Data.** Limitations the SNO will impose upon the uses of information provided by Data Providers, including uses prohibited by the Common Framework Policies and Procedures, state or local laws and regulations specific to the SNO, and other prohibitions the SNO determines are appropriate (but not in conflict with the Common Framework Policies and Procedures).

8. **Software and/or Hardware Provided by SNO.** The Model assumes that the SNO will provide certain software and/or hardware Participants would use to access the System (“Associated Software and/or Hardware”). If the SNO does not provide software and/or hardware to Participants, this section would be omitted.

8.1 **Description.** A description of any software and/or hardware that the SNO will provide to Participants.

8.2 **Grant of License.** A description of the Participant's right to use the Associated Software and/or Hardware.

8.3 **Copying.** Restrictions upon the Participant's right to copy software provided by the SNO.
8.4 Third-Party Software, Hardware and/or Services. How the SNO and Participants will address requirements imposed by third-party software, hardware, and/or service vendors.


9.2 Additional Requirements. Provisions requiring compliance with patient information privacy, security and use laws imposed at the state and/or local level and/or other requirements that the SNO otherwise determines are appropriate (but not inconsistent with the Common Framework Policies and Procedures).

9.3 Business Associate Agreement. Provisions addressing the SNO’s potential role as a business associate of the Participant.

10. Other Obligations of Participants. Additional terms governing the conduct of Participants.

10.1 Compliance with Laws and Regulations. The Participant’s obligations to comply with applicable laws and regulations, generally.

10.2 System Security. The Participant’s obligations to implement reasonable and appropriate measures to maintain the security of the SNO System and to notify the SNO of breaches in security.

10.3 Software and/or Hardware Provided by Participant. Provision requiring the Participant to obtain and maintain all hardware and software required to use the SNO’s System and Services that are not to be provided by the SNO.

10.4 Viruses and Other Threats. Requirements that Participants take appropriate measures to prevent damage to the SNO’s System.

10.5 Training. A description of the training, if any, that the SNO will require the Participant to provide to its personnel.

11. SNO Operations and Responsibilities. Provisions describing the role and responsibilities of the SNO.

11.1 Compliance. The SNO’s obligations to require that all Participants agree to be bound by the SNO Terms and Conditions.

11.2 Training. The SNO’s obligations to provide training for Participants and/or their Authorized Users.

11.3 Telephone and/or E-Mail Support. The SNO’s obligations to provide support for the Participant’s use of the SNO’s System and/or Services.

11.4 Audits and Reports. Audits the SNO is to perform, and reports it is to provide, to Participants.

11.5 Management Committee. Any role Participants would have in governance or decision-making by the SNO.
11.5.1 Composition. The composition of a body in which Participants would be involved.

11.5.2 Meetings and Responsibilities of Management Committee. The responsibilities of such a body and how often it would meet.

11.5.3 Management Committee Bylaws. How this body would be organized and governed.

12. Fees and Charges. Terms regarding amounts, if any, that the Participant will be required to pay to the SNO in order to use the Services.

12.1 Agreed-Upon Fees. Provision for a Participant’s written agreement to take precedence over the SNO Terms and Conditions.

12.2 Service Fees. The SNO’s fees for Participants.

12.3 Changes to Fee Schedule. Provisions allowing the SNO to change its Fee Schedule.

12.4 Miscellaneous Charges. Provisions addressing the SNO’s ability to charge for additional services.

12.5 Payment. How and when payment is due and payable.

12.6 Late Charges. Whether the SNO would impose late charges on delinquent Service Fees and Miscellaneous Charges.

12.7 Suspension of Service. Whether the SNO would be permitted to suspend services until the Participant pays amounts that are due.

12.8 Taxes. The party responsible for payment of taxes arising out of the use of the SNO’s System and/or Services.

12.9 Other Charges and Expenses. The extent to which Participants and/or the SNO are responsible to pay for other expenses relating to their respective roles.

13. Proprietary Information. Provisions concerning the parties’ respective obligations to preserve the confidentiality of others’ proprietary information (i.e., other than health information).


14.1 Carrier lines. The parties’ respective responsibilities with respect to the use of carrier, e.g., telephone lines.

14.2 No Warranties. The extent to which the SNO disclaims warranties it might otherwise be assumed to be making to Participants.

14.3 Other Participants. The extent to which the SNO is responsible for uses of information and/or the Network by others.

14.4 Participant’s Actions. The extent to which the Participant assumes responsibility for its own actions or those of its Authorized Users.
14.5 **Unauthorized Access; Lost or Corrupt Data.** The extent to which the parties are responsible for others’ access to information through the Network, or for misconduct related to the use and/or disclosure of that data, or for the accuracy or completeness of that data.

14.6 **Inaccurate Data.** The extent to which the parties are responsible for inaccurate data obtained through the Network.

14.7 **Patient Care.** The parties’ responsibilities with respect to patient outcomes affected by use of the Network.

14.8 **Limitation of Liability.** The extent to which the parties’ potential legal liabilities to each other are limited.

15. **Insurance and Indemnification.**

15.1 **Insurance.** Whether and to what extent the parties are to be required to carry insurance.

15.2 **Indemnification.** Whether and to what extent the parties would agree to indemnify each other for losses sustained as a result of their relationships or conduct.

15.3 **General Provisions.** General provisions appropriate to a contract including the foregoing terms.
Acknowledgements

The members of the Connecting for Health Policy Subcommittee have accomplished an extraordinary task in less than a year's time—the development of an evolving piece of work that can serve as the core of nationwide health information exchange—the policy components of The Common Framework. During this time, we have been fortunate to work with respected experts in the fields of health, information technology, and privacy law, all of whom have contributed their time, energy, and expertise to a daunting enterprise. Our consultants and volunteers have worked long hours in meetings and conference calls to negotiate the intricacies of such issues as privacy, security, authentication, notification, and consent in health information exchange. We offer them our heartfelt thanks for taking on this journey with us, and look forward to the remaining work ahead.

In addition, we would like to offer special thanks to the volunteers and consultants who authored the initial drafts of this body of work—their hard work created a strong foundation upon which to focus the Subcommittee’s deliberations: Stefaan Verhulst, Clay Shirky, Peter Swire, Gerry Hinkley, Allen Briskin, Marcy Wilder, William Braithwaite, and Janlori Goldman.

Finally, we must note that none of this work would have been possible without the leadership and inspiration of our co-chairs, William Braithwaite and Mark Frisse. They have led us with steady hands and determination of spirit.

Connecting for Health Policy Subcommittee

William Braithwaite, MD, eHealth Initiative, (Co-Chair)
Seth Foldy, MD, City of Milwaukee Health Department

Mark Frisse, MD, MBA, MSc, Vanderbilt Center for Better Health, (Co-Chair)
Janlori Goldman, JD, Columbia College of Physicians and Surgeons

Laura Adams, Rhode Island Quality Institute
Ken Goodman, PhD, University of Miami

Phyllis Borzi, JD, George Washington University Medical Center
John Halamka, MD, CareGroup Healthcare System

Susan Christensen*, JD, Agency for Healthcare Research and Quality, United States Department of Health and Human Services
Joseph Heyman, MD, American Medical Association

Art Davidson, MD, MSHP, Denver Public Health
Gerry Hinkley, JD, Davis, Wright, Tremaine LLP

Mary Jo Deering*, PhD, National Cancer Institute/National Institutes of Health, United States Department of Health and Human Services
Charles Jaffe, MD, PhD, Intel Corporation

Jim Dempsey, JD, Center for Democracy and Technology
Jim Keese, Eastman Kodak Company

Hank Fanberg, Christus Health
Linda Kloss, RHIA, CAE, American Health Information Management Association

Linda Fischetti*, RN, MS, Veterans Health Administration
Gil Kuperman, MD, PhD, New York-Presbyterian Hospital

Omid Moghadam, Intel Corporation
Ned McCulloch, JD, IBM Corporation

Patrick McMahon, Microsoft Corporation
Joyce Niland, PhD, City of Hope National Medical Center

Louise Novotny, Communication Workers of America

Michele O’Connor, MPA, RHIA, MPI Services Initiate

Victoria Prescott, JD, Regenstrief Institute for Healthcare

Marc A. Rodwin, JD, PhD, Suffolk University Law School

Kristen B. Rosati, JD, Coppersmith Gordon Schermer Owens & Nelson PLC

Sara Rosenbaum, JD, George Washington University Medical Center

David A. Ross, ScD, Public Health Informatics Institute

Clay Shirky, New York University (Chair, Technical Subcommittee)

Don Simborg, MD, American Medical Informatics Association

Michael Skinner, Santa Barbara Care Data Exchange

Joel Slackman, BlueCross/BlueShield Association

Peter P. Swire, JD, Moritz College of Law, Ohio State University

Paul Tang, MD, Palo Alto Medical Foundation

Micky Tripathi, Massachusetts eHealth Collaborative

Cynthia Wark*, CAPT, United States Public Health Service Commissioned Corps, Centers for Medicare and Medicaid Services, United States Department of Health and Human Services

John C. Wiesendanger, MHS, West Virginia Medical Institute/Quality Insights of Delaware/Quality Insights of Pennsylvania

Marcy Wilder, JD, Hogan & Hartson LLP

Scott Williams, MD, MPH, HealthInsight

Robert B. Williams, MD, MIS, Deloitte

Joy Wilson, National Conference of State Legislatures

Rochelle Woolley, RxHub

Amy Zimmerman-Levitan, MPH, Rhode Island State Department of Health

*Note: Federal employees participate in the Subcommittee but make no endorsement
A Model Contract for Health Information Exchange
A Model Contract for Health Information Exchange
The document you are reading is part of *The Connecting for Health Common Framework*, which is available in full and in its most current version at: [http://www.connectingforhealth.org/](http://www.connectingforhealth.org/). The Common Framework will be revised and expanded over time. As of October 2006, the Common Framework included the following published components:

**The Common Framework: Overview and Principles**

**Policy Guides: How Information is Protected**
- P1: The Architecture for Privacy in a Networked Health Information Environment
- P2: Model Privacy Policies and Procedures for Health Information Exchange
- P3: Notification and Consent When Using a Record Locator Service
- P4: Correctly Matching Patients with Their Records
- P5: Authentication of System Users
- P6: Patients’ Access to Their Own Health Information
- P7: Auditing Access to and Use of a Health Information Exchange
- P8: Breaches of Confidential Health Information
- P9: A Common Framework for Networked Personal Health Information

**Future Policy Guides**

**Technical Guides: How Information is Exchanged**
- T1: The Common Framework: Technical Issues and Requirements for Implementation
- T2: Health Information Exchange: Architecture Implementation Guide
- T3: Medication History Standards
- T4: Laboratory Results Standards
- T5: Background Issues on Data Quality
- T6: Record Locator Service: Technical Background from the Massachusetts Prototype Community

**Future Technical Guides**

**Model Contractual Language**
- M1: Key Topics in a Model Contract for Health Information Exchange
- M2: A Model Contract for Health Information Exchange
A Model Contract for Health Information Exchange*

Introduction. This document (“Model”) is a model for the organization and content of the Terms and Conditions of a sub-network organization (“SNO”).

Background. A SNO is to operate as a health information data exchange organization (both regional and affinity-based) that operates as a part of the National Health Information Network (“NHIN”), a nationwide environment for the electronic exchange of health information made up of a “network of networks.”

Use of Model. The Model is based on a number of assumptions, which are described in the following discussion. The Model is not the “answer” for all SNOs. Instead, it is intended to assist in the organization of a SNO by providing a basis upon which to begin drafting that SNO’s Terms and Conditions. All language provided in the Model is intended for informational and educational purposes only. It is not intended, nor should it be used, as a substitute for legal advice. In preparing its own Terms and Conditions, or other legal documents used in connection with its participation in the NHIN, an organization should consult with legal counsel. Each SNO will have to draft its Terms and Conditions based upon its own organization, operations, system and services, regulatory environment, and so on. Some of the Model’s terms will be inapplicable to some SNOs. The Model shows where some of the variations might be expected to occur.

Overview of Structure

Common Framework Policies and Procedures. The Model assumes that the NHIN will be implemented in accordance with a compilation of documents to be known as the “Common Framework Policies and Procedures.” The Common Framework Policies and Procedures will describe how the NHIN works and will include certain terms that should apply to all SNOs. The Model makes a number of assumptions about the future structure and content of the Common Framework Policies and Procedures, which are identified throughout the document. The Model should be revisited and revised as necessary to work with the Common Framework Policies and Procedures as they develop.

SNO Terms and Conditions. The Model assumes that each SNO will adopt its own “Terms and Conditions” which will be comprised of terms that apply to that SNO only, and will also incorporate the provisions of the Common Framework Policies and Procedures that apply to all SNOs.

Registration and Registration Agreements. The Model assumes that Participants will receive access to the SNO’s Services and/or access to the SNO’s System by registering with a SNO and entering into a “Registration Agreement.” The Registration Agreement will incorporate the SNO Terms and Conditions by reference and will require the Participant to comply with those parts of the Terms and Conditions that apply to the Participant, based on how the Participant uses the SNO’s Services and/or System.

SNO Organization and Operations. The Model assumes that the SNO is a nonprofit or for-profit legal entity that is organized and operated for a single purpose, i.e., to operate as a SNO. The SNO is assumed to operate with a record locator service-based, peer-to-peer network, and to provide, or provide access

* Connecting for Health thanks Gerry Hinkley and Allen Briskin of Davis Wright Tremaine LLP for drafting this document.

©2006, Markle Foundation
This work was originally published as part of The Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange and is made available subject to the terms of a license (License) which may be viewed in its entirety at: http://www.connectingforhealth.org/license.html. You may make copies of this work; however, by copying or exercising any other rights to the work, you accept and agree to be bound by the terms of the License. All copies of this work must reproduce this copyright information and notice.
to, the software Participants require to use the SNO’s Services. SNOs may provide a different system or services, such as by acting as an application service provider (“ASP”), and the Model identifies some of the variations that are likely if the SNO is organized differently from what the Model assumes.

**Defined Terms.** The Model assumes that a variety of different types of entities will participate in the SNO, and that these Participants will have a variety of roles. Section 2 (Definitions) of the Model provides a framework for naming these different Participants and their respective roles.

For each section of the Model, this document provides a brief description of the contents of the section and the critical legal and policy issues raised by each. For some sections, alternative provisions are offered.
# Table of Contents

1. Introduction... 
  1.1 Nature of Organization. .......................................................... 1
  1.2 Purposes. ............................................................................. 1
  1.3 Description of Services. ....................................................... 1
  1.4 Change or Termination of Services....................................... 2

2. Definitions. 

3. Terms and Conditions. 
  3.1 Generally ........................................................................... 5
  3.2 Development and Dissemination; Amendments. ...................... 5
  3.3 Relationship to Common Framework Policies and Procedures. .... 5

4. Registration Agreements. 
  4.1 Registration Required. ........................................................... 6
  4.2 Registration by Agreement. ................................................... 6
  4.3 Online Registration............................................................... 6
  4.3.1 Registration Form. ............................................................ 7
  4.3.2 Participant Type. .............................................................. 7
  4.3.3 Approval and Disapproval of Registration Forms. ................. 7
  4.3.4 Acceptance of Registration. .............................................. 8
  4.4 Effect of Terms and Conditions Upon Registration Agreements. .... 8
  4.5 Changes to Terms and Conditions. ...................................... 8
  4.6 Termination Based on Objection to Change. ............................ 9
  4.7 Participant’s Other Rights to Terminate Registration Agreement. .... 10
  4.8 Participant’s Right to Terminate for Breach of Business Associate Agreement. 11
  4.9 [SNO Name]’s Right to Terminate Registration Agreements. ......... 12
  4.10 Effect of Termination. ......................................................... 13
  4.11 Survival of Provisions. ......................................................... 13

5. Authorized Users. 
  5.1 Identification of Authorized Users. ........................................ 14
  5.2 Certification of Authorized Users. ......................................... 14
  5.3 Passwords and Other Security Mechanisms. ............................. 15
  5.4 No Use by Other than Authorized Users. ............................... 15
  5.5 Responsibility for Conduct of Participant and Authorized Users. .... 15
  5.6 Termination of Authorized Users. ......................................... 16

  6.1 Grant of Rights. ..................................................................... 17
  6.1.1 Grant by [SNO Name]. ...................................................... 17
  6.1.2 Applicable Common Framework Policies and Procedures. ...... 17
  6.2 Permitted Uses. .................................................................... 18
  6.3 Prohibited Uses. .................................................................... 18
  6.3.1 No Services to Third Parties. ............................................. 19
  6.3.2 No Services Prohibited by Local Laws. .............................. 19
  6.3.3 No Use for Comparative Studies ...................................... 19

7. Data Provider’s Obligations. 
  7.1 Grant of Rights. ..................................................................... 20
  7.1.1 Grant by [SNO Name]. ...................................................... 20
  7.1.2 Applicable Common Framework Policies and Procedures. ...... 20
  7.2 Provision of Data. .................................................................. 20
  7.2.1 Data Providers with Written Registration Agreements. .......... 21
  7.2.2 Data Providers Registering Online. .................................... 21
  7.3 Measures to Assure Accuracy of Data. .................................... 21
  7.3.1 Applicable Common Framework Policies and Procedures. ...... 22
  7.3.2 [SNO Name] Requirements. ............................................. 22
  7.4 License. ............................................................................... 22
  7.5 Limitations on Use of Patient Data. ....................................... 23
  7.5.1 Uses Prohibited by Policies and Procedures. ...................... 23
8. **Software and/or Hardware Provided by [SNO Name]**

8.1 Description. .......................................................................................................................... 24
8.2 Grant of License. .................................................................................................................... 24
8.3 Copying. .................................................................................................................................. 24
8.4 Modifications; Derivative Works. ............................................................................................. 25
8.5 Third-Party Software, Hardware, and/or Services. ................................................................. 25

9. **Protected Health Information**

9.1 Compliance with Policies and Procedures............................................................................. 26
9.2 Additional Requirements. .......................................................................................................... 26
9.3 Reporting of Serious Breaches. ................................................................................................. 26
9.4 Business Associate Agreement. ............................................................................................... 27
9.4.1 Use and Disclosure. ............................................................................................................. 27
9.4.2 Appropriate Safeguards. ....................................................................................................... 27
9.4.3 Reports to Participant. .......................................................................................................... 28
9.4.4 Agents, Subcontractors. ....................................................................................................... 28
9.4.5 Inspection and Copying. ....................................................................................................... 28
9.4.6 Amendments. ..................................................................................................................... 28
9.4.7 Reports. ............................................................................................................................. 28
9.4.8 Availability of Records. ....................................................................................................... 28
9.4.9 Action Upon Termination. ................................................................................................. 29
9.4.10 Special Termination. ......................................................................................................... 29

10. **Other Obligations of Participants**

10.1 Compliance with Laws and Regulations. ............................................................................ 30
10.2 System Security. ................................................................................................................... 30
10.2.1 [Additional Security Measures, if desired]. ........................................................................ 30
10.3 Software and Hardware Provided by Participant. .................................................................. 30
10.4 Malicious Software, Viruses, and Other Threats. ................................................................. 31
10.5 Training. ............................................................................................................................... 31

11. **[SNO Name]’s Operations and Responsibilities**

11.1 Compliance with Terms and Conditions. ............................................................................ 32
11.2 Maintenance of System. ......................................................................................................... 32
11.3 Training. ............................................................................................................................... 32
11.4 Telephone and/or E-Mail Support. ......................................................................................... 32
11.5 Audits and Reports. ................................................................................................................. 33
11.5.1 Usage Reports. .................................................................................................................. 33
11.5.2 Reports to Public Agencies. ............................................................................................... 33
11.5.3 Audit Trail Reports. .......................................................................................................... 33
11.6 Management Committee. ...................................................................................................... 33
11.6.1 Composition....................................................................................................................... 33
11.6.2 Meetings and Responsibilities of Management Committee. ............................................ 34
11.6.3 Management Committee Bylaws. ..................................................................................... 34

12. **Fees and Charges**

12.1 Agreed-Upon Fees................................................................................................................ 35
12.2 Service Fees. ........................................................................................................................ 35
12.3 Changes to Fee Schedule. ..................................................................................................... 35
12.4 Miscellaneous Charges. ........................................................................................................ 35
12.5 Payment................................................................................................................................. 36
12.6 Late Charges........................................................................................................................ 36
12.7 Suspension of Service. ......................................................................................................... 36
12.8 Taxes.................................................................................................................................... 36
12.9 Other Charges and Expenses............................................................................................... 37

13. **Proprietary Information**

13.1 Scope of Proprietary Information. ....................................................................................... 38
13.2 Nondisclosure of Proprietary Information............................................................................ 38
13.3 Equitable Remedies............................................................................................................... 39
### 13.4 Notice of Disclosure

**14. Disclaimers, Exclusions of Warranties, Limitations of Liability, and Indemnifications**

- **14.1 Carrier Lines.**
- **14.2 No Warranties.**
- **14.3 Other Participants.**
- **14.4 Participant's Actions.**
- **14.5 Unauthorized Access; Lost or Corrupt Data.**
- **14.6 Inaccurate Data.**
- **14.7 Patient Care.**
- **14.8 Limitation of Liability.**

**15. Insurance and Indemnification**

- **15.1 Insurance.**
  - [Additional Insurance Requirements, if desired]
- **15.2 Indemnification.**
  - **15.2.1 Generally.**
  - **15.2.2 Specific Indemnities.**
  - **15.2.3 Rules for Indemnification.**

**16. General Provisions**

- **16.1 Applicable Law.**
- **16.2 Non-Assignability.**
- **16.3 Third-Party Beneficiaries.**
- **16.4 Supervening Circumstances.**
- **16.5 Severability.**
- **16.6 Notices.**
- **16.7 Waiver.**
- **16.8 Complete Understanding.**
## 1. Introduction.

A description of the sub-network organization or (“SNO”) and how it is organized and operated, in order to provide information that may be helpful for putting the remainder of the Terms and Conditions into context. The SNO may choose to omit some or all of this section if it is found to be unnecessary.

### 1.1 Nature of Organization.

The legal structure within which the SNO is organized, and the SNO’s essential relationships to sponsors, founders, and others.

[Name of SNO] ("[SNO Name]") is [insert type of organization and state in which organized, e.g., a California public benefit corporation], organized by [insert description of founders, sponsors, etc.]. [SNO Name] is a participant in the National Health Information Network ("NHIN").

The Model provides that the SNO may make changes to its Terms and Conditions at any time (Section 3.2 (Development and Dissemination; Amendments)). Changes that would affect a Participant’s rights and obligations would require the Participant’s consent or acquiescence, and Participants are not required to be bound by such changes if they object to them (Section 4.5 (Changes to Terms and Conditions)). The SNO would be free to change other parts of the SNO Terms and Conditions at will. Therefore, the SNO could change these sections at any time if organizational changes were desired.

### 1.2 Purposes.

The purposes for which the SNO is organized.

[SNO Name] is organized to facilitate health information sharing and aggregation for treatment, payment, operations, public health and research-related purposes through the NHIN and in a manner that complies with all applicable laws and regulations, including without limitation those protecting the privacy and security of health information.

This section would be consistent with the SNO’s mission statement, if applicable.

### 1.3 Description of Services.

The facilities and services of the SNO that are subject to the SNO Terms and Conditions, and that are available to Participants.

[SNO Name] owns and operates an Internet-based authenticated peer-to-peer computer system and search engine for patient health, demographic, and related information that assists its users in locating, and facilitates the sharing and aggregation of, patient data held by multiple health care organizations with disparate health information computer applications ("System"). The System makes the following services available to Participants:  

- [detailed description of Services and Service levels, which—if lengthy—may be described in an exhibit].

The Model assumes that the SNO’s System will facilitate the sharing and aggregation of health information maintained separately by various health care organizations, and not maintained by the SNO itself, i.e., the SNO will not provide a centralized repository for health information.

The SNO will revise this section as necessary to reflect the system and services actually provided by the SNO. It should describe the SNO’s System and Services in detail sufficient for the purposes of Participants’ multilateral participation agreements.

The Model provides that a Participant will be permitted to share and aggregate health information only for specific “permitted uses” and not for “prohibited uses” (see Section 6.2 (Permitted Uses) and Section 6.3 (Prohibited Uses)).
### 1.4 Change or Termination of Services.
The SNO’s right to change its services or to cease providing services.

**Alternative One:** SNO may change or terminate in sole discretion.
[SNO Name] may cease to participate in the NHIN, or may change the System and/or the Services, or may cease providing the Services, at any time in its sole discretion upon notice to Participants.

**OR**

**Alternative Two:** SNO may change or terminate upon minimum period of prior notice.
[SNO Name] may cease to participate in the NHIN, or may change the System and/or the Services, or may cease providing the Services, at any time in its sole discretion upon not less than ninety (90) days prior notice to Participants.

**OR**

**Alternative Three:** SNO may change or terminate upon approval of Management Committee, i.e., body through which Participants and others influence SNO management and governance (see Section 11.6 (Management Committee)).
[SNO Name] may cease to participate in the NHIN, or may change the System and/or the Services, or may cease providing the Services, at any time upon the approval of the Management Committee and upon not less than ninety (90) days prior notice to Participants.

---

Some SNOs may find that certain Participants (e.g., major hospital systems that the SNO determines are essential to the SNO), or their communities generally, will require that the SNO agree to provide its services for at least a specified term and/or continue to participate in the NHIN. This provision preserves the SNO’s rights to change or terminate its services, except as it agrees otherwise in written Registration Agreements with such Participants, as contemplated by Section 4.2 (Registration by Agreement).
## Model Terms and Conditions

<table>
<thead>
<tr>
<th>Notes</th>
</tr>
</thead>
</table>
| **2. Definitions.**  
The definitions of certain important terms used in the Terms and Conditions. Some of these definitions may not correspond to their use in certain other contexts, and are likely to vary if the SNO’s organization, operations, system, services, and/or relationships with others are different than those assumed by the Model. |

| Authorized User | The term “Authorized User” is used to identify the individual users of the SNO’s Services. Authorized Users would receive their rights to use the SNO’s Services either by registering as Participants themselves or through another organization that registers as a Participant and designates individuals who will be authorized to use the SNO’s Services on the Participant’s behalf. For example, an Authorized User may be an individual physician who registers as a Participant. In addition, an Authorized User may be a member of that physician’s office staff designated by the physician, or any one of a number of a hospital’s employees and/or medical staff members authorized by the hospital to act as Authorized Users under the hospital’s registration as a Participant. |

| Data Provider | The Model distinguishes between those Participants who provide data to the Network (“Data Providers”) and those who use that data (“Data Recipients”). A Participant may be a Data Provider, a Data Recipient, or both. Participants are identified as Data Providers and/or Data Recipients during the registration process (Section 4.1 (Registration Required)). Because the SNO is assumed to operate as a record-locator service-based, peer-to-peer network, and not as a maintainer of health information, the Model does not contemplate that individuals will register as Data Providers who would add their own health information to the Network. However, an entity providing such a service to individuals could register as a Data Provider under the Model. |

| Data Recipient | The Model distinguishes between those Participants who provide data to the Network (“Data Providers”) and those who use that data (“Data Recipients”). A Participant may be a Data Provider, a Data Recipient, or both. Participants are identified as Data Providers and/or Data Recipients during the registration process (Section 4.1 (Registration Required)). |

| HIPAA | The term “Participant” is used to refer to both Data Providers and Data Recipients. |

| Participant | The term “Participant” is used to refer to both Data Providers and Data Recipients. |

| HIPAA means the Health Insurance Portability and Accountability Act of 1996 and the regulations promulgated thereunder at 45 CFR Parts 160 and 164. |

| Data Recipient | The Model distinguishes between those Participants who provide data to the Network (“Data Providers”) and those who use that data (“Data Recipients”). A Participant may be a Data Provider, a Data Recipient, or both. Participants are identified as Data Providers and/or Data Recipients during the registration process (Section 4.1 (Registration Required)). |

<p>| Participant | The term “Participant” is used to refer to both Data Providers and Data Recipients. |</p>
<table>
<thead>
<tr>
<th><strong>Model Terms and Conditions</strong></th>
<th><strong>Notes</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Participant Type&quot; means the category of Participants to which a particular Participant is assigned based upon that Participant's role in the health care system, as more specifically described in Section 4.3.2 (Participant Type).</td>
<td></td>
</tr>
<tr>
<td>&quot;Patient Data&quot; means information provided by a Data Provider pursuant to Section 7.2 (Provision of Data).</td>
<td></td>
</tr>
<tr>
<td>&quot;Registration Agreement&quot; means a legally binding agreement between [SNO Name] and a Participant pursuant to which [SNO Name] registers the Participant in accordance with, and the Participant agrees to comply with, the Terms and Conditions.</td>
<td>If the SNO does not wish to obtain Registration Agreements from Participants, this section should be omitted.</td>
</tr>
<tr>
<td>&quot;Services&quot; means the information-sharing and aggregation services and/or software described in Section 1.3 (Description of Services) for which the Participant registers as described in Section 4.1 (Registration Required).</td>
<td>In some situations, particularly where definitions of terms are long and complex, or are better understood in context, the Definitions section may simply provide cross-references to core provisions of the SNO Terms and Conditions.</td>
</tr>
<tr>
<td>&quot;System&quot; means [SNO Name]'s Internet-based authenticated peer-to-peer computer system and search engine for patient health, demographic, and related information that assists its users in locating, and facilitates the sharing and aggregation of, patient data held by multiple health care organizations with disparate health information computer applications, and which allows Authorized Users to authenticate and communicate securely over an untrusted network to provide access to and to maintain the integrity of Patient Data.</td>
<td></td>
</tr>
<tr>
<td>&quot;Terms and Conditions&quot; means the terms and conditions set forth in this document, as amended, repealed, and/or replaced from time to time as described herein.</td>
<td></td>
</tr>
</tbody>
</table>
### 3. Terms and Conditions.
The role of the SNO Terms and Conditions, and how they are developed and administered. These terms are intended to be helpful in putting the other provisions of the SNO Terms and Conditions into context.

#### 3.1 Generally.
The Terms and Conditions apply to the operation of the System, the provision of the Services, and the relationships among [SNO Name] and Participants with respect thereto.

#### 3.2 Development and Dissemination; Amendments.
How the SNO adopts the SNO Terms and Conditions, makes changes to the Terms and Conditions, and informs Participants of those changes.

[SNO Name] is solely responsible for the development of the Terms and Conditions, and may amend, or repeal and replace, the Terms and Conditions at any time as [SNO Name] determines is appropriate. [SNO Name] generally shall notify all Participants of any changes to the Terms and Conditions at least thirty (30) days prior to the implementation of the change. However, if the change is required in order for [SNO Name] and/or Participants to comply with applicable laws or regulations, [SNO Name] may implement the change within a shorter period of time as [SNO Name] determines is appropriate under the circumstances.

Because the SNO Terms and Conditions are to be incorporated into each Participant's Registration Agreement, the SNO may find it necessary to limit its ability to change certain provisions of the SNO Terms and Conditions. These limits may be described in this part of the SNO Terms and Conditions. The Model assumes that the SNO may make changes at will, but that Participants must either consent or acquiesce to changes that affect their rights or obligations (see Section 4.2 (Registration by Agreement) and Section 4.5 (Changes to Terms and Conditions)).

The SNO may find that Participants or other members of the SNO's community wish to participate in the development of the Terms and Conditions, as well as participate in the decision to make changes. For this reason, the Model's discussion of the Management Committee allows for the possibility that Participants and/or others will be involved in deciding upon changes to the Terms and Conditions (see Section 11.6 (Management Committee)).

#### 3.3 Relationship to Common Framework Policies and Procedures.
The relationship of the SNO Terms and Conditions to the Common Framework Policies and Procedures.

[SNO Name] has agreed to participate in the NHIN and to comply with the Common Framework Policies and Procedures (the "Common Framework Policies and Procedures"). The Terms and Conditions are intended to, and shall be construed to, comply with the Common Framework Policies and Procedures. The Terms and Conditions incorporate the Common Framework Policies and Procedures, as described herein. Any change to the Common Framework Policies and Procedures that [SNO Name] determines applies to [SNO Name] shall also be incorporated into the Terms and Conditions as of the time [SNO Name] determines is appropriate.

The Model makes a number of assumptions about the future structure and content of the Common Framework Policies and Procedures. The Model should be revisited and revised as necessary to work with the Common Framework Policies and Procedures as they develop.

The Model incorporates by reference into the SNO Terms and Conditions the relevant provisions of the Common Framework Policies and Procedures. Alternatively, the SNO may wish to have the SNO Terms and Conditions repeat the applicable terms of the Common Framework Policies and Procedures.
### Model Terms and Conditions

<table>
<thead>
<tr>
<th>4. Registration Agreements.</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Who may be a Participant, and how the SNO will register each Participant. The Model uses the concept of “registering” Participants as the device by which the SNO will monitor and control who uses the SNO’s System and Services, and assumes that the SNO will require Participants to enter into “Registration Agreements” in order to assure that all parties with access to the SNO’s System and Services will be covered by an agreement to comply with the SNO Terms and Conditions.</td>
<td>The Model uses the legal term “person” to describe both individuals and legal entities (e.g., corporations, limited liability companies, partnerships, etc.). The Model provides that each Participant’s registration will record whether the Participant is a Data Provider, a Data Recipient or both and, if the Participant is a Data Recipient, whether the Participant will be permitted to use some or all of the SNO’s Services.</td>
</tr>
</tbody>
</table>

| 4.1 Registration Required. | The Model assumes that the SNO may wish to enter into written agreements with certain classes of Participants, such as those with whom the SNO wishes either to make special agreements not to be made with all Participants (e.g., a major provider) or those from whom the SNO wishes to obtain special terms (e.g., a major Data Provider). Written Registration Agreements may be comprehensive documents or, to simplify drafting, may incorporate the SNO Terms and Conditions by reference or include the SNO Terms and Conditions as an exhibit. |

| Participants are to be registered with the SNO. | The Model assumes that the SNO may wish to enter into written agreements with certain classes of Participants, such as those with whom the SNO wishes either to make special agreements not to be made with all Participants (e.g., a major provider) or those from whom the SNO wishes to obtain special terms (e.g., a major Data Provider). Written Registration Agreements may be comprehensive documents or, to simplify drafting, may incorporate the SNO Terms and Conditions by reference or include the SNO Terms and Conditions as an exhibit. |

| Only persons who are registered with [SNO Name] as Participants shall be permitted to access the System and use the Services. A Participant may be registered as a Data Provider or as a Data Recipient or as both, as described in this Section 4 (Registration Agreements). A Participant may be registered to use some or all of the Services, as specified in that Participant’s Registration Agreement. | The Model assumes that the SNO may wish to enter into written agreements with certain classes of Participants, such as those with whom the SNO wishes either to make special agreements not to be made with all Participants (e.g., a major provider) or those from whom the SNO wishes to obtain special terms (e.g., a major Data Provider). Written Registration Agreements may be comprehensive documents or, to simplify drafting, may incorporate the SNO Terms and Conditions by reference or include the SNO Terms and Conditions as an exhibit. |

| 4.2 Registration by Agreement. | The Model assumes that the SNO may wish to enter into written agreements with certain classes of Participants, such as those with whom the SNO wishes either to make special agreements not to be made with all Participants (e.g., a major provider) or those from whom the SNO wishes to obtain special terms (e.g., a major Data Provider). Written Registration Agreements may be comprehensive documents or, to simplify drafting, may incorporate the SNO Terms and Conditions by reference or include the SNO Terms and Conditions as an exhibit. |

| How Participants may enter into a written Registration Agreement with the SNO. | The Model assumes that the SNO may wish to enter into written agreements with certain classes of Participants, such as those with whom the SNO wishes either to make special agreements not to be made with all Participants (e.g., a major provider) or those from whom the SNO wishes to obtain special terms (e.g., a major Data Provider). Written Registration Agreements may be comprehensive documents or, to simplify drafting, may incorporate the SNO Terms and Conditions by reference or include the SNO Terms and Conditions as an exhibit. |

| A person may register with [SNO Name] as a Participant by entering into a written Registration Agreement with [SNO Name]. Such a Registration Agreement shall describe: | The Model assumes that the SNO may wish to enter into written agreements with certain classes of Participants, such as those with whom the SNO wishes either to make special agreements not to be made with all Participants (e.g., a major provider) or those from whom the SNO wishes to obtain special terms (e.g., a major Data Provider). Written Registration Agreements may be comprehensive documents or, to simplify drafting, may incorporate the SNO Terms and Conditions by reference or include the SNO Terms and Conditions as an exhibit. |

| a) the Participant’s Participant Type, as described in Section 4.3.2 (Participant Type); | The Model assumes that the SNO may wish to enter into written agreements with certain classes of Participants, such as those with whom the SNO wishes either to make special agreements not to be made with all Participants (e.g., a major provider) or those from whom the SNO wishes to obtain special terms (e.g., a major Data Provider). Written Registration Agreements may be comprehensive documents or, to simplify drafting, may incorporate the SNO Terms and Conditions by reference or include the SNO Terms and Conditions as an exhibit. |

| b) whether the Participant is a Data Provider or a Data Recipient, or both; | The Model assumes that the SNO may wish to enter into written agreements with certain classes of Participants, such as those with whom the SNO wishes either to make special agreements not to be made with all Participants (e.g., a major provider) or those from whom the SNO wishes to obtain special terms (e.g., a major Data Provider). Written Registration Agreements may be comprehensive documents or, to simplify drafting, may incorporate the SNO Terms and Conditions by reference or include the SNO Terms and Conditions as an exhibit. |

| c) if the Participant is registered as a Data Recipient, which of the Services the Participant may use; and | The Model assumes that the SNO may wish to enter into written agreements with certain classes of Participants, such as those with whom the SNO wishes either to make special agreements not to be made with all Participants (e.g., a major provider) or those from whom the SNO wishes to obtain special terms (e.g., a major Data Provider). Written Registration Agreements may be comprehensive documents or, to simplify drafting, may incorporate the SNO Terms and Conditions by reference or include the SNO Terms and Conditions as an exhibit. |

| d) (d) such other terms and conditions as [SNO Name] and the Participant shall agree. | The Model assumes that the SNO may wish to enter into written agreements with certain classes of Participants, such as those with whom the SNO wishes either to make special agreements not to be made with all Participants (e.g., a major provider) or those from whom the SNO wishes to obtain special terms (e.g., a major Data Provider). Written Registration Agreements may be comprehensive documents or, to simplify drafting, may incorporate the SNO Terms and Conditions by reference or include the SNO Terms and Conditions as an exhibit. |

| 4.3 Online Registration. | The Model includes an online registration mechanism to provide a simple way for the SNO to obtain Registration Agreements from those Participants with whom the SNO will not negotiate individual written agreements. If the SNO does not wish to implement or require online registration, this section may be omitted. |

| How Participants may register online. | The Model includes an online registration mechanism to provide a simple way for the SNO to obtain Registration Agreements from those Participants with whom the SNO will not negotiate individual written agreements. If the SNO does not wish to implement or require online registration, this section may be omitted. |
### Model Terms and Conditions

<table>
<thead>
<tr>
<th><strong>4.3.1 Registration Form.</strong></th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>How the SNO administers online registration.</em></td>
<td>A sample online Registration Form is attached as Exhibit 1 (Registration Application and Agreement). Online registration offers a mechanism for collecting Participant information and effecting Registration Agreements efficiently, but it is recognized that the SNO should review and approve and/or authenticate each registration (see Section 4.3.3 (Approval and Disapproval of Registration Forms) and Section 4.3.4 (Acceptance of Registration)) and assure that Participants are appropriately trained in not only the use of the System and the Services but also in the Participant's legal obligation to comply with the terms of its Registration Agreement (see Section 10.5 (Training)).</td>
</tr>
</tbody>
</table>

Each person wishing to register online to access the System and use the Services as a Participant shall complete the Registration Form provided by [SNO Name] at [insert web address]. [SNO Name] may change its Registration Form at any time. A person's Registration Form shall be that person's application to become a Participant. A sample online Registration Form is attached as Exhibit 1 (Registration Application and Agreement). Online registration offers a mechanism for collecting Participant information and effecting Registration Agreements efficiently, but it is recognized that the SNO should review and approve and/or authenticate each registration (see Section 4.3.3 (Approval and Disapproval of Registration Forms) and Section 4.3.4 (Acceptance of Registration)) and assure that Participants are appropriately trained in not only the use of the System and the Services but also in the Participant’s legal obligation to comply with the terms of its Registration Agreement (see Section 10.5 (Training)).

<table>
<thead>
<tr>
<th><strong>4.3.2 Participant Type.</strong></th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>How the SNO will categorize Participants by their respective roles in the health care system.</em></td>
<td>The Model assumes that the SNO will wish to have each Participant assigned to a particular category or “Participant Type,” based on the role that Participant plays in the health care system. The list of Participant Types provided is illustrative only, and each SNO will need to modify the list of categories to conform to the SNO’s System.</td>
</tr>
</tbody>
</table>

Each registrant shall register to participate in one of the following Participant Types:

- a) Physician or medical group;
- b) Laboratory;
- c) Hospital;
- d) Public health agency;
- e) Pharmacy;
- f) Pharmacy benefit manager;
- g) Health plan, insurer or other payor;
- h) Researcher; and
- i) [additional or different provider types selected by the SNO, subject to any limits imposed by the Common Framework Policies and Procedures].

The Model is drafted to provide the SNO maximum flexibility in controlling who may become a Participant. The SNO may wish to reserve the right not to register a particular Participant if, for example, the SNO determines that the person is not eligible to participate or is not expected to comply with the SNO Terms and Conditions. In addition, the SNO may wish to adopt specific credentialing criteria for Participants, which may, if desired by the SNO, be set forth in the SNO Terms and Conditions. The SNO may wish to consider whether it wishes to disclose to an unsuccessful applicant the bases upon which its application for registration was not approved.

<table>
<thead>
<tr>
<th><strong>4.3.3 Approval and Disapproval of Registration Forms.</strong></th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>The SNO will be entitled to review all registration forms and decide not to accept any given party’s registration.</em></td>
<td>The Model is drafted to provide the SNO maximum flexibility in controlling who may become a Participant. The SNO may wish to reserve the right not to register a particular Participant if, for example, the SNO determines that the person is not eligible to participate or is not expected to comply with the SNO Terms and Conditions. In addition, the SNO may wish to adopt specific credentialing criteria for Participants, which may, if desired by the SNO, be set forth in the SNO Terms and Conditions. The SNO may wish to consider whether it wishes to disclose to an unsuccessful applicant the bases upon which its application for registration was not approved.</td>
</tr>
</tbody>
</table>

[SNO Name] shall review each Registration Form and shall approve or disapprove each in accordance with the Terms and Conditions and as [SNO Name] determines in its sole discretion is appropriate. [SNO Name] shall not be required to approve any Registration Form or other application to be a Participant. |
<table>
<thead>
<tr>
<th>Model Terms and Conditions</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>4.3.4 Acceptance of Registration.</strong>&lt;br&gt;How registration agreements will be created for online registrants.</td>
<td>Upon [SNO Name]'s acceptance of a Registration Form, that Registration Form will be the Participant's Registration Agreement and shall be legally binding upon [SNO Name] and the Participant as of the effective date [SNO Name] shall provide to the Participant.</td>
</tr>
<tr>
<td><strong>4.4 Effect of Terms and Conditions Upon Registration Agreements.</strong>&lt;br&gt;How Participants will agree to comply with the Terms and Conditions.</td>
<td>The Model assumes that the SNO Terms and Conditions will contain virtually all of the material terms and conditions that apply to a Participant’s use of the SNO’s System and Services, and therefore will contain most of the terms of each Participant’s multilateral participation agreement. Under this approach, both written and online Registration Agreements will incorporate the SNO Terms and Conditions by reference and contain only those additional terms that apply to the Participant alone, e.g., the Participant’s name, whether the Participant is a Data Provider or Data Recipient or both, the Participant’s Participant Type, etc. The Model gives the SNO broad discretion to create exceptions to the Terms and Conditions, as the SNO determines necessary for particular Participants that enter into written Registration Agreements. The SNO should exercise care in making such exceptions, lest it undermine the effectiveness of the Terms and Conditions with respect to other Participants.</td>
</tr>
<tr>
<td><strong>4.5 Changes to Terms and Conditions.</strong>&lt;br&gt;How Participants will be aware of changes to the SNO Terms and Conditions, and will be legally obligated to comply therewith.</td>
<td>[SNO Name] may amend, repeal and replace the Terms and Conditions at any time, and shall give Participants notice of those changes, as described in Section 3.2 (Development and Dissemination: Amendments). Subject to Section 4.6 (Termination Based on Objection to Change), any such change to the Terms and Conditions shall automatically be incorporated by reference into each Registration Agreement, and be legally binding upon [SNO Name] and the Participant, as of the effective date of the change. The SNO may make changes to the SNO Terms and Conditions at any time. The Model suggests a mechanism by which those changes are automatically incorporated into Registration Agreements, unless a Participant objects to the change.</td>
</tr>
</tbody>
</table>
### 4.6 Termination Based on Objection to Change.

How a Participant may avoid being bound to a Registration Agreement if the Participant objects to a change to the SNO Terms and Conditions.

If a change to the Terms and Conditions described in Section 4.5 (Changes to Terms and Conditions) affects a material right or obligation of a Participant under that Participant’s Registration Agreement, and the Participant objects to that change, that Participant may terminate its Registration Agreement by giving [SNO Name] written notice thereof not more than thirty (30) days following [SNO Name]’s notice of the change. Such termination of the Participant’s Registration Agreement shall be effective as of the effective date of the change to which the Participant objects; provided, however, that any change to the Terms and Conditions that [SNO Name] determines is required to comply with any federal, state, or local law or regulation shall take effect as of the effective date [SNO Name] determines is required, and the termination of any Participant’s Registration Agreement based on the Participant’s objection to the change shall be effective as of [SNO Name]’s receipt of the Participant’s notice of termination.

<table>
<thead>
<tr>
<th>Model Terms and Conditions</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>4.6 Termination Based on Objection to Change.</strong> How a Participant may avoid being bound to a Registration Agreement if the Participant objects to a change to the SNO Terms and Conditions.</td>
<td>The Model allows the SNO to change the SNO Terms and Conditions at will and allows Participants to opt out if they object to the change. Alternatively, the SNO may decide to limit its ability to make changes to the SNO Terms and Conditions and its Registration Agreements.</td>
</tr>
</tbody>
</table>

The Model provides a mechanism for Participants to avoid being bound to changes in the SNO’s Terms and Conditions, but it also recognizes the SNO’s ability to make changes and the potential for Participants to opt out if they object. This section outlines the process for such terminations and emphasizes the importance of communicating changes in a timely manner to ensure all Participants are aware of their rights and obligations under the Registration Agreement.

---

**Connecting for Health Common Framework**

www.connectingforhealth.org | April 2006
### Model Terms and Conditions

<table>
<thead>
<tr>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>The SNO may wish to allow Participants to terminate their participation freely at any time, or to require that termination be preceded by a substantial period of advance notice, or to require that Participants maintain their participation for a year (or longer) at a time. If the SNO wishes to limit further certain Participants’ (e.g., certain data providers) rights to terminate their participation, the SNO may provide for such special terms in written Registration Agreements described in Section 4.2 (Registration by Agreement). If the SNO places limits upon the Participant’s right to terminate, the SNO may wish to provide for the Participant’s right to terminate based on the SNO’s failure to perform. The Model provides a simple &quot;termination for cause&quot; provision. The SNO may wish to qualify a Participant’s right to terminate, e.g., by providing in addition that if the SNO’s failure to perform is one that the SNO cannot reasonably cure within the specified period, then the termination will not take effect so long as the SNO commences and diligently pursues work to cure the failure.</td>
</tr>
</tbody>
</table>

| **4.7 Participant’s Other Rights to Terminate Registration Agreement.** |
| How a Participant may cease to be a Participant, generally. |

**Alternative One: Participant may terminate at any time without cause.**
A Participant may terminate its Registration Agreement at any time without cause by giving notice of that termination to [SNO Name].

**OR**

**Alternative Two: Participant may terminate without cause with prior written notice.**
A Participant may terminate its Registration Agreement at any time without cause by giving not less than ______ days prior notice to [SNO Name].

**OR**

**Alternative Three: Participant may terminate as of the next anniversary of having entered into the Registration Agreement.**
A Participant may terminate its Registration Agreement at any time without cause as of the next anniversary of the effective date of the Participant’s Registration Agreement, by giving not less than _____ days prior notice to [SNO Name].

**OR**

**Alternative Four: Participant may terminate for cause (may be combined with Alternatives Two or Three and/ or Five).**
A Participant may terminate its Registration Agreement upon [SNO Name]’s failure to perform a material responsibility arising out of the Participant’s Registration Agreement, and that failure continues uncured for a period of sixty (60) days after the Participant has given [SNO Name] notice of that failure and requested that [SNO Name] cure that failure.

**OR**

**Alternative Five: Participant may terminate for specified cause (may be combined with Alternatives Two or Three and/ or Four).**
A Participant may terminate its Registration Agreement upon a Serious Breach of Confidentiality or Security, as described in Section 9.3 (Reporting of Serious Breaches), when such Serious Breach of Confidentiality or Security continues uncured for a period of sixty (60) days after the Participant has given [SNO Name] notice of that failure and requested that [SNO Name] cure that breach.
<table>
<thead>
<tr>
<th>Model Terms and Conditions</th>
<th>Notes</th>
</tr>
</thead>
</table>
| **4.8 Participant’s Right to Terminate for Breach of Business Associate Agreement.**  
A Participant’s right to terminate its Registration Agreement based on the SNO’s failure to perform its obligations.  
Notwithstanding any other provision of this Section 4 (Registration Agreements) to the contrary, if Section 9.4 (Business Associate Agreement) applies to a Participant’s Registration Agreement, the Participant may terminate its Registration Agreement as set forth in Section 9.4.10 (Special Termination). |
### Model Terms and Conditions

**4.9 [SNO Name]'s Right to Terminate Registration Agreements.**

*How the SNO may terminate a Participant's Registration Agreement.*

**Alternative One:** SNO may terminate at any time without cause.

Except as provided otherwise in a written Registration Agreement entered into pursuant to Section 4.2 (Registration by Agreement), [SNO Name] may terminate any Participant’s Registration Agreement without cause by giving notice of that termination to the Participant.

**OR**

**Alternative Two:** SNO may terminate without cause with prior written notice.

Except as provided otherwise in a written Registration Agreement entered into pursuant to Section 4.2 (Registration by Agreement), [SNO Name] may terminate any Participant’s Registration Agreement at any time without cause by giving not less than _______ days prior notice to the Participant.

**OR**

**Alternative Three:** SNO may terminate as of the next anniversary of having entered into the Registration Agreement.

Except as provided otherwise in a written Registration Agreement entered into pursuant to Section 4.2 (Registration by Agreement), [SNO Name] may terminate any Participant’s Registration Agreement at any time without cause effective as of the next anniversary of the effective date of the Participant’s Registration Agreement, by giving not less than _____ days prior notice to the Participant.

**OR**

**Alternative Four:** SNO may terminate for cause (may be combined with Alternatives Two or Three).

[SNO Name] may terminate any Participant’s Registration Agreement upon the Participant’s failure to perform a material responsibility arising out of the Participant’s Registration Agreement, and that failure continues uncured for a period of sixty (60) days after [SNO Name] has given the Participant notice of that failure and requested that the Participant cure that failure.

### Notes

It is anticipated that certain Participants, including without limitation those who make substantial investments in order to act as Data Providers, will object to the SNO having the freedom to terminate Registration Agreements without cause. Three alternative approaches are provided here.

In addition, some Participants entering into written Registration Agreements as described in Section 4.2 (Registration by Agreement), may wish to have their agreements further restrict the SNO’s ability to terminate without cause.
### Model Terms and Conditions

#### 4.10 Effect of Termination.
*The consequences of terminating a Registration Agreement.*

Upon any termination of a Participant's Registration Agreement, that party shall cease to be a Participant and thereupon and thereafter neither that party nor its Authorized Users shall have any rights to use the System or the Services. Certain provisions of the Terms and Conditions shall continue to apply to the former Participant and its Authorized Users following that termination, as described in Section 4.11 (Survival Provisions).

#### 4.11 Survival of Provisions.
*The provisions of the Registration Agreement that shall continue to bind the Participant following termination.*

The following provisions of the Terms and Conditions shall survive any termination of a Participant’s Registration Agreement: Section 5.5 (Responsibility for Conduct of Participant and Authorized Users), Section 9 (Protected Health Information), Section 13 (Proprietary Information), Section 14.8 (Limitation on Liability) and Section 15.2.1 (Indemnification).
### 5. Authorized Users.
Terms that govern use of the services by the Participant’s Authorized Users. The Model assumes that user agreements will not be required of every individual who uses the SNO’s System or Services. Instead, Participants will be responsible for designating the individuals within their organizations who would be authorized to use the SNO’s System and Services (“Authorized Users”).

#### 5.1 Identification of Authorized Users.
How the Participant will designate individuals who will access the SNO’s System and/or use the SNO’s Services.

Each Participant shall provide [SNO Name] with a list in a medium and format approved by [SNO Name] identifying all the Participant’s Authorized Users, together with the information described in Schedule 5 (Required Information for Authorized Users), to enable [SNO Name] to establish a unique identifier for each Authorized User. The Participant shall update such list whenever an Authorized User is added or removed by reason of termination of employment or otherwise.

The Model assumes that the Participant will be permitted to select its Authorized Users without review or approval by the SNO. The SNO may, however, wish to adopt specific credentialing criteria for Authorized Users that would be administered by the SNO, and which may, if desired, be set forth in the SNO Terms and Conditions.

The Model assumes that Participants will be required to inform the SNO of changes to their lists of Authorized Users on an ongoing basis. This provision is likely to vary from one SNO to another, depending upon how each SNO decides to allocate responsibilities between the SNO and Participants regarding the administration of Authorized Users.

#### 5.2 Certification of Authorized Users.
How the Participant will provide assurances that its Authorized Users have been trained appropriately.

At the time that Participant identifies an Authorized User to [SNO Name] pursuant to Section 5.1 (Identification of Authorized Users), Participant shall certify to [SNO Name] that the Authorized User:

a) Has completed a training program conducted by Participant in accordance with Section 10.5 (Training);

b) Will be permitted by Participant to use the Services and the System only as reasonably necessary for the performance of Participant’s activities as the Participant Type under which Participant is registered with [SNO Name] pursuant to Section 4.3.2 (Participant Type);

c) Has agreed not to disclose to any other person any passwords [and/or other security measures] issued to the Authorized User pursuant to Section 5.3 (Passwords and Other Security Mechanisms);

d) Has acknowledged [in writing] that his or her failure to comply with the Terms and Conditions may result in the withdrawal of privileges to use the Services and the System and may constitute cause for disciplinary action by Participant; and

e) [Others, if desired].
### Model Terms and Conditions

#### 5.3 Passwords and Other Security Mechanisms.

*How security mechanisms will be administered, including without limitation how log-on passwords will be provided to Authorized Users.*

Based on the information provided by the Participant pursuant to Section 5.1 ([Identification of Authorized Users](#)), [SNO Name] shall issue a user name and password [and/or other security measure] to each Authorized User that shall permit the Authorized User to access the System and use the Services. [SNO Name] shall provide each such user name and password [and/or other security measure] to the Participant and the Participant shall be responsible to communicate that information to the appropriate Authorized User. When the Participant removes an individual from its list of Authorized Users, and informs [SNO Name] of the change, pursuant to Section 5.1 ([Identification of Authorized Users](#)), [SNO Name] shall cancel the user name and password [and/or other security measure] of such individual with respect to the Participant, and cancel and de-activate the user name and password [and/or other security measure] of such individual if that individual is as a result of the change no longer an Authorized User of any Participant.

The Model assumes that the SNO will issue and manage passwords for Authorized Users. This provision is likely to vary from one SNO to another, depending upon how each SNO decides to allocate responsibilities between the SNO and Participants regarding the administration of Authorized Users. It is also likely that the Common Framework Policies and Procedures will impose minimum requirements for passwords and/or other security measures, with which the SNO will be required to comply.

#### 5.4 No Use by Other than Authorized Users.

*A requirement that the SNO’s System and Services be accessed and used only by Authorized Users.*

The Participant shall restrict access to the System and, if applicable, use of the Services, only to the Authorized Users the Participant has identified to [SNO Name] in accordance with Section 5.1 ([Identification of Authorized Users](#)).

#### 5.5 Responsibility for Conduct of Participant and Authorized Users.

*The Participant’s responsibility for the conduct of its Authorized Users.*

The Participant shall be solely responsible for all acts and omissions of the Participant and/or the Participant’s Authorized Users, and all other individuals who access the System and/or use the Services either through the Participant or by use of any password, identifier or log-on received or obtained, directly or indirectly, lawfully or unlawfully, from the Participant or any of the Participant’s Authorized Users, with respect to the System, the Services and/or any confidential and/or other information accessed in connection therewith, and all such acts and omissions shall be deemed to be the acts and omissions of the Participant.

It is likely that the Common Framework Policies and Procedures will include terms that address the liability of SNOs and their Participants for losses their acts or omissions cause to other SNOs and their Participants and/or whether insurance to cover that liability will be required and/or provided (e.g., through an excess insurance pool in which SNOs may or will be required to participate).
<table>
<thead>
<tr>
<th><strong>Model Terms and Conditions</strong></th>
<th><strong>Notes</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>5.6 Termination of Authorized Users.</strong>&lt;br&gt;How the SNO will assure that Participants perform their responsibilities to control the acts of Authorized Users.</td>
<td>Participant shall require that all of its Authorized Users use the System and the Services only in accordance with the Terms and Conditions, including without limitation those governing the confidentiality, privacy and security of protected health information. Participant shall discipline appropriately any of its Authorized Users who fail to act in accordance with the Terms and Conditions in accordance with Participant's disciplinary policies and procedures.</td>
</tr>
</tbody>
</table>
Provisions that apply specifically to “Data Recipients” (i.e., Participants registered to use the SNO’s Services).
Provisions that apply specifically to “Data Providers” (i.e., Participants registered to provide data to the SNO) appear in Section 7 (Data Provider’s Obligations).

If the Participant is registered with [SNO Name] as a Data Recipient, the terms of this Section 6 (Data Recipient’s Right to Use Services) shall apply to that Participant.

<table>
<thead>
<tr>
<th>Model Terms and Conditions</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>6. Grant of Rights.</strong></td>
<td></td>
</tr>
<tr>
<td>The nature of the Data Recipient’s right to use the SNO’s System and Services.</td>
<td></td>
</tr>
<tr>
<td><strong>6.1 Grant by [SNO Name].</strong></td>
<td></td>
</tr>
<tr>
<td>The SNO’s grant of a license to use the SNO Services.</td>
<td>The Model uses the legal term “license” to describe the specific rights to be granted to each Data Recipient.</td>
</tr>
<tr>
<td>[SNO Name] grants to each Data Recipient, and each Data Recipient shall be deemed to have accepted, a non-exclusive, personal, nontransferable, limited right to have access to and to use the System and the Services for which that Data Recipient has registered, subject to the Data Recipient’s full compliance with the Terms and Conditions and the Data Recipient’s Registration Agreement. [SNO Name] retains all other rights to the System and all the components thereof. No Data Recipient shall obtain any rights to the System except for the limited rights to use the System expressly granted by the Terms and Conditions.</td>
<td></td>
</tr>
<tr>
<td><strong>6.1.2 Applicable Common Framework Policies and Procedures.</strong></td>
<td></td>
</tr>
<tr>
<td>The terms of the Common Framework Policies and Procedures that apply to a Data Recipient’s right to use the SNO Services and ownership of the network and information obtained through the network.</td>
<td>As is described in connection with Section 3.3 (Relationship to Common Framework Policies and Procedures), the Model assumes that the SNO Terms and Conditions will incorporate the Common Framework Policies and Procedures by reference.</td>
</tr>
<tr>
<td>All issues concerning the ownership and rights in the NHIN and data and information obtained therefrom shall be as set forth in the Common Framework Policies and Procedures, which is incorporated herein by reference.</td>
<td></td>
</tr>
</tbody>
</table>
### Model Terms and Conditions

| **6.2 Permitted Uses.**  
The permitted uses of the SNO System and Services. | **Notes** |
|---|---|
| **Alternative One: The SNO Terms and Conditions**  
permit Participants to use the System and the Services for any use permitted by the Common Framework Policies and Procedures.  
A Data Recipient may use the System and the Services for which the Participant has registered only for the permitted purposes described in the Common Framework Policies and Procedures, which is incorporated herein by reference. | The Model assumes that the Common Framework Policies and Procedures will describe generally the scope of permitted uses of the Network and information Data Recipients will be able to access through the Network.  
The Model provides that Data Recipients may use only those services for which the Data Recipient has registered pursuant to Section 4.1 (Registration Required). |
| **OR**  
**Alternative Two: The SNO Terms and Conditions**  
would permit a narrower range of use than permitted by the Policies and Procedures, such as limiting use to the location and retrieval of specified data sets.  
A Data Recipient may use the System and the Services only to locate and retrieve the following data sets described for each Service as described on Schedule 6.2 (Permitted Uses). |  |
| **OR**  
**Alternative Three: The SNO Terms and Conditions**  
would permit specific uses for different types of Data Recipients, based on the Participant Type under which the Data Recipient is registered pursuant to Section 4.3.2 (Participant Type).  
A Data Recipient may use the System and the Services only for the permitted uses described on Schedule 6.2 (Permitted Uses) that apply to the Participant Type under which the Data Recipient is registered pursuant to Section 4.3.2 (Participant Type). |  |

### 6.3 Prohibited Uses.

The prohibited uses of the SNO System and the SNO Services applicable under the Common Framework Policies and Procedures, and additional prohibitions imposed by the SNO, if any.

A Data Recipient shall not use or permit the use of the System or the Services for any prohibited use described in the Common Framework Policies and Procedures, which is incorporated herein by reference. [Optional: Without limiting the generality of the foregoing, a Data Recipient shall not use or permit the use of the Services for any use or purpose described below:]

**Examples of additional prohibited uses follow:**

---

The SNO Terms and Conditions may also permit a variety of additional uses, so long as they are not prohibited by the Common Framework Policies and Procedures, e.g., aggregating data for research and chronic disease management studies, public health functions, and measuring provider compliance with standards and protocols such as pay-for-performance standards.
<table>
<thead>
<tr>
<th>Model Terms and Conditions</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>6.3.1. No Services to Third Parties.</strong></td>
<td></td>
</tr>
<tr>
<td>The Data Recipient shall use the System and the Services for which the Data Recipient has registered only for the Data Recipient's own account, and shall not use any part of the System or the Services to provide separate services or sublicenses to any third party, including without limitation providing any service bureau services or equivalent services to a third party.</td>
<td></td>
</tr>
<tr>
<td><strong>6.3.2. No Services Prohibited by Local Laws.</strong></td>
<td></td>
</tr>
<tr>
<td>The Data Recipient shall not use the System or the Services for which the Data Recipient has registered for any purpose or in any manner that is prohibited by the laws of the State of _____________. Without limiting the generality of the foregoing, the Data Recipient shall comply with the following: [list of state or local legal requirements, if desired].</td>
<td></td>
</tr>
<tr>
<td><strong>6.3.3. No Use for Comparative Studies.</strong></td>
<td></td>
</tr>
<tr>
<td>A Data Recipient shall not use the Services to aggregate data to compare the performance of other Participants and/or Authorized Users, without the express written consent of [SNO Name] and each of the Participants and Authorized Users being compared.</td>
<td></td>
</tr>
</tbody>
</table>
### 7. Data Provider’s Obligations.
Provisions that apply specifically to “Data Providers” (i.e., Participants registered to provide data). Provisions that apply specifically to “Data Recipients” (i.e., Participants registered to use the SNO’s Services) appear at Section 6 (Data Recipient’s Right to Use Services).

If the Participant is registered with [SNO Name] as a Data Provider, the terms of this Section 7 (Data Provider's Obligations) shall apply to that Participant.

<table>
<thead>
<tr>
<th>Model Terms and Conditions</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>7.1 Grant of Rights.</strong></td>
<td><strong>The nature of the Data Provider's right to use the System.</strong></td>
</tr>
<tr>
<td><strong>7.1.1 Grant by [SNO Name].</strong></td>
<td><strong>The SNO’s grant of a license to use the SNO System.</strong></td>
</tr>
<tr>
<td>[SNO Name] grants to each Data Provider, and each Data Provider shall be deemed to have accepted, a non-exclusive, personal, nontransferable, limited right to have access to and to use the System for the purposes of complying with the obligations described in this Section 7 (Data Provider's Obligations), subject to the Data Provider's full compliance with the Terms and Conditions and the Data Provider's Registration Agreement. [SNO Name] retains all other rights to the System and all the components thereof. No Data Provider shall obtain any rights to the System except for the limited rights to use the System expressly granted by the Terms and Conditions.</td>
<td>The Model uses the legal term “license” to describe the specific rights to be granted to each Data Provider. The Model generally restricts the Data Provider’s rights to access the SNO’s System to those necessary to provide data in accordance with Section 7.2 (Provision of Data).</td>
</tr>
<tr>
<td><strong>7.1.2 Applicable Common Framework Policies and Procedures.</strong></td>
<td><strong>The terms of the Common Framework Policies and Procedures that apply to a Data Provider’s right to provide data through the SNO System, and ownership of the network and information obtained through the network.</strong></td>
</tr>
<tr>
<td>All issues concerning the ownership and rights in the NHIN shall be as set forth in the Common Framework Policies and Procedures, which is incorporated herein by reference.</td>
<td>As is described in connection with Section 3.3 (Relationship to Common Framework Policies and Procedures), the Model assumes that the SNO Terms and Conditions will incorporate by reference certain specific provisions of the Common Framework Policies and Procedures.</td>
</tr>
<tr>
<td><strong>7.2 Provision of Data.</strong></td>
<td><strong>Terms that apply to the Data Provider's delivery of data to the Network, e.g., format(s), standards, etc.</strong></td>
</tr>
<tr>
<td>Model Terms and Conditions</td>
<td>Notes</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------</td>
</tr>
</tbody>
</table>
| **7.2.1. Data Providers with Written Registration Agreements.**  
*How a written Registration Agreement will describe the Data Provider’s obligations to provide data.*  
If the Data Provider has entered into a written Registration Agreement with [SNO Name] pursuant to Section 4.2 (Registration by Agreement), the Data Provider shall provide the data described in that agreement. | Section 7.2.2 (Data Providers Registering Online) is intended to facilitate administration of a variety of different types of Data Providers. For limited numbers of certain Data Providers, the SNO may find it preferable to enter into specific written agreements that will describe their obligations. |
| **7.2.2. Data Providers Registering Online.**  
*The terms regarding the Data Provider’s obligations to provide data that apply to all other Data Providers.*  
*Alternative One: Data Providers are required to provide specific data sets in specific format(s) based on their type of provider.*  
If the Data Provider has registered with [SNO Name] online pursuant to Section 4.3 (Online Registration), the Data Provider shall participate in and maintain its connection to the System’s record locator service-based, peer-to-peer network and provide through the System the information described in Schedule 7.2 (Provision of Data) as required for the Participant Type under which the Data Provider has registered under Section 4.3.2 (Participant Type) (“Patient Data”).  
*OR*  
*Alternative Two: At the time of registration, Data Providers register to provide specific data sets in specific format(s).*  
If the Data Provider has registered with [SNO Name] online pursuant to Section 4.3 (Online Registration), the Data Provider shall participate in and maintain its connection to the System’s record locator, service-based peer-to-peer network and provide through the System the information the Data Provider registered to provide pursuant to the registration process (“Patient Data”). | Data Providers who did not enter into specific agreements with the SNO would be required to provide the information identified by the SNO as appropriate for providers of their respective type (e.g., laboratories would be required to provide certain types of data and emergency departments would be required to provide different types of data).  
In the alternative, the SNO could decide that the Data Provider would register to provide certain types of data from a list of choices provided online at the time of registration. |
| **7.3. Measures to Assure Accuracy of Data.**  
*The Data Provider’s obligations to provide accurate, complete and timely information.* | The Model assumes that the Common Framework Policies and Procedures will establish minimum standards for Data Providers’ obligations to provide accurate, complete, and timely information. |
### Model Terms and Conditions

<table>
<thead>
<tr>
<th>7.3.1. Applicable Common Framework Policies and Procedures.</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Data Provider’s obligations to comply with the applicable provisions of the Common Framework Policies and Procedures.</td>
<td>The Data Provider shall, in accordance with the Common Framework Policies and Procedures, use reasonable and appropriate efforts to assure that all data it provides to the System is accurate, free from serious error, reasonably complete, and provided in a timely manner.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>7.3.2 [SNO Name] Requirements.</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>The SNO may adopt additional requirements regarding the accuracy of data.</td>
<td>The SNO’s own measures may include, for example, requiring Data Providers to adopt benchmark practices for increasing and maintaining data quality and/or requiring Participants to conduct a data quality assessment and improvement project either before or after becoming a Participant.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>7.4 License.</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Data Provider’s agreement that the data it provides will be available for use through the Network.</td>
<td>The Model uses the legal term “license” to describe the specific rights to be granted with respect to the use of Patient Data provided by the Data Provider.</td>
</tr>
</tbody>
</table>

Subject to Section 7.5 (Limitations on Use of Patient Data), the Data Provider grants to [SNO Name] a perpetual, fully-paid, worldwide, non-exclusive, royalty-free right and license (i) to license and/or otherwise permit others to access through the System and/or the NHIN and use all Patient Data provided by the Data Provider in accordance with the Common Framework Policies and Procedures and the Terms and Conditions, and (ii) to use such Patient Data to carry out [SNO Name]’s duties under the Common Framework Policies and Procedures and the Terms and Conditions, including without limitation system administration, testing, problem identification and resolution, management of the System, data aggregation activities as permitted by applicable state and federal laws and regulations, including without limitation, those promulgated under HIPAA, and otherwise as [SNO Name] determines is necessary and appropriate to comply with and carry out its obligations under all applicable federal, state, and local laws and regulations.
### Model Terms and Conditions

<table>
<thead>
<tr>
<th>Notes</th>
</tr>
</thead>
</table>

#### 7.5 Limitations on Use of Patient Data.  
Limitations the SNO may impose upon the uses of information provided by Data Providers.

Notwithstanding Section 7.4 (License), Patient Data provided by a Data Provider shall not be used for any of the following purposes:

| **7.5.1. Uses Prohibited by Policies and Procedures.**  
The provisions of the Common Framework Policies and Procedures that apply to the use of information provided by Data Providers. |
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Any use that is prohibited by the Common Framework Policies and Procedures.</td>
</tr>
</tbody>
</table>

| **7.5.2. Uses Prohibited by Law.**  
Restrictions imposed by laws that are specific to the SNO, e.g., state and/or local laws. |
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Any use that is prohibited by the laws of the State of ____________. Without limiting the generality of the foregoing, the Data Provider shall comply with the following: [list of state or local legal requirements, if desired].</td>
</tr>
</tbody>
</table>

**Additional prohibitions, if desired, such as:**

| **7.5.3. Comparative Studies.**  
The performance of comparisons of the performance of other Participants and/or Authorized Users without the express written consent of [SNO Name] and each of the Participants and Authorized Users being compared. |
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>See Section 6.3.3 (No Use for Comparative Studies).</td>
</tr>
</tbody>
</table>
### Model Terms and Conditions

<table>
<thead>
<tr>
<th>8. Software and/or Hardware Provided by [SNO Name].</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>8.1 Description.</strong>&lt;br&gt;A description of any software and/or hardware that the SNO will provide to Participants.</td>
<td>The Model assumes that the SNO will provide some of the software and hardware Participants would use to access the System. If the SNO does not provide software and/or hardware to Participants, this section would be omitted. The specific language shown in this section is for illustration only. The SNO will need to tailor the language of this section to the limitations imposed by the SNO’s software and hardware vendor(s).</td>
</tr>
<tr>
<td>[SNO Name] shall provide to each Participant the software and/or hardware required to access the System and use the Services the Participant has registered to receive, as more particularly described on Schedules 8.1(a) (Software) and 8.1(b) (Hardware) (the “Associated Software” and “Associated Hardware,” respectively).</td>
<td>The Model assumes that the SNO will provide some of the software and hardware that Participants will require to use the System, as described in Section 8 (Software and Hardware Provided by [SNO Name]), and that the Participant will be required to provide the remainder (e.g., a personal computer with an operating system and web browser meeting certain specifications), as described in Section 10.3 (Software and Hardware Provided by Participant). The terms of Section 8 (Software and/or Hardware Provided by [SNO Name]) and Section 10.3 (Software and Hardware Provided by Participant) should be revised as necessary to conform to each other.</td>
</tr>
<tr>
<td><strong>8.2 Grant of License.</strong>&lt;br&gt;A description of the Participant’s right to use the Associated Software and Hardware.</td>
<td>The Model assumes that Stark and Anti-Kickback law issues that, depending upon the relationship of the SNO to its Participant, may arise from the SNO’s provision of software, hardware and services, will have been resolved.</td>
</tr>
<tr>
<td>[SNO Name] grants to each Participant a non-exclusive, personal, nontransferable, limited license to use the Associated Software and the Associated Hardware for access to or use of the System and, if the Participant is a Data Recipient, for the purpose of obtaining the Services (the “Associated Software”).</td>
<td>The Model uses the legal term “license” to describe the specific rights to be granted to each Participant.</td>
</tr>
<tr>
<td><strong>8.3 Copying.</strong>&lt;br&gt;Restrictions upon the Participant’s right to copy software provided by the SNO.</td>
<td></td>
</tr>
<tr>
<td><strong>Alternative One: Participant may not make copies.</strong>&lt;br&gt;The Participant shall not, without [SNO Name]’s prior written consent, copy any of the Associated Software.</td>
<td></td>
</tr>
<tr>
<td><strong>OR</strong>&lt;br&gt;<strong>Alternative Two: Participant may make limited copies.</strong>&lt;br&gt;The Participant may make one (1) copy of the whole or any part of the Associated Software in executable form for back-up or archival purposes; provided, that such copy must reproduce and include the copyright notice of [SNO Name].</td>
<td></td>
</tr>
<tr>
<td>Model Terms and Conditions</td>
<td>Notes</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------</td>
</tr>
</tbody>
</table>
| **8.4 Modifications; Derivative Works.**  
*Restrictions upon the Participant's right to modify the System or the Services.*  
The Participant shall not modify, reverse engineer, decompile, disassemble, re-engineer or otherwise create or permit or assist others to create the Associated Software or the System otherwise, or to create any derivative works from the Associated Software or the System. The Participant shall not modify the Associated Software or combine the Associated Software with any other software or services not provided or approved by [SNO Name]. | |
| **8.5 Third-Party Software, Hardware, and/or Services.**  
*How the SNO and Participants will address requirements imposed by third-party software, hardware, and/or service vendors.*  
The Associated Software includes certain third-party software, hardware, and services, which may be subject to separate licenses or subscription or other agreements or may require that a Participant enter into such agreements with third-party vendors. Each Participant shall execute such agreements as may be required for the use of such software, hardware or services, and to comply with the terms of any applicable license or other agreement relating to third-party products included in Associated Software. | |
### 9. Protected Health Information.

*Provisions addressing compliance with applicable laws addressing the confidentiality, security, and use of patient health information.*

<table>
<thead>
<tr>
<th><strong>9.1 Compliance with Policies and Procedures.</strong></th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Provisions requiring compliance with the Common Framework Policies and Procedures.</em></td>
<td>The Model assumes that the Common Framework Policies and Procedures will establish minimum standards regarding the privacy and security of protected health information, and compliance with related requirements, e.g., the maintenance of information required for accounting of disclosures under HIPAA (45 CFR § 164.528), that will apply to all Participants (including Participants that are not “covered entities” under HIPAA, e.g., law enforcement agencies, business associates of covered entities, etc.). The Common Framework Policies and Procedures are anticipated to comply with HIPAA, and may impose higher standards. The SNO Terms and Conditions would incorporate those provisions of the Common Framework Policies and Procedures by reference.</td>
</tr>
<tr>
<td>[SNO Name] and each Participant shall comply with the standards for the confidentiality, security, and use of patient health information, including without limitation protected health information described in HIPAA, as provided in the Common Framework Policies and Procedures, which is incorporated herein by reference. Each Participant shall comply with such standards regardless of whether or not that Participant is a “covered entity” under HIPAA.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>9.2 Additional Requirements.</strong></th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Provisions requiring compliance with patient information privacy, security, and use laws imposed at the state and/or local level.</em></td>
<td>This language is provided for illustration only. The SNO would revise this section to correspond to the terminology and requirements of applicable state and/or local laws.</td>
</tr>
<tr>
<td>[SNO Name] and each Participant shall comply with the requirements for the privacy, security, and use of patient health information imposed under the laws of the State of ____________. Without limiting the generality of the foregoing, [SNO Name] and each Participant shall comply with the following: [list of state or local legal requirements, if desired].</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>9.3 Reporting of Serious Breaches.</strong></th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Provisions requiring the SNO and Participant to report to each other concerning serious breaches of confidentiality of patient health information.</em></td>
<td>The SNO may wish to make other or more specific provisions for the parties’ obligations to report privacy and security breaches, and to define which of those breaches are sufficiently serious as to merit reporting. For example, the SNO could seek the input of the Management Committee 11.6 (Management Committee) or another body.</td>
</tr>
<tr>
<td>Without limiting Section 9.4.7(Reports), if applicable to [SNO Name], [SNO Name] and Participant shall report to the other any serious use or disclosure of Protected Health Information not provided for by the Terms and Conditions of which [SNO Name] or Participant becomes aware, and any security incident concerning electronic Protected Health Information (a “Serious Breach of Confidentiality or Security”). A “Serious Breach of Confidentiality or Security” is one that adversely affects (a) the viability of the NHIN; (b) the trust among Participants or (c) the SNO’s legal liability.</td>
<td></td>
</tr>
</tbody>
</table>
### 9.4 Business Associate Agreement.

Provisions addressing the SNO’s potential role as a business associate of the Participant.

If, through any Data Recipient’s use of the Services, [SNO Name]’s performance of its responsibilities described in the Terms and Conditions causes [SNO Name] to act as the “business associate” of the Data Recipient (as defined in 45 CFR Part 160.103), the provisions of this Section 9.4 (Business Associate Agreement) shall apply, in order to implement the requirements imposed under HIPAA for agreements between covered entities and their business associates. All capitalized terms not defined herein shall have the meanings given to them pursuant to 45 CFR Part 160.103.

#### 9.4.1 Use and Disclosure.

[SNO Name] shall use and disclose Protected Health Information only for the purposes of [SNO Name]’s performance of its responsibilities described in the Terms and Conditions. Without limiting the foregoing, [SNO Name] may use and disclose Protected Health Information for the proper management and administration of [SNO Name]’s business and to carry out its own legal responsibilities; provided, that any disclosure pursuant to this Section 9.4.1 (Use and Disclosure) shall either be required by law or be made with reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to such person, and that the person will notify [SNO Name] of any instances of which it is aware in which the confidentiality of the information has been breached.

#### 9.4.2 Appropriate Safeguards.

[SNO Name] shall use appropriate safeguards to prevent use or disclosure of Protected Health Information other than as permitted by the Terms and Conditions, including administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of that Protected Health Information.
### Model Terms and Conditions

#### 9.4.3. Reports to Participant.

[SNO Name] shall report to the Participant any use or disclosure of Protected Health Information of the Participant not provided for by the Terms and Conditions of which [SNO Name] becomes aware, and any security incident concerning electronic Protected Health Information.

#### 9.4.4. Agents, Subcontractors.

[SNO Name] shall ensure that its agents, including any subcontractor, to whom [SNO Name] provides Protected Health Information agree to the restrictions and conditions that apply to [SNO Name] with respect to such information and implement the safeguards required by Section 9.4.2 (Appropriate Safeguards) with respect to electronic Protected Health Information.

#### 9.4.5. Inspection and Copying.

[SNO Name] shall make Protected Health Information available to a Participant or any person authorized by the Participant for inspection and copying within twenty (20) days of a request by the Participant therefor.

This provision is required only if the SNO maintains a designated record set for the Participant.

#### 9.4.6. Amendments.

[SNO Name] shall make Protected Health Information available for amendment and incorporate any amendments to Protected Health Information requested by the Participant.

This provision is required only if the SNO maintains a designated record set for the Participant.

#### 9.4.7 Reports.

[SNO Name] shall promptly report to the Participant concerning all disclosures of Protected Health Information by [SNO Name] or any subcontractors or agents to whom it discloses Protected Health Information upon request, other than disclosures to carry out treatment, payment, and health care operations on behalf of Participant, or that are incident to such disclosures.


[SNO Name] shall make its internal practices, books, and records relating to the use and disclosure of Protected Health Information available to the Secretary of the United States Department of Health and Human Services, for purposes of determining the Participant’s compliance with its legal obligations.
### Model Terms and Conditions

<table>
<thead>
<tr>
<th>9.4.9. Action Upon Termination.</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Given the role of the System and the NHIN, the destruction or return to the Participant of Protected Health Information following the termination of the Participant's Registration Agreement would be infeasible. Therefore, upon termination of the Participant's Registration Agreement, [SNO Name] shall extend the protections of this Section 9.4 (Business Associate Agreement) to such information, and shall limit further use and disclosure of the information to those purposes that make the return or destruction of the information infeasible.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>9.4.10 Special Termination.</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notwithstanding any other provision of the Terms and Conditions to the contrary, the Participant may immediately terminate its Registration Agreement if it determines that [SNO Name] has violated a material term of this Section 9.4 (Business Associate Agreement), and [SNO Name] fails to remedy the violation within thirty (30) days following receipt of written notice thereof.</td>
<td></td>
</tr>
<tr>
<td>Model Terms and Conditions</td>
<td>Notes</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------</td>
</tr>
</tbody>
</table>
| **10. Other Obligations of Participants.**  
*Additional terms governing the conduct of Participants.* | |
| **10.1 Compliance with Laws and Regulations.**  
*The Participant's obligations to comply with applicable laws and regulations, generally.* | The Model assumes that security requirements are to be described in the Common Framework Policies and Procedures. However, the SNO may wish to adopt additional specific measures to be required, provided that it does so in a manner that is not inconsistent with the Common Framework Policies and Procedures. |
| Without limiting any other provision of the Terms and Conditions relating to the parties' compliance with applicable laws and regulations, the Participants shall perform in all respects as contemplated by the Terms and Conditions, in compliance with applicable federal, state, and local laws, ordinances and regulations. | |
| **10.2 System Security.**  
*The Participant's obligations to implement reasonable and appropriate measures to maintain the security of the SNO System and to notify the SNO of breaches in security.* | |
| The Participant shall implement security measures with respect to the System and the Services in accordance with the Common Framework Policies and Procedures, which is incorporated herein by reference. [Optional: Without limiting the generality of the foregoing, the Participant shall also adopt and implement the additional security measures described below:] | The Model assumes that the SNO will provide some of the software and hardware that Participants will require to use the System, as described in Section 8 (Software and Hardware Provided by [SNO Name]), and that the Participant will be required to provide the remainder (e.g., a personal computer with an operating system and web browser meeting certain specifications), as described in Section 10.3 (Software and/or Hardware Provided by Participant). The terms of Section 8 (Software and/or Hardware Provided by [SNO Name]) and Section 10.3 (Software and Hardware Provided by Participant) should be revised as necessary to conform to each other. |
| **10.2.1 [Additional Security Measures, if desired].** | |
| **10.3 Software and Hardware Provided by Participant.**  
*Provision requiring the Participant to obtain and maintain all hardware and software required to use the System and the Services that is not to be provided by the SNO.* | |
<p>| Each Participant shall be responsible for procuring all equipment and software necessary for it to access the System, use the Services (including the Associated Software), and provide to [SNO Name] all information required to be provided by the Participant (“Participant's Required Hardware and Software”). Each Participant's Required Hardware and Software shall conform to [SNO Name]'s then-current specifications. [SNO Name] may change such specifications from time to time in its sole discretion upon not less than sixty (60) days prior notice to each Participant affected by the change. As part of the Participant's obligation to provide Participant's Required Hardware and Software, the Participant shall be responsible for ensuring that all the Participant's computers to be used to interface with the System are properly configured, including but not limited to the operating system, web browser, and Internet connectivity. |</p>
<table>
<thead>
<tr>
<th><strong>Model Terms and Conditions</strong></th>
<th><strong>Notes</strong></th>
</tr>
</thead>
</table>
| **10.4 Malicious Software, Viruses, and Other Threats.**  
*Requirements that Participants take appropriate measures to prevent damage to the SNO’s System.*  
The Participant shall use reasonable efforts to ensure that its connection to and use of the System, including without limitation the medium containing any data or other information provided to the System, does not include, and that any method of transmitting such data will not introduce, any program, routine, subroutine, or data (including without limitation malicious software or “malware,” viruses, worms, and Trojan Horses) which will disrupt the proper operation of the System or any part thereof or any hardware or software used by [SNO Name] in connection therewith, or which, upon the occurrence of a certain event, the passage of time, or the taking of or failure to take any action will cause the System or any part thereof or any hardware, software or data used by [SNO Name] or any other Participant in connection therewith, to be destroyed, damaged, or rendered inoperable. | |
| **10.5 Training.**  
*A description of the training, if any, that the SNO will require the Participant to provide to its personnel.*  
The Participant shall provide appropriate and adequate training to all of the Participant’s personnel, including without limitation Authorized Users, in the requirements of applicable laws and regulations governing the confidentiality, privacy, and security of protected health information, including without limitation requirements imposed under HIPAA. | |
### Model Terms and Conditions

<table>
<thead>
<tr>
<th>11. [SNO Name]'s Operations and Responsibilities.</th>
<th>Notes</th>
</tr>
</thead>
</table>
| Provisions describing the role and responsibilities of the SNO. | The Model assumes that the SNO will provide a variety of services to Participants. Responsibilities may include:  
- System support  
- Installation support  
- Initial and ongoing training  
- Help desk  
- Problem resolution  
- Auditing and reporting access and use  
- Reporting unauthorized uses and security incidents  
Some examples are provided for purposes of illustration. |

<table>
<thead>
<tr>
<th>11.1 Compliance with Terms and Conditions.</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>The SNO’s obligations to require that all Participants agree to be bound by the SNO Terms and Conditions.</td>
<td>[SNO Name] shall require that all Participants enter into a Registration Agreement or another legally binding agreement to comply with the Terms and Conditions in such form as [SNO Name] determines is appropriate.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>11.2 Maintenance of System.</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>The SNO’s obligations to maintain the functionality of the System and the Services, and to provide updates.</td>
<td>[SNO Name] shall maintain the functionality of the System and the Services in accordance with the Common Framework Policies and Procedures, and shall provide such service, security, and other updates as [SNO Name] determines are appropriate from time to time.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>11.3 Training.</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>The SNO’s obligations to provide training for Participants and/or its Authorized Users.</td>
<td>[SNO Name] shall provide training to each Participant [and/or Authorized User] regarding the Participant’s [and/or the Authorized User’s] rights and obligations under its Registration Agreement and the Terms and Conditions, and the access and use of the System and Services, including such user manuals and other resources [SNO Name] determines appropriate to support the System and Services, including without limitation training for new or additional Authorized Users when added by the Participant.</td>
</tr>
<tr>
<td>Model Terms and Conditions</td>
<td>Notes</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>11.4 Telephone and/or E-Mail Support.</strong>&lt;br&gt;The SNO’s obligations to provide support for the Participant’s use of the SNO’s System and/or Services.</td>
<td></td>
</tr>
<tr>
<td><strong>Alternative One: SNO provides help desk functions.</strong>&lt;br&gt;[SNO Name] shall provide, by telephone and/or e-mail, during normal business hours, support and assistance in resolving difficulties in accessing and using the System and the Services.</td>
<td></td>
</tr>
<tr>
<td><strong>OR</strong>&lt;br&gt;<strong>Alternative Two: SNO supports the Participant’s help desk.</strong>&lt;br&gt;[SNO Name] shall provide, by telephone and/or e-mail, during normal business hours, support and assistance to the Participant’s help desk or other facility that supports use of the System and Services by Authorized Users.</td>
<td></td>
</tr>
<tr>
<td><strong>11.5 Audits and Reports.</strong>&lt;br&gt;Audits the SNO is to perform and reports it is to provide to Participants.</td>
<td>The following provisions are examples of the reports the SNO might provide to Participants.</td>
</tr>
<tr>
<td>[SNO Name] shall perform the following audits and provide the following reports to each Participant:</td>
<td></td>
</tr>
<tr>
<td><strong>11.5.1 Usage Reports.</strong>&lt;br&gt;[Specified statistical reports regarding the Participant’s usage of the Services].</td>
<td></td>
</tr>
<tr>
<td><strong>11.5.2 Reports to Public Agencies.</strong>&lt;br&gt;[Specified reports that certain Participants may be required to make to public health agencies.]</td>
<td></td>
</tr>
<tr>
<td><strong>11.5.3 Audit Trail Reports.</strong>&lt;br&gt;[Specified reports that pertain to audit trail tracking.]</td>
<td></td>
</tr>
<tr>
<td><strong>11.6 Management Committee.</strong>&lt;br&gt;Certain SNOs may wish to include certain terms regarding internal governance and management as a part of the SNO Terms and Conditions, to assure that Participants may be involved in their governance and/or management. The language provided here is for illustration only, and is not intended to limit how the SNO would structure its governance or Participants’ involvement in governance and management. SNOs that do not desire such provisions would omit this section entirely.</td>
<td></td>
</tr>
<tr>
<td>Model Terms and Conditions</td>
<td>Notes</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>11.6.1 Composition.</strong></td>
<td>[SNO Name] shall create and maintain a Management Committee (the “Management Committee”) composed of [specified personnel/representatives of SNO and specified number of Participant representatives, who shall be selected in a specified manner].</td>
</tr>
<tr>
<td><strong>11.6.2 Meetings and Responsibilities of Management Committee.</strong></td>
<td>Issues that a Management Committee could address include, without limitation, technical issues, confidentiality, the scope of information stored and accessed by Participants, the use of the information, changes to the Terms and Conditions, and any other issues related to the network or the parties’ participation therein.</td>
</tr>
<tr>
<td>The Management Committee shall meet [describe intervals, e.g., monthly] to consider and resolve various issues pertaining to the use of the System and the Services by Participants, including [list].</td>
<td></td>
</tr>
<tr>
<td><strong>11.6.3 Management Committee Bylaws.</strong></td>
<td>Bylaws customarily would provide procedures and rules concerning how the Management Committee would hold its meetings and take action.</td>
</tr>
<tr>
<td>The Management Committee shall adopt bylaws for the conduct of its meetings and other proceedings.</td>
<td></td>
</tr>
<tr>
<td>Model Terms and Condition</td>
<td>Notes</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------</td>
</tr>
<tr>
<td><strong>12. Fees and Charges.</strong>  Terms regarding amounts that the Participant will be required to pay to the SNO in order to use the Services.</td>
<td>It is anticipated that SNOs will adopt a variety of approaches to requiring that Participants pay to use the System and the Services. The following compensation terms are for illustration only, and describe an approach intended to give the SNO flexibility in determining its fee policies.</td>
</tr>
<tr>
<td><strong>12.1 Agreed-Upon Fees.</strong> Provision for a Participant’s written agreement to take precedence over the SNO Terms and Conditions.</td>
<td></td>
</tr>
<tr>
<td>If the Participant has entered into a written Registration Agreement with [SNO Name] pursuant to Section 4.2 (Registration by Agreement), the terms and conditions of that Registration Agreement with respect to the payment of fees and charges shall apply.</td>
<td></td>
</tr>
<tr>
<td><strong>12.2 Service Fees.</strong> <strong>Alternative One:</strong> SNO’s fee schedule is not a part of the SNO Terms and Conditions. Unless the Participant’s Registration Agreement provides otherwise, each Participant shall pay to [SNO Name] [SNO Name]’s Service Fees, in accordance with [SNO Name]’s then-current Fee Schedule, for those Services for which the Participant has registered.</td>
<td>A SNO’s Fee Schedule may include a variety of fee levels, permitting the SNO to charge greater and lesser amounts to Participants, depending upon the extent to which each elects to receive Services and/or hardware and software. In addition, the Fee Schedule should address the extent, if any, to which Data Providers are to pay.</td>
</tr>
<tr>
<td><strong>OR</strong> <strong>Alternative Two:</strong> SNO’s fee schedule is a part of the SNO Terms and Conditions. Unless the Participant’s Registration Agreement provides otherwise, each Participant shall pay to [SNO Name] [SNO Name]’s Service Fees, in accordance with the Fee Schedule attached as Schedule 12.2 (Service Fees), for those Services for which the Participant has registered.</td>
<td></td>
</tr>
<tr>
<td><strong>12.3 Changes to Fee Schedule.</strong> Provision allowing the SNO to change its Fee Schedule. <strong>Alternative One:</strong> SNO may change its fee schedule at will. [SNO Name] may change its Fee Schedule at any time upon thirty (30) days prior written notice to Participants. <strong>OR</strong> <strong>Alternative Two:</strong> SNO may change its fee schedule once per year after a required period of notice. [SNO Name] may change its Fee Schedule as of January 1 of any calendar year, provided, that [SNO Name] shall give Participants not less than thirty (30) days prior written notice of any such change.</td>
<td>Such changes to the SNO’s Fee Schedule would not apply to Participants that have written agreements that address fees (see Section 12.1 (Agreed-Upon Fees)).</td>
</tr>
</tbody>
</table>
### 12.4 Miscellaneous Charges.

Unless the Participant’s Registration Agreement provides otherwise, the Participant also shall pay [SNO Name]’s charges for all goods or services that [SNO Name] provides at the Participant’s request that are not specified in [SNO Name]’s then-current Fee Schedule (“Miscellaneous Charges”).

A SNO may wish to make provision for situations in which the SNO provides additional services at a Participant’s request and wishes to obligate the Participant to pay for those additional services.

### 12.5 Payment.

The Participant shall pay all Service Fees and any Miscellaneous Charges within thirty (30) days following the date of invoice by [SNO Name] sent to the Participant’s address as shown in [SNO Name]’s records or e-mailed in accordance with the Participant’s Registration Agreement.

The Model assumes that the SNO will wish to have strict terms regarding payment by Participants. A SNO may wish to adopt measures that are either more or less strict than shown here.

### 12.6 Late Charges.

*Provision calling for late charges on delinquent Service Fees and Miscellaneous Charges.*

Service Fees and Miscellaneous Charges not paid to [SNO Name] within ___________ (__) business days following the due date therefor are subject to a late charge of five percent (5%) of the amount owing and interest thereafter at the rate of one and one-half percent (1½ %) per month on the outstanding balance, or the highest amount permitted by law, whichever is lower.

The Model assumes that the SNO will wish to have strict terms regarding payment by Participants. A SNO may wish to adopt measures that are either more or less strict than shown here.

### 12.7 Suspension of Service.

*Provision permitting the SNO to suspend services until the Participant pays amounts that are due.*

Failure to pay Service Fees and Miscellaneous Charges within ___________ (__) days following the due date therefor may result in termination of the Participant’s access to the System and/or use of the Services on ___________ (__) days prior notice. A reconnection fee equal to ________________ shall be assessed to re-establish connection after termination due to non-payment.

The Model assumes that the SNO will wish to have strict terms regarding payment by Participants. A SNO may wish to adopt measures that are either more or less strict than shown here.

### 12.8 Taxes.

All Service Fees and Miscellaneous Charges shall be exclusive of all federal, state, municipal, or other government excise, sales, use, occupational, or like taxes now in force or enacted in the future, and the Participant shall pay any tax (excluding taxes on [SNO Name]’s net income) that [SNO Name] may be required to collect or pay now or at any time in the future and that are imposed upon the sale or delivery of items and services provided pursuant to the Terms and Conditions.
<table>
<thead>
<tr>
<th>Model Terms and Condition</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>12.9 Other Charges and Expenses.</strong></td>
<td>The Participant shall be solely responsible for any other charges or expenses the Participant may incur to access the System and use the Services, including without limitation, telephone and equipment charges, and fees charged by third-party vendors of products and services.</td>
</tr>
</tbody>
</table>
### 13. Proprietary Information.

Provisions concerning the parties’ respective obligations to preserve the confidentiality of others’ proprietary information (i.e., other than health information).

#### 13.1 Scope of Proprietary Information.

In the performance of their respective responsibilities pursuant to the Terms and Conditions, [SNO Name] and Participants may come into possession of certain Proprietary Information of the other. For the purposes hereof, “Proprietary Information” means all trade secrets, business plans, marketing plans, know-how, data, contracts, documents, scientific and medical concepts, member and customer lists, costs, financial information, profits and billings, and referral sources, existing or future services, products, operations, management, pricing, financial status, goals, strategies, objectives, and agreements of the Shareholder and the Corporation, whether written or verbal, that are confidential in nature; provided, however, that Proprietary Information shall not include any information that:

- (a) is in the public domain;
- (b) is already known or obtained by any other party other than in the course of the other party's performance pursuant to the Terms and Conditions;
- (c) is independently developed by any other party;
- and/or
- (d) becomes known from an independent source having the right to disclose such information and without similar restrictions as to disclosure and use and without breach of the Terms and Conditions, or any other confidentiality or nondisclosure agreement by such other party.

#### 13.2 Nondisclosure of Proprietary Information.

[SNO Name] and the Participant each (i) shall keep and maintain in strict confidence all Proprietary Information received from the other, or from any of the other’s employees, accountants, attorneys, consultants, or other agents and representatives, in connection with the performance of their respective obligations under the Terms and Conditions; (ii) shall not use, reproduce, distribute or disclose any such Proprietary Information except as permitted by the Terms and Conditions; and (iii) shall prevent its employees, accountants, attorneys, consultants, and other agents and representatives from making any such use, reproduction, distribution, or disclosure.
### 13.3 Equitable Remedies.

All Proprietary Information represents a unique intellectual product of the party disclosing such Proprietary Information (the “Disclosing Party”). The unauthorized disclosure of said Proprietary Information would have a detrimental impact on the Disclosing Party. The damages resulting from said detrimental impact would be difficult to ascertain but would result in irreparable loss. It would require a multiplicity of actions at law and in equity in order to seek redress against the receiving party in the event of such an unauthorized disclosure. The Disclosing Party shall be entitled to equitable relief in preventing a breach of this Section 13 (Proprietary Information) and such equitable relief is in addition to any other rights or remedies available to the Disclosing Party.

### 13.4 Notice of Disclosure.

Notwithstanding any other provision hereof, nothing in this Section 13 (Proprietary Information) shall prohibit or be deemed to prohibit a party hereto from disclosing any Proprietary Information (or any other information the disclosure of which is otherwise prohibited hereunder) to the extent that such party becomes legally compelled to make such disclosure by reason of a subpoena or order of a court, administrative agency or other governmental body of competent jurisdiction, and such disclosures are expressly permitted hereunder; provided, however, that a party that has been requested or becomes legally compelled to make a disclosure otherwise prohibited hereunder by reason of a subpoena or order of a court, administrative agency or other governmental body of competent jurisdiction shall provide the other party with notice thereof within five (5) calendar days, or, if sooner, at least three (3) business days before such disclosure will be made so that the other party may seek a protective order or other appropriate remedy. In no event shall a party be deemed to be liable hereunder for compliance with any such subpoena or order of any court, administrative agency or other governmental body of competent jurisdiction.
# Model Terms and Conditions

<table>
<thead>
<tr>
<th>Notes</th>
</tr>
</thead>
</table>
| **14. Disclaimers, Exclusions of Warranties, Limitations of Liability, and Indemnifications.**  
Standard terms directed to avoiding inappropriate legal claims between the parties. The specific language shown in this section is for illustration only. The SNO would need to tailor the language of this section to comply with applicable state laws regarding the content and presentation (e.g., capital letters) of disclaimers and limitations of warranties and similar issues. |

### 14.1 Carrier Lines.

By using the System and the Services, each Participant shall acknowledge that access to the System is to be provided over various facilities and communications lines, and information will be transmitted over local exchange and Internet backbone carrier lines and through routers, switches, and other devices (collectively, “carrier lines”) owned, maintained, and serviced by third-party carriers, utilities, and Internet service providers, all of which are beyond [SNO name]’s control. [SNO Name] assumes no liability for or relating to the integrity, privacy, security, confidentiality, or use of any information while it is transmitted on the carrier lines, or any delay, failure, interruption, interception, loss, transmission, or corruption of any data or other information attributable to transmission on the carrier lines. Use of the carrier lines is solely at user’s risk and is subject to all applicable local, state, national, and international laws.

### 14.2 No Warranties.

Access to the System, use of the Services, and the information obtained by a Data Recipient pursuant to the use of those services are provided “as is” and “as available” without any warranty of any kind, expressed or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. The Participant is solely responsible for any and all acts or omissions taken or made in reliance on the System or the information in the System, including inaccurate or incomplete information. It is expressly agreed that in no event shall [SNO Name] be liable for any special, indirect, consequential, or exemplary damages, including but not limited to, loss of profits or revenues, loss of use, or loss of information or data, whether a claim for any such liability or damages is premised upon breach of contract, breach of warranty, negligence, strict liability, or any other theories of liability, even if [SNO Name] has been apprised of the possibility or likelihood of such damages occurring. [SNO Name] disclaims any and all liability for erroneous transmissions and loss of service resulting from communication failures by telecommunication service providers or the System.

The Model assumes that the SNO will wish to limit its potential liability arising out of the use of data through the System. A SNO may wish to assume a greater degree of potential responsibility.
**Model Terms and Conditions**

### 14.3 Other Participants.

By using the System and the Services, each Participant shall acknowledge that other Participants have access to the System and Services, and that other parties have access to the information contained in the System through their participation in the NHIN. Such other Participants have agreed to comply with the Common Framework Policies and Procedures, concerning use of the information made available through the NHIN; however, the actions of such other parties are beyond the control of [SNO Name]. Accordingly, [SNO Name] does not assume any liability for or relating to any impairment of the privacy, security, confidentiality, integrity, availability, or restricted use of any information on the System resulting from any Participant’s actions or failures to act.

The Model assumes that the contracting parties will wish to limit the SNO’s potential liability arising out of the use of data through the System. Participants and SNOs may of course choose a system whereby the SNO assumes a greater degree of potential responsibility.

### 14.4 Participant’s Actions.

The Participant shall be solely responsible for any damage to a computer system, loss of data, and any damage to the System caused by that Participant or any person using a user ID assigned to the Participant or a member of the Participant’s workforce.

### 14.5 Unauthorized Access; Lost or Corrupt Data.

[SNO Name] is not responsible for unauthorized access to the Participant’s transmission facilities or equipment by individuals or entities using the System or for unauthorized access to, or alteration, theft, or destruction of the participant’s data files, programs, procedures, or information through the System, whether by accident, fraudulent means or devices, or any other method. The Participant is solely responsible for validating the accuracy of all output and reports and protecting the Participant’s data and programs from loss by implementing appropriate security measures, including routine backup procedures. The Participant waives any damages occasioned by lost or corrupt data, incorrect reports, or incorrect data files resulting from programming error, operator error, equipment or software malfunction, security violations, or the use of third-party software. [SNO Name] is not responsible for the content of any information transmitted or received through [SNO name]’s provision of the Services.
### 14.6 Inaccurate Data.

All data to which access is made through the System and/or the Services originates from Data Providers and other parties making data available through the NHIN, and not from [SNO Name]. All such data is subject to change arising from numerous factors, including without limitation, changes to patient health information made at the request of the patient, changes in the patient’s health condition, the passage of time and other factors. [SNO Name] neither initiates the transmission of any data nor monitors the specific content of data being transmitted. Without limiting any other provision of the Terms and Conditions, [SNO Name] shall have no responsibility for or liability related to the accuracy, content, currency, completeness, content, or delivery of any data either provided by a Data Provider, or used by a Data Recipient, pursuant to the Terms and Conditions.

### 14.7 Patient Care.

Without limiting any other provision of the Terms and Conditions, the Participant and the Participant’s Authorized Users shall be solely responsible for all decisions and actions taken or not taken involving patient care, utilization management, and quality management for their respective patients and clients resulting from or in any way related to the use of the System or the Services or the data made available thereby. No Participant or Authorized User shall have any recourse against, and through the Registration Agreements that apply thereto, each shall waive, any claims against [SNO Name] for any loss, damage, claim, or cost relating to or resulting from its own use or misuse of the System and/or the Services or the data made available thereby.

### 14.8 Limitation of Liability.

Notwithstanding anything in the Terms and Conditions to the contrary, to the maximum extent permitted by applicable laws, the aggregate liability of [SNO Name], and [SNO Name]’s officers, directors, employees, and other agents, under any Participant’s Registration Agreement, regardless of theory of liability, shall be limited to the aggregate fees actually paid by the Participant in accordance with the Terms and Conditions for the six- (6) month period preceding the event first giving rise to the claim.

The SNO may wish to limit its exposure to damage claims that could be brought by Participants.
<table>
<thead>
<tr>
<th>Model Terms and Conditions</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>15. Insurance and Indemnification.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>15.1 Insurance.</strong> Requirements that Participants have appropriate insurance coverage.</td>
<td>The Model assumes that the Common Framework Policies and Procedures will address insurance requirements for Participants (such as general liability and professional liability insurance). The SNO may adopt additional insurance requirements that are not inconsistent with the Common Framework Policies and Procedures.</td>
</tr>
<tr>
<td>The Participant shall obtain and maintain insurance coverage in accordance with the Common Framework Policies and Procedures, which is incorporated herein by reference. [Optional: Without limiting the generality of the foregoing, the Participant shall also comply with the insurance requirements described below:]</td>
<td></td>
</tr>
<tr>
<td><strong>15.1.1 [Additional Insurance Requirements, if desired].</strong></td>
<td></td>
</tr>
<tr>
<td><strong>15.2 Indemnification</strong></td>
<td></td>
</tr>
</tbody>
</table>
### Model Terms and Conditions

#### 15.2.1. Generally.

**Alternative One: Provisions requiring the parties to indemnify each other for losses caused by claims by third parties.**

[SNO Name] and each Participant (each, an "Indemnifying Party") each shall hold the other (the "Indemnified Party") free of and harmless from all liability, judgments, costs, damages, claims, or demands, including reasonable attorneys' fees, net of the proceeds of insurance, arising out of the act or omission of the Indemnifying Party or any of the Indemnifying Party's Authorized Users, members, agents, staff, or employees, including the Indemnifying Party's failure to comply with or perform its obligations under the applicable Registration Agreement.

**OR**

**Alternative Two: Provisions requiring the parties to indemnify each other as well as requiring Participants to indemnify each other:**

[SNO Name] and each Participant (each, an "Indemnifying Party") each shall hold the other and, if the Participant is the Indemnifying Party, the other Participants (the "Indemnified Party") free of and harmless from all liability, judgments, costs, damages, claims, or demands, including reasonable attorneys' fees, net of the proceeds of insurance, arising out of the act or omission of the Indemnifying Party or any of the Indemnifying Party's Authorized Users, members, agents, staff, or employees, including the Indemnifying Party's failure to comply with or perform its obligations under the applicable Registration Agreement.

**OR**

**Alternative Three: Making no special provision for indemnification, but allowing the parties' existing legal obligations to remain in effect.**

Nothing in the Terms and Conditions or any Registration Agreement shall limit [SNO Name]'s or a Participant's respective legal and equitable obligations to each other and to other Participants arising out of the doctrines of equitable indemnity, comparative negligence, contribution or other common law bases of liability.
### Model Terms and Conditions

<table>
<thead>
<tr>
<th><strong>15.2.2 Specific Indemnities.</strong></th>
<th><strong>Notes</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Provisions calling for special indemnification terms.</strong></td>
<td>The SNO may choose to adopt special rules governing indemnification for particular situations, such as a breach of confidentiality of protected health information, or a Data Provider’s provision of inaccurate data. The provisions shown here are provided as examples.</td>
</tr>
</tbody>
</table>

**Alternative One: SNO and Participant indemnify each other for Serious Breaches of Confidentiality or Security for which they are responsible.**

Notwithstanding Section 15.2.1 (Generally), [SNO Name] and each Participant (each, an “Indemnifying Party”) each shall hold the other (the “Indemnified Party”) free of and harmless from all liability, judgments, costs, damages, claims, or demands, including reasonable attorneys’ fees, net of the proceeds of insurance, arising out of any Serious Breach of Confidentiality or Security arising out of the act or omission of the Indemnifying Party or any of the Indemnifying Party’s Authorized Users, members, agents, staff, or employees.

**AND/OR**

**Alternative Two: Data Provider indemnifies SNO for losses caused by the Data Provider’s provision of inaccurate data.**

Notwithstanding Section 15.2.1 (Generally), a Data Provider shall hold [SNO Name] free of and harmless from all liability, judgments, costs, damages, claims, or demands, including reasonable attorneys’ fees, net of the proceeds of insurance, arising out of Data Provider’s provision of any Patient Data that is inaccurate, incomplete, or defamatory.
### Model Terms and Conditions

#### 15.2.3 Rules for Indemnification.

Provisions governing the parties’ indemnification obligations.

Any indemnification made pursuant to the Terms and Conditions shall include payment of all costs associated with defending the claim or cause of action involved, whether or not such claims or causes of action are meritorious, including reasonable attorneys’ fees and any settlement by or judgment against the party to be indemnified. In the event that a lawsuit is brought against the party to be indemnified, the party responsible to indemnify that party shall, at its sole cost and expense, defend the party to be indemnified, if the party to be indemnified demands indemnification by written notice given to the indemnifying party within a period of time wherein the indemnifying party is not prejudiced by lack of notice. Upon receipt of such notice, the indemnifying party shall have control of such litigation but may not settle such litigation without the express consent of the party to be indemnified, which consent shall not be unreasonably withheld, conditioned or delayed. The indemnification obligations of the parties shall not, as to third parties, be a waiver of any defense or immunity otherwise available, and the indemnifying party, in indemnifying the indemnified party, shall be entitled to assert in any action every defense or immunity that the indemnified party could assert on its own behalf.

### Notes

Provisions governing indemnification and related matters should be tailored to the specific wishes and requirements of the SNO, and to comply with applicable state laws. The language provided is for illustration only.

*Miscellaneous provisions that apply to the SNO Terms and Conditions.*

#### 16.1 Applicable Law.

The interpretation of the Terms and Conditions and the resolution of any disputes arising under the Terms and Conditions and Participants’ Registration Agreements shall be governed by the laws of the State of ___________. If any action or other proceeding is brought on or in connection with the Terms and Conditions or a Registration Agreement, the venue of such action shall be exclusively in ____________ County, in the State of _____________.

The Model does not propose a specific alternate dispute resolution mechanism, e.g. arbitration and/or mediation, but individual SNOs may wish to consider including such a mechanism.

#### 16.2 Non-Assignability.

No rights of the Participant under its Registration Agreement may be assigned or transferred by the Participant, either voluntarily or by operation of law, without the prior written consent of [SNO Name], which it may withhold in its sole discretion.

#### 16.3 Third-Party Beneficiaries.

There shall be no third-party beneficiaries of any Registration Agreement.

#### 16.4 Supervening Circumstances.

Neither the Participant nor [SNO Name] shall be deemed in violation of any provision of a Registration Agreement if it is prevented from performing any of its obligations by reason of: (a) severe weather and storms; (b) earthquakes or other natural occurrences; (c) strikes or other labor unrest; (d) power failures; (e) nuclear or other civil or military emergencies; (f) acts of legislative, judicial, executive, or administrative authorities; or (g) any other circumstances that are not within its reasonable control. This Section 16.4 (Supervening Circumstances) shall not apply to obligations imposed under applicable laws and regulations or obligations to pay money.

#### 16.5 Severability.

Any provision of the Terms and Conditions or any Participant Registration Agreement that shall prove to be invalid, void, or illegal, shall in no way affect, impair, or invalidate any other provision of the Terms and Conditions or such Registration Agreement, and such other provisions shall remain in full force and effect.
## 16.6 Notices.

Any and all notices required or permitted under the Terms and Conditions shall be sent by United States mail, overnight delivery service, or facsimile transmission to the address provided by the Participant in its Registration Form or such different addresses as a party may designate in writing. If the Participant has supplied [SNO Name] with an electronic mail address, [SNO Name] may give notice by email message addressed to such address; provided that if [SNO Name] receives notice that the email message was not delivered, it shall give the notice by United States mail, overnight delivery service, or facsimile.

## 16.7 Waiver.

No provision of the Terms and Conditions or any Participant Registration Agreement shall be deemed waived and no breach excused, unless such waiver or consent shall be in writing and signed by the party claimed to have waived or consented. Any consent by any party to, or waiver of a breach by the other, whether expressed or implied, shall not constitute a consent to, waiver of, or excuse for any other different or subsequent breach.

## 16.8 Complete Understanding.

With respect to any Participant Registration Agreement made pursuant to the Terms and Conditions, that Agreement and the Terms and Conditions together contain the entire understanding of the parties, and there are no other written or oral understandings or promises between the parties with respect to the subject matter of any Registration Agreement other than those contained or referenced in that Registration Agreement. All modifications or amendments to any Registration Agreement shall be in writing and signed by all parties.
To apply to participate in [SNO Name] as a Participant, please provide the following information, and then click “Next” below.

<table>
<thead>
<tr>
<th>Type the Applicant’s Name:</th>
<th>Choose a Participant Name (must be at least 10 characters):</th>
</tr>
</thead>
</table>

**[Optional, not to be used if SNO will issue and manage passwords:]** Choose a Password (must be at least 8 characters): 

<table>
<thead>
<tr>
<th>[Optional:] Confirm Password:</th>
</tr>
</thead>
</table>

State whether the Applicant is an individual person or a partnership, corporation, or other organization (pick one from [pull down] list): 

<table>
<thead>
<tr>
<th>Individual Person</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partnership</td>
</tr>
<tr>
<td>Limited Partnership</td>
</tr>
<tr>
<td>Limited Liability Company</td>
</tr>
<tr>
<td>Corporation</td>
</tr>
<tr>
<td>Other Organization (specify):_____________</td>
</tr>
</tbody>
</table>

Provide name and telephone number of person to contact: 

Provide Applicant’s address (Number, Street, and Suite No.): 

Provide Applicant’s Participant Category (pick one from [pull down] list): 

<table>
<thead>
<tr>
<th>Health Care Provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Services Provider</td>
</tr>
<tr>
<td>Health Plan, Insurer, or Other Payer</td>
</tr>
<tr>
<td>Public Health Authority</td>
</tr>
<tr>
<td>Other Government Agency</td>
</tr>
<tr>
<td>Researcher</td>
</tr>
<tr>
<td>[Others]</td>
</tr>
</tbody>
</table>

[Other information if required]:

To proceed to [Participant] Registration Agreement, click “Next” →

SCREEN 1
[Name of SNO]
[PARTICIPANT] REGISTRATION AGREEMENT

All [Participants] must agree to the terms and conditions of [SNO Name]’s [Participant] Registration Agreement, which provides as follows:

1. **[SNO Name] Terms and Conditions.** All of the terms of the [SNO Name] Terms and Conditions are hereby incorporated by reference into this [Participant] Registration Agreement. Words in this [Participant] Registration Agreement shall have the meanings given to them by the [SNO Name] Terms and Conditions. All Applicants are required to read and agree to the [SNO Name] Terms and Conditions prior to completing this application.

The Applicant hereby represents and warrants that the Applicant, or an authorized person acting on the Applicant’s behalf, has read and agrees to comply with all [SNO Name] Terms and Conditions.

Select One: Yes/No

To proceed, click “Next” →

SCREEN 2
2. **Review of Application**

[SNO Name] will review this application for registration and may accept or reject this application in accordance with the terms and conditions set forth in Section __ of the [SNO Name] Terms and Conditions. Upon [SNO Name]'s acceptance of this application, [SNO Name] shall notify the Applicant and shall register the Applicant as a [Participant]. [Optional, if SNO is to issue passwords:] [SNO Name] shall issue each Participant a [User I.D. and] password to access and use the [SNO Name] System and the [SNO Name] Services.

3. **[Participant] Agreement**

Upon receipt of [SNO Name]'s notice that it has accepted this application, the Applicant shall be legally bound to comply with all of the terms and conditions of [SNO Name]'s Terms and Conditions that apply to [Participant] and may then commence to access and use the [SNO Name] System and [SNO Name] Services, subject to all of the terms and conditions of this Registration Agreement and the [SNO Name] Terms and Conditions.

4. **Changes to Terms and Conditions**

The [SNO Name] Terms and Conditions shall be subject to change from time to time, and all such changes shall be incorporated by reference into this [Participant] Registration Agreement upon the effective date selected by [SNO Name]. The [Participant] shall be informed of all such changes prior to their effectiveness. If the [Participant] objects to the changes, the [Participant] may terminate this Agreement and, by doing so, cease to be a [Participant], as described in the [SNO Name] Terms and Conditions.

5. **Term and Termination**

This [Participant] Registration Agreement shall continue in effect until it is terminated, in accordance with the [SNO Name] Terms and Conditions.

The Applicant hereby represents and warrants that the Applicant, or a duly authorized person acting on the Applicant's behalf, has read the [SNO Name] Terms and Conditions and this Registration Agreement and, by selecting “Yes” below, hereby applies for registration as a [Participant] and agrees to all the terms and conditions of the [SNO Name] Terms and Conditions and this Registration Agreement.

Yes ___ No ___

To proceed, click “Next” →

Next

SCREEN 3
Thank you for your application. [SNO Name] will review your application and send you a response within approximately _____ days.

To return to the [SNO Name] web site, click “Return” → Return

SCREEN 4
A Model Contract for Health Information Exchange

EXHIBIT 2

Bibliography

In preparing the Model Contract for Health Information Exchange, user agreements made available by the following organizations (in alphabetical order) were particularly helpful:


- Indiana Network for Patient Care, Indianapolis Regional Network For Primary and Emergency Care Second Participants’ Agreement, http://www.regenstrief.org/medinformatics/inpc/.


Acknowledgements
The members of the Connecting for Health Policy Subcommittee have accomplished an extraordinary task in less than a year's time—the development of an evolving piece of work that can serve as the core of nationwide health information exchange—the policy components of The Common Framework. During this time, we have been fortunate to work with respected experts in the fields of health, information technology, and privacy law, all of whom have contributed their time, energy, and expertise to a daunting enterprise. Our consultants and volunteers have worked long hours in meetings and conference calls to negotiate the intricacies of such issues as privacy, security, authentication, notification, and consent in health information exchange. We offer them our heartfelt thanks for taking on this journey with us, and look forward to the remaining work ahead.

In addition, we would like to offer special thanks to the volunteers and consultants who authored the initial drafts of this body of work—their hard work created a strong foundation upon which to focus the Subcommittee's deliberations: Stefaan Verhulst, Clay Shirky, Peter Swire, Gerry Hinkley, Allen Briskin, Marcy Wilder, William Braithwaite, and Janlori Goldman.

Finally, we must note that none of this work would have been possible without the leadership and inspiration of our co-chairs, William Braithwaite and Mark Frisse. They have led us with steady hands and determination of spirit.

Connecting for Health Policy Subcommittee

William Braithwaite, MD, eHealth Initiative, (Co-Chair)

Seth Foldy, MD, City of Milwaukee Health Department

Mark Frisse, MD, MBA, MSc, Vanderbilt Center for Better Health, (Co-Chair)

Janlori Goldman, JD, Columbia College of Physicians and Surgeons

Laura Adams, Rhode Island Quality Institute

Ken Goodman, PhD, University of Miami

Phyllis Borzi, JD, George Washington University Medical Center

John Halamka, MD, CareGroup Healthcare System

Susan Christensen*, JD, Agency for Healthcare Research and Quality, United States Department of Health and Human Services

Joseph Heyman, MD, American Medical Association

Art Davidson, MD, MSHP, Denver Public Health

Gerry Hinkley, JD, Davis, Wright, Tremaine LLP

Mary Jo Deering*, PhD, National Cancer Institute/National Institutes of Health, United States Department of Health and Human Services

Charles Jaffe, MD, PhD, Intel Corporation

Jim Dempsey, JD, Center for Democracy and Technology

Jim Keese, Eastman Kodak Company

Hank Fanberg, Christus Health

Linda Kloss, RHIA, CAE, American Health Information Management Association

Linda Fischetti*, RN, MS, Veterans Health Administration

Gil Kuperman, MD, PhD, New York-Presbyterian Hospital

Omid Moghadam, Intel Corporation

Ned McCulloch, JD, IBM Corporation

Patrick McMahon, Microsoft Corporation
Joyce Niland, PhD, City of Hope National Medical Center

Louise Novotny, Communication Workers of America

Michele O'Connor, MPA, RHIA, MPI Services Initiate

Victoria Prescott, JD, Regenstrief Institute for Healthcare

Marc A. Rodwin, JD, PhD, Suffolk University Law School

Kristen B. Rosati, JD, Coppersmith Gordon Schermer Owens & Nelson PLC

Sara Rosenbaum, JD, George Washington University Medical Center

David A. Ross, ScD, Public Health Informatics Institute

Clay Shirky, New York University (Chair, Technical Subcommittee)

Don Simborg, MD, American Medical Informatics Association

Michael Skinner, Santa Barbara Care Data Exchange

Joel Slackman, BlueCross/BlueShield Association

Peter P. Swire, JD, Moritz College of Law, Ohio State University

Paul Tang, MD, Palo Alto Medical Foundation

Micky Tripathi, Massachusetts eHealth Collaborative

Cynthia Wark*, CAPT, United States Public Health Service Commissioned Corps, Centers for Medicare and Medicaid Services, United States Department of Health and Human Services

John C. Wiesendanger, MHS, West Virginia Medical Institute/Quality Insights of Delaware/Quality Insights of Pennsylvania

Marcy Wilder, JD, Hogan & Hartson LLP

Scott Williams, MD, MPH, HealthInsight

Robert B. Williams, MD, MIS, Deloitte

Joy Wilson, National Conference of State Legislatures

Rochelle Woolley, RxHub

Amy Zimmerman-Levitan, MPH, Rhode Island State Department of Health

*Note: Federal employees participate in the Subcommittee but make no endorsement