THE COMMON FRAMEWORK:

Overview and Principles

CONNECTING FOR HEALTH℠
MARKLE FOUNDATION A Public-Private Collaborative

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

Carol Diamond, MD, MPH, Markle Foundation, (Chair)

Daniel Garrett, Computer Sciences Corporation's Global Health Solutions Practice, (Vice Chair)

John R. Lumpkin, MD, MPH, Robert Wood Johnson Foundation, (Vice Chair)

Herbert Pardes, MD, New York-Presbyterian Hospital, (Vice Chair)

Peter A. Andersen, MD, Lockheed Martin Information Technology

Zoë Baird, Markle Foundation, (ex-officio)

Robert Bogin, MD, American Cancer Society

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

Claire Broome*, MD, Centers for Disease Control and Prevention

Gary Christopherson*, Centers For Medicare and Medicaid Services

Carolyn Clancy*, MD, Agency for Healthcare Research and Quality, United States Department of Health and Human Services

Janet Corrigan, PhD, National Committee for Quality Health Care

Mike Cummins, VHA Inc.

Francois de Brantes, Bridges To Excellence and Prometheus

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

David A. Epstein, IBM Software Group

Colin Evans, Intel Corporation

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

J. Peter Geerlofs, MD, Allscripts Healthcare Solutions

John Glaser, PhD, Partners HealthCare System

John Halamka, MD, CareGroup Healthcare System

Linda Harris*, PhD, National Cancer Institute/National Institutes of Health, United States Department of Health and Human Services

Douglas Henley, MD, American Academy of Family Physicians

Joseph Heyman, MD, American Medical Association

Yin Ho, MD, Pfizer, Inc.

Kevin Hutchinson, SureScripts

Michael Jackman, Eastman Kodak Company

William F. Jessee, MD, Medical Group Management Association

Y. Michele Kang, Northrop Grumman Corporation

Michael L. Kappel, McKesson Provider Technologies

Brian Keaton, MD, FACEP, American College of Emergency Physicians

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

Allan Korn, MD, FACP, Blue Cross/Blue Shield Association

David Lansky, PhD, Markle Foundation, (Chair, Personal Health Technology Council)

Gail Latimer, MSN, RN, Siemens Corporation

Jack Lewin, MD, California Medical Association

Stephen Lieber, CAE, Healthcare Information and Management Systems Society

Patricia MacTaggart, EDS Executive State and Local Government

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.*

The Common Framework:

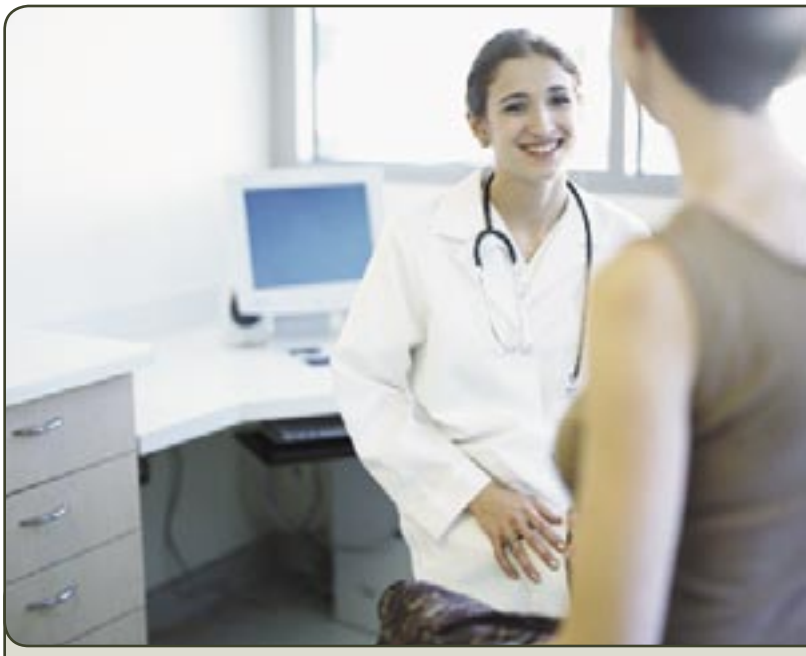
Overview and Principles*

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 complicate matters, some proposals that provide



What is Connecting for Health?

Connecting for Health is a public-private collaborative made up of leaders and innovators from more than 100 organizations representing a diverse array of private, public, and not-for-profit groups. Participants are listed at: www.connectingforhealth.org.

* **Connecting for Health** thanks Lygeia Ricciardi and David Lansky, both of the Markle Foundation, for drafting this paper.

What can the Common Framework do for those interested in health information exchange?

The Common Framework puts forth a model of health information exchange that:

- Protects patient privacy by allowing health information to remain under local control, with the doctors and hospitals patients trust, thus avoiding the need for large, centralized databases or creation of a national patient ID.
- Avoids large scale disruption and huge up front capital investments by making use of existing hardware and software. This flexibility enables innovation and the ability to customize solutions to meet local needs.
- Supports better informed decisions about key policy topics related to sharing health information.
- Establishes trust among collaborating organizations by applying well-vetted model contract language, in consultation with local advisors, to fit their needs.

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.

Connecting for Health's Policy Principles

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.

Components of the Common Framework

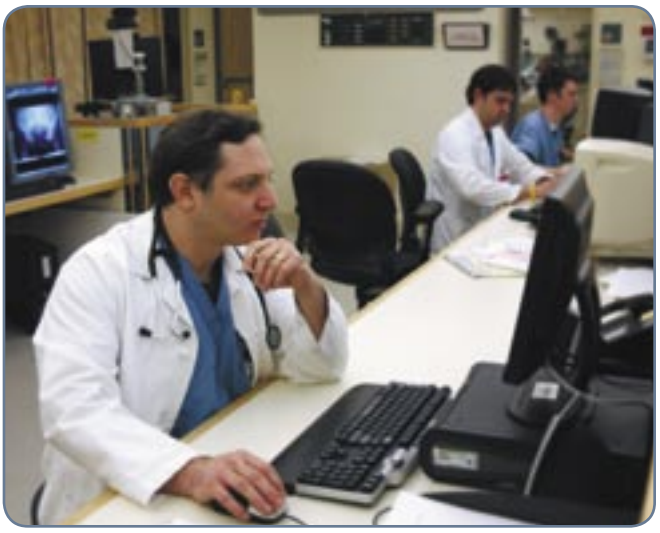
These technology and policy principles guided the specific, practical decisions about the architecture, specifications, and policies that support private and secure sharing of health information across the nation. From these, **Connecting for Health** has developed a skeletal framework of technology 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.

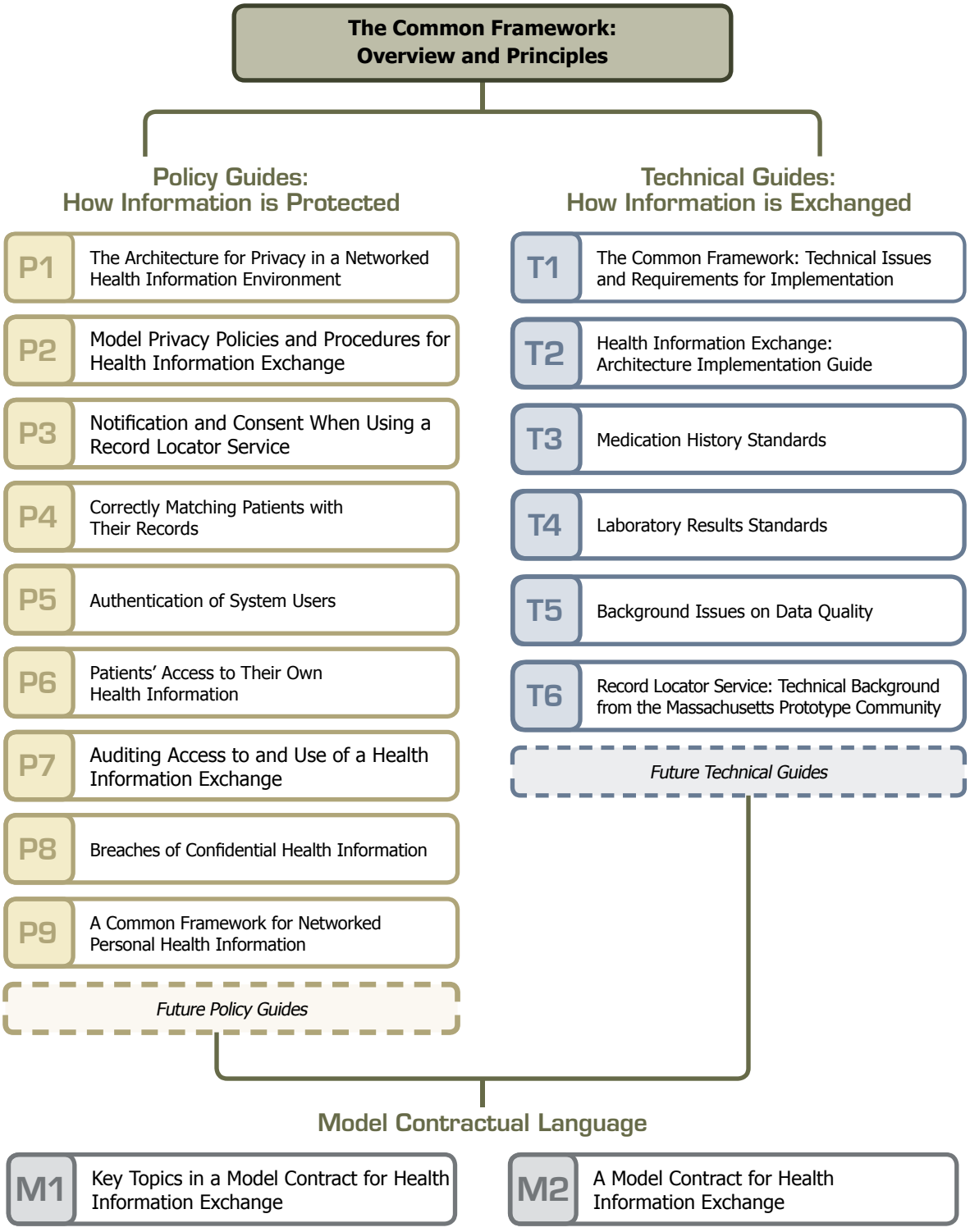
With regard to model contractual language:

- 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.

The Connecting for Health Common Framework:

Resources for Implementing Private and Secure Health Information Exchange



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.

Notification and Consent When Using a Record Locator Service—Recommended policies for what an institution or provider participating in the Record Locator Service should be required to do to inform patients and give them the ability to decide not to be listed in the index, consistent with the privacy principles articulated in "**The Connecting for Health** Architecture for Privacy in a Networked Health Information Environment."

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.

Technical Guides: How Information is Exchanged

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.

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.

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.

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.**

CONNECTING FOR HEALTH℠
MARKLE FOUNDATION
A Public-Private Collaborative

www.connectingforhealth.org