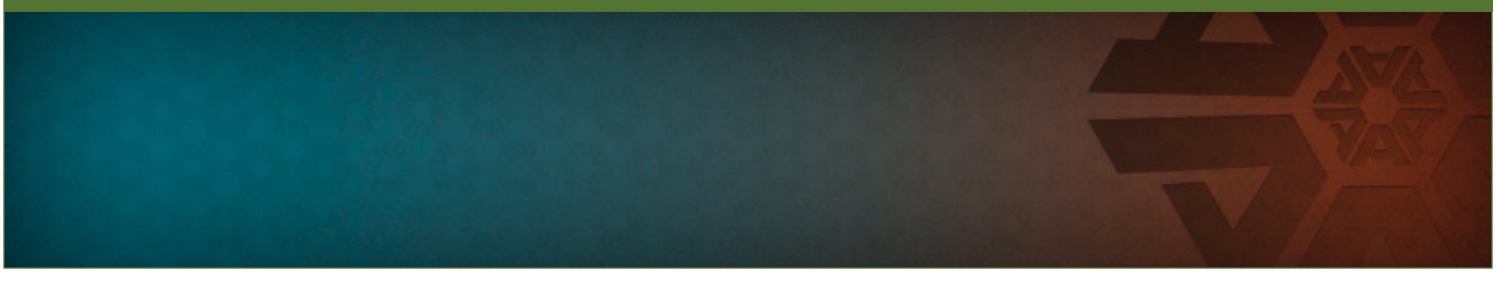
Markle Connecting for Health
Common Framework for Private and
Secure Health Information Exchange

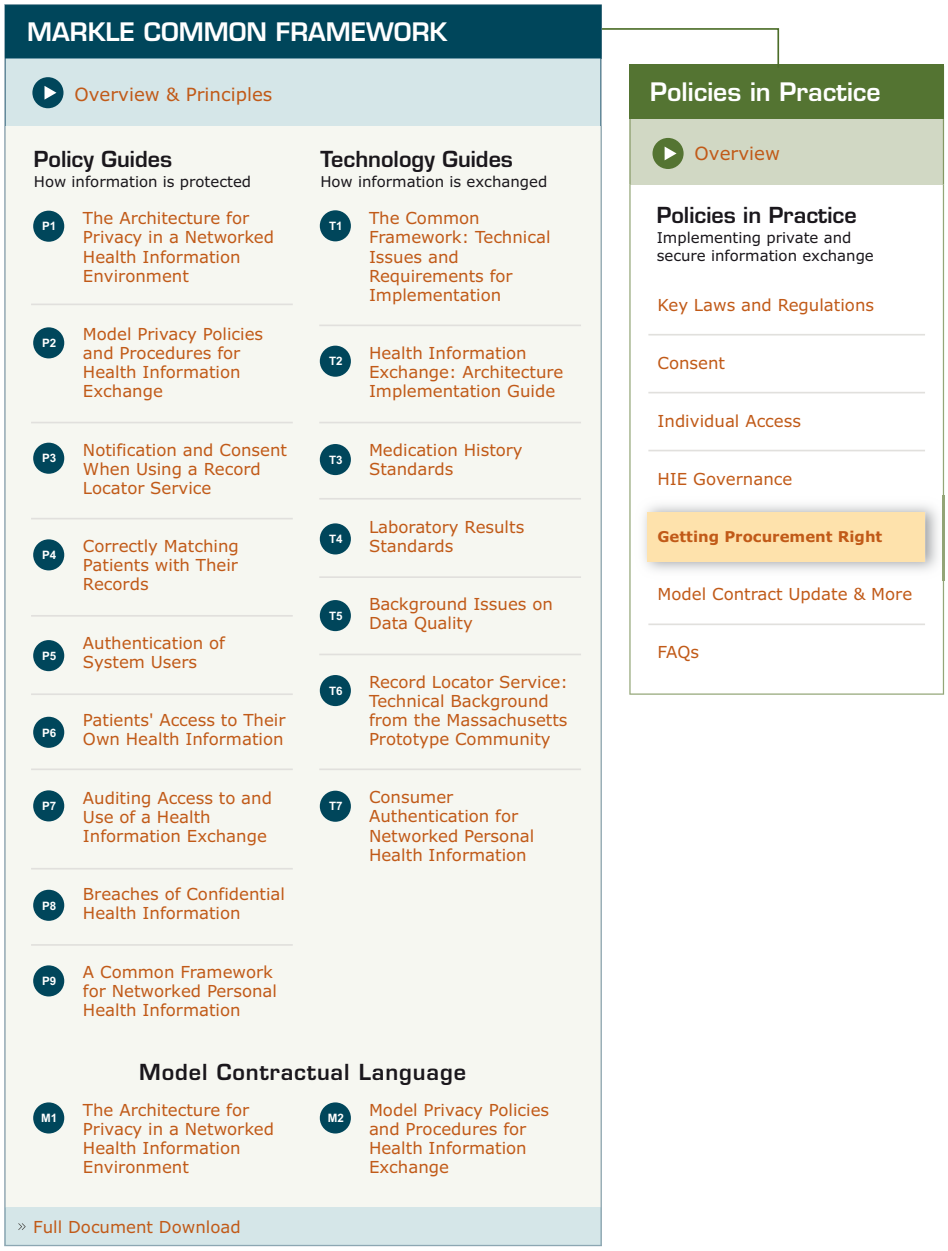
Policies in Practice

Policy-Aware Procurement Strategies and Practices: Asking the Right Questions & Reaching the Right Answers

MARKLE
CONNECTING FOR HEALTH



The document you are reading is a Markle Connecting for Health Common Framework Policies in Practice for Health Information Sharing (Policies in Practice) resource which supplements the Markle Connecting for Health Common Framework for Private and Secure Health Information Exchange (Markle Common Framework) available in its full and most current version at www.markle.org/health/markle-common-framework/connecting-professionals. The Markle Common Framework includes a set of foundational policy and technology guides published in 2006. In April 2012, a set of Policies in Practice was published to further specify these foundational documents and address a range of critical health information sharing implementation needs identified by experts working in the field.



POLICIES IN PRACTICE

Policy-Aware Procurement Strategies and Practices: Asking the Right Questions & Reaching the Right Answers

Executive Summary

Based on Fair Information Practice Principles (FIPPs), the principles, policies, and technology practices of the Markle Connecting for Health Common Framework for Private and Secure Health Information Exchange (Markle Common Framework) were developed by a diverse group of health care leaders to lay a blueprint for an integrated and comprehensive framework of trust. The Markle Common Framework relies on policy and technology decisions to work together to support this framework of trust. **Policy** provides the rules of the road for information-sharing, while **technology** enables information sharing in accordance with policy as well as provides tools to enforce policy.

Policy and technology are inextricably linked. However, in practice, when implementing health information sharing efforts,[1] often decisions related to procurement of health information products and/or services ("Technology") are made independently. In this non-integrated approach, there are risks that the Technology purchased will not be able to support the desired policies, or, if technology is purchased prior to, or in the absence of, addressing key policy decisions, there is the potential for technology capabilities to create de facto policy.

By addressing policy objectives before and during the procurement process, health information sharing efforts can avoid these unintended discrepancies between policy objectives and technical capabilities, and work to procure and implement systems that promote trust among health information sharing participants. This Policies in Practice describes how health information sharing efforts can use their privacy and security policies and procedures to guide their dialogue with prospective technology developers toward the procurement and implementation of health information products and/or services that support policy objectives.

---

[1] The Policies in Practice apply the term "health information sharing effort" broadly to refer to any initiative that supports the electronic exchange of health information between data holders. Similar terminology includes "health information exchange (HIE)", "regional health information organization (RHIO)", and "sub-network organization (SNO)".

Markle Connecting for Health thanks Allen Briskin, Pillsbury Winthrop Shaw Pittman for drafting this paper. We also thank members of the Markle Connecting for Health Health Information Exchange Advisory Committee *for their contribution in developing this paper.*

This Policies in Practice provides a:

1. Description of key policy decisions, organized by the Markle Connecting for Health FIPPs-based privacy principles, and a sample framework for guiding these decisions to be made prior to procurement of specific Technology;

2. Recommended approach for having the health information sharing effort's policies reflected in its description to prospective vendors of the technical requirements for the Technology;

3. Recommended approach by which the health information sharing effort can assure that prospective developers' or vendors' proposals respond to the health information sharing effort's policy-driven specifications and other requirements; and

4. Glossary of important Privacy and Security terms used in Technology procurement, in order to assist procuring organizations and prospective vendors to communicate effectively regarding the organizations' Technology needs.

This Policies in Practice outlines the following key recommendations:

1. Include individuals with specialized expertise in information technology as well as privacy/security matters in the development of Privacy and Security Policies and decision making about technology procurement. "Policy" and "technology" discussions should occur concurrently rather than in isolation.

2. Provide each prospective technology developer or vendor with a copy of the Privacy Policies or provide context as necessary. In most circumstances, this is the most effective means of describing the health information sharing effort's policy requirements to inform the procurement process.

3. Develop use cases that will allow prospective technology developers or vendors to present demonstrations of their Technology in specific situations to satisfy policy objectives.

4. Support openness and transparency and create a sense of shared goals between those acquiring and those supplying Technology by developing and sharing written criteria to evaluate such products and/or services.

5. Assure compliance with policy goals by requiring each prospective vendor or developer to describe how the proposed Technology can address the requirements now as well as maintain flexibility to evolve with changing policy and maintain compatibility in exchanging information with other systems.

6. Ask the prospective vendor or developer to provide its own privacy and security policies for review and analysis to determine whether those policies are consistent with the health information sharing effort's Privacy Policies and request any necessary changes to satisfy the health information sharing effort's requirements.

I. Introduction

This Policies in Practice describes how health information sharing efforts can use their privacy and security policies and procedures ("Privacy Policies") to guide their dialogue with prospective technology developers toward the procurement and implementation of health information products and/or services ("Technology") that accomplish those Privacy Policies' objectives. As envisioned by the Markle Common Framework, health information sharing efforts offer their health information sharing participants two sets of tools: policies and practices for health information sharing, and certain technological tools to facilitate that sharing. To be effective, the Technology must work in accordance with the health information sharing effort's Privacy Policies.

This resource can assist health information sharing efforts to identify and act upon the policy decisions that should be made prior to the procurement of Technology, and to describe practices that will help ensure that prospective vendors and those who are involved in implementation understand these policy decisions, and that the Technology must have the capabilities to support them. By addressing policy objectives before and during the procurement process, health information sharing efforts can avoid unintended discrepancies between policy objectives and technical capabilities, and procure and implement systems that promote trust among health information sharing participants.

The Markle Common Framework, including its Privacy and Technology Guides, are applicable to a wide variety of health information sharing efforts. Users of this Policies in Practice should also consult appropriate resources that address applicable federal, state or other procurement requirements, as well as state and other applicable privacy laws and regulations, plus other guidance that they determine to be appropriate.

Health information sharing efforts should expect that their Privacy Policies will need to evolve over time. Privacy Policies, and health information sharing efforts' policy development processes, will be required to address changes and other developments in the laws that regulate health information privacy and sharing, and in the overarching legal environment in which health information sharing occurs. In addition, evolving experience and expectations among health information sharing efforts, health information sharing participants, and the individuals and communities they serve will also require that health information sharing efforts' Privacy Policies continue to evolve. Therefore, a policy-aware arrangement with a health information technology (health IT) developer must include mechanisms to identify and accommodate the policy and technological changes that will be required over time.

This Policies in Practice provides a:

1. Description of key policy decisions;
2. Sample framework for making those decisions;
3. Recommended approach for having the health information sharing effort's policies reflected in its description to prospective vendors of its technical requirements for the Technology; and

4. Recommended approach by which the health information sharing effort can assure that prospective developers' or vendors' proposals respond to the health information sharing effort's policy-driven specifications and other requirements.

These elements are supplemented by a recommended Glossary of important terms used in health IT procurement, to assist procuring organizations and prospective vendors on how to communicate effectively regarding the organizations' needs for Technology, and how the prospective vendors' products and services will satisfy those needs. This Glossary incorporates a number of defined terms included in the Markle Common Framework for Private and Secure Health Information Exchange's Model Contract for Health Information Exchange, such as referring to the health information sharing effort as a "sub-network organization" or "SNO."

II. Assuring Support for and Compliance with Privacy Policies

This Policies in Practice seeks to assist a health information sharing effort obtain technological support for and compliance with its Privacy Policies through Technology implementations that are most often conducted by health IT developers and vendors, simultaneously providing a framework for reasonably protecting Patient Data from inappropriate uses and/or disclosures, and permitting the use of that Patient Data in ways that are both productive and meaningful.

In developing its Privacy Policies, specifications for Technology, and other materials for the procurement process, as well as in reviewing prospective responses, the health information sharing effort may wish to involve individuals with specialized expertise in IT and/or privacy and security matters. Involving subject matter experts early and throughout the policy development and procurement process can be helpful. However, to avoid actual or apparent conflicts of interest, the health information sharing effort should consider managing the participation in a manner which may involve excluding prospective technology developers or vendors from some part or all of the process or otherwise.

In order to give prospective technology developers or vendors the opportunity to provide the relevant support, the health information sharing effort must describe its privacy and security requirements in detail. Early in the procurement process, the health information sharing effort should provide copies of its Privacy Policies, as well as the use cases and other materials described below, or make other access to those materials available. The health information sharing effort should also consider whether it wishes to provide specific objectives and measures to address some or all of the capabilities that they have determined need to be provided in the Technology.

In most circumstances, the most effective means of describing the health information sharing effort's requirements would be to provide each prospective technology developer or vendor with a copy of the Privacy Policies, together with any other appropriate documentation that explains the Privacy Policies or otherwise provides necessary context or describes any technical specifications.

The health information sharing effort may wish to consider supplementing its Privacy Policies by developing use cases that will allow prospective technology developers or vendors to present demonstrations of their Technology in specific situations, and involving specific parties, that demonstrate how they will comply with and accomplish the objectives of the health information sharing effort's Privacy Policies. Such use cases should illustrate both the experience of the typical Authorized User of the Technology, and the experience of Authorized Users with oversight responsibilities.

It is best to develop the written criteria by which it will evaluate prospective responses and/or demonstrations. Doing so can promote an atmosphere of openness and transparency to the procurement process and create a sense of shared goals that will facilitate effective relationships.

The following pages raise a number of issues regarding how the prospective Technology will assure that the health information sharing effort's System is compliant with the principles upon which its Privacy Policies are based. The health information sharing effort should explain that each of these issues will require a response from the Technology that will implement the Privacy Policies. The health information sharing effort should require that each response describe in addition the nature and extent of the Technology's flexibility and compatibility in exchanging information with other systems, such as those with which the Technology will be used, and any alternative technology to which the health information sharing effort will wish to affect a transition at a later time.

Prospective technology developers and vendors should be required to explain, in their own words, their understanding of the health information sharing effort's Privacy Policies, in order to demonstrate an appropriate level of understanding, and to help identify any issues for which clarification is appropriate. In addition, each should be required to explain and demonstrate how its Technology and processes work to support each factor, measure, and/or standard that the health information sharing effort has required. Prospective technology developers or vendors may be asked to provide alternative means to achieve the health information sharing effort's objectives with respect to each of these matters.

When a prospective Technology is not available for review and evaluation during the procurement process, a number of additional issues are raised. The health information sharing effort should obtain detailed commitments regarding compliance with specifications and delivery times, together with remedial measures and fee adjustments.

In addition, the health information sharing effort should review and analyze each prospective technology developer's or vendor's own privacy and security policies to determine whether those policies are consistent with the health information sharing effort's Privacy Policies, or require changes to satisfy the health information sharing effort's requirements.

Note: Capitalized terms have the meanings given to them in the attached Glossary, which includes a number of terms defined in the Model Contract for Health Information Exchange.

III. Key Privacy and Security Policies and Procedures to Guide Procurement

ISSUE	COMMENTS
1. What controls, measures and/or standards does the health information sharing effort require to assure that it achieves an appropriate degree of **openness and transparency** regarding developments, procedures, policies, technology and practices with respect to the treatment of Patient Data? Factors to consider include the ability of individuals to obtain an understanding of: • The information about them that is being collected, made available for disclosure, and actually disclosed and used (*i.e.*, Patient Data); and • How they can exercise reasonable control over their Patient Data.	The health information sharing effort will want to understand the extent to which the products and/or services facilitate (a) making specified information available to Participants and Individuals; (b) communicating that information to Participants and Individuals; and/or (c) providing a mechanism by which Participants and Individuals can communicate with the health information sharing effort regarding matters of concern. The health information sharing effort should provide copies of, or other access to, their applicable policies and procedures, to provide an understanding of the health information sharing effort's objectives regarding the promotion and maintenance of openness and transparency, and any specific means adopted by the health information sharing effort to promote and/or maintain openness and transparency, including without limitation the health information sharing effort's notice of privacy practices. It may be helpful for the health information sharing effort to provide a summary of its policy objectives regarding openness and transparency, in order to describe clearly the specific objectives they are seeking to achieve with respect to these matters. The health information sharing effort's specifications for the Technology should include any specific measures for openness and transparency described by their applicable policies and procedures, or otherwise what they determined. Specific matters to be addressed should include, without limitation, audit capabilities, and how the Technology will support transparency and accountability, (*e.g.*, the generation of alerts when certain potentially problematic events occur).

ISSUE	COMMENTS
2. What controls, measures and/or standards does the health information sharing effort wish to adopt to provide for **purpose specification and minimization** for Patient Data? Factors to consider include: • Limitations upon the use of Patient Data to the minimum amount necessary to accomplish the health information sharing effort's specified purposes; and • Measures to prevent collection of Patient Data for unauthorized purposes and its use or reuse for different or unauthorized purposes; • Measures to track adherence to standards regarding minimum necessary uses and disclosures of Patient Data; and • The extent to which the Technology meet current and emerging interoperability standards.	The health information sharing effort will want to understand how the Technology products and/or services assist in the management of purpose specification and minimization, both with respect to the collection of that information and in connection with the making of that information for disclosure and/or use through health information sharing efforts. Again, the health information sharing effort should provide copies of, and/or other access to, all applicable policies and procedures. It may be helpful to provide a summary of policy objectives and specific measures that are sought. The prospective technology developers' or vendor's privacy and security policies should be examined as well. Specific matters to be addressed should include: • Response to queries: Which information is returned in the query process? • Role-based access: How does an Authorized User's role effect what information is available based on the role? • Which information is exposed through the User Interface? • Which information is documented by each audit report for a patient query and retrieval of patient information?
3. What measures and/or standards does the health information sharing effort wish to adopt to accomplish **collection limitation** for Patient Data? Factors to consider include: • Participants' obtaining Patient Data by fair and lawful means only; • Participants' obtaining Patient Data with the knowledge and/or consent of the Patient, if and to the extent required; *(continued on next page)*	For each of these issues, the prospective Vendor should explain and demonstrate how its privacy and security policies, as implemented through the Technology, accomplish these objectives. In addition, the prospective Vendor should provide a copy of its privacy policies and procedures. Specific matters to be addressed should include: • Technology specifications to ensure that an Individual's documented desire for limiting Patient Data are communicated and that they are honored. • Requirements for role-based access.

ISSUE	COMMENTS
• Measures to inform Patients of the methods and extent of information collection and the potential uses (and abuses) of their Patient Data in an electronic networked environment; and • Measures to track adherence to standards regarding minimum necessary uses and disclosures of Patient Data.	
4. What measures and/or standards does the health information sharing effort wish to adopt to accomplish **use limitation** for Patient Data? Factors to consider include: • Controls to reasonably assure use of Patient Data by Data Recipients for the purposes upon which they based their requests for that Patient Data; • Ability to permit other uses under appropriate exceptions, e.g., law enforcement, security, etc.; • Measures to provide for the exchange of Patient Data only in compliance with each Data Provider's applicable policies and procedures; and • Measures to assure de-identification and/or anonymization of Patient Data for any other uses.	The health information sharing effort should develop specific measures based upon its privacy policies, and require the proposal to describe how its products and services achieve each of these goals.
5. What measures and/or standards does the health information sharing effort wish to adopt to provide for Patients' **individual participation and control** over their Patient Data? Factors to consider include: • Extent, if any, to which the health information sharing effort wishes to adopt policies that impose requirements in addition to those that apply under HIPAA, HITECH and other applicable laws. *(continued on next page)*	The health information sharing effort should require a demonstration of how the Technology will support implementation of patient consent decisions, as applicable, *e.g.*, prior notice, opportunity to decline, giving of specific authorization(s), etc. In addition, the Technology should support the application of each Data Provider's applicable policies for the exchange of Patient Data. Finally, the Technology should support the application of a Patient's differing consents on a Participant-by-Participant basis or with respect to the particular types of information involved.

ISSUE	COMMENTS
• Requirements regarding Patients' consent or authorization for, or imposition of restrictions upon, their inclusion in the Record Locator Service ("RLS") and/or the exchange of their Patient Data or certain categories of Patient Data; • Measures to facilitate Patients' requests for and receipt of information regarding who has their Patient Data and which Patient Data they have; • Measures to facilitate Patients' requests for access to and copies of their Patient Data; • Measures to permit Participants to withhold such access and/or copying when appropriate; • Measures to facilitate Patients' requests for accountings of disclosures and amendments to Patient Data; and • Measures to facilitate communications to Patients regarding a Participant's decision to deny access to their information or to decline to make an amendment requested by the Patient.	
6. What measures and/or standards does the health information sharing effort wish to adopt to assure **data integrity and quality**? Factors to consider include: • Measures to assure that Patient Data is accurate, complete, relevant, up-to-date and otherwise useful; • Measures to permit Patients to view their Patient Data and have it amended to assure accuracy and completeness; and • Measures to assure that queries to the RLS return results that are not over- or under-inclusive.	The health information sharing effort should require explanation and demonstration of how the Technology works to support each factor, measure, and/or standard.

ISSUE	COMMENTS
7. What **security safeguards and controls** does the health information sharing effort wish to adopt to prevent loss, corruption, unauthorized use, modification and/or disclosure of Patient Data? Factors to consider include: • Susceptibility of networked environments to cyber crime; • Design and implementation of technical and process-based measures for accomplishing identification, authentication and authorization for access to Patient Data; • Design and implementation of technical and process-based security controls, *e.g.*, identity management tools, data scrubbing, hashing, authenticating, etc.; • Availability of other tools to strengthen privacy and security; • Capabilities to apply different rules to different types of Patient Data, *e.g.*, sensitive data or other data specifically protected by law; • Capabilities to escape matching thresholds, authentication or authorization requirements, or other measures, if appropriate; and • Capabilities to audit, alert and report based on the health information sharing effort's policies.	The health information sharing effort should require explanation and demonstration of how the Technology works to support each factor, measure, and/or standard.
8. How does the health information sharing effort wish to accomplish and maintain **accountability and oversight** for compliance with privacy and security standards? Factors to consider include: • Training of Authorized Users and others; • Oversight of Participants and Authorized Users; *(continued on next page)*	The health information sharing effort should require explanation and demonstration of how the Technology works to support each factor, measure, and/or standard. In addition, the prospective technology developer or vendor should be required also to demonstrate how its own internal controls for ensuring accountability and oversight support the accomplishment of their objectives.

ISSUE	COMMENTS
• Measures to track specified incidents, e.g., incidental disclosures; • Measures to facilitate accountability, e.g., availability to Data Providers and Data Users of information regarding uses and disclosures of Patient Data and compliance with privacy and security standards, measures to support logging and audits; • Measures to enforce accountability for non-compliance; and • Measures to help improve compliance, e.g., identifying and correcting weaknesses.	
9. What measures does the health information sharing effort wish to adopt to provide **remedies** for privacy and/or security breaches or other performance problems? Factors to consider include: • Legal and financial devices; • Standards for accountability; • Standards for process and fairness; • Processes to communicate with Patients and Participants regarding compliance and corrective measures; and • Processes to mitigate harm caused by privacy and security violations.	The health information sharing effort should require explanation and demonstration of how the Technology works to support each factor, measure, and/or standard. To have a meaningful basis from which to determine when remedies are required and which remedies are appropriate to the circumstances, prospective technology developers or vendors should provide specific service level and other commitments that will be incorporated into the Agreement and against which performance can be measured.

Glossary of Terms for Privacy and Security Terms for Procurement

TERM	DEFINITION	COMMENTS
Acceptable Use Policy	*Noun*. A set of rules and guidelines, adopted by the health information sharing effort, that specify appropriate uses of computer systems, networks and/or information.	
Access Control	*Noun*. A mechanism or set of mechanisms designed to prevent the unauthorized access or use of Resources by limiting the number of parties that have access to or ability to use those Resources and/or by limiting the scope of such access or ability to use those Resources.	
Accountability	*Noun*. A mechanism or set of mechanisms that allows for the actions of an individual or other person with respect to the access or use of Resources may be traced to that individual or other person, and then reported to the health information sharing effort, Participants and/or others.	
American Recovery and Reinvestment Act of 2009 (ARRA)	*Noun*. Public Law 111-5, enacted February 17, 2009, that provides aid to states and cities, funding for transportation and infrastructure projects, expansion of the Medicaid program to cover more unemployed workers, health IT funding, and personal and business tax breaks, among other provisions designed to "stimulate" the economy.	
Anonymized	*Adjective*. In the case of information, having been subjected to a process by which it is impossible to determine the individual to whom that information pertains. *Compare:* De-identified.	

TERM	DEFINITION	COMMENTS
Application Programming Interface or API	*Noun*. An interface implemented by a software program that enables that program to interact with other software and facilitates interaction among software programs similar to the way the user interface facilitates interaction between humans and computers; an API is implemented by applications, libraries, and operating systems to determine their vocabularies and calling conventions, and is used to access their services, and may include specifications for routines, data structures, object classes, and protocols used to communicate between the consumer and the implementer of the API.	
Application Service Provider or ASP	*Noun*. An individual or other person that deploys, hosts, and manages access to software applications for multiple parties from a central facility.	
Audit Trail	*Noun*. A record that identifies the individuals who have accessed and/or used a Resource and that describes the nature and extent of that access or use.	
Authentication	*Noun*. The verification of the identity of an individual user, process, or device before allowing access to Resources.	
Certification	*Noun*. The examination of an information system to determine that the system can perform at a specified level required to support the specified results and/or meet specified standards.	
Clinical Document Architecture or CDA	*Noun*. A set of specifications for the electronic exchange of clinical documents and other health information.	

TERM	DEFINITION	COMMENTS
Computerized Provider Order Entry or CPOE	*Noun*. A program that allows the orders of a physician or other legally authorized person for diagnostic and treatment services (e.g., medications, devices and laboratory and other tests) to be entered electronically, and that provides specified services with respect thereto (e.g., comparing the order against standards for dosing, checking for allergies or interactions with other medications, and warning the prescriber about other potential problems).	
Confidentiality	*Noun*. The obligation of an individual or other person that receives information to protect that information from unauthorized uses or disclosures, in compliance with the health information sharing effort's applicable policies and procedures.	
Consent	*Noun*. The permission granted by an authorized individual for specified uses and/or disclosures of information.	
Data Provider	*Noun*. A Participant that is registered with the health information sharing effort to provide information to the health information sharing effort for use through the Services.	
Data Recipient	*Noun*. A Participant that uses the Services to obtain information.	
Data Repository	*Noun*. An electronic facility for the storage of information.	
Data Synchronization/ Data Syncing	*Noun*. A process by which the information stored on two or more computing devices are conformed to one another, by a mobile computing device or other mode.	

TERM	DEFINITION	COMMENTS
Decision Support Application	*Noun*. A program that analyzes data and presents results of that analysis to assist in medical and other clinical decision-making (*e.g.*, by providing evidence-based knowledge in the context of specific data).	
De-identified	*Adjective*. With respect to information, having been subjected to a process by which all identifiers of individuals, or of relatives, employers, or household members, described in 45 C.F.R. § 164.514(b)(2)(i) have been removed from that information, or by which that information has been rendered not individually identifiable in a manner that complies with the requirements of 45 C. F.R. § 164.514(b)(1).	
Digital Certificate	*Noun*. An electronic "certificate" expressed in the form of a number that establishes an individual's identity.	
Digital Signature	*Noun*. An electronic "certificate" expressed in the form of a number that is used by an individual to express his or her receipt, understanding, authorship or approval of a document.	
Disclosure	*Noun*. The release, transfer, provision of, access to, or divulging in any other manner of information to any individual or other person outside the person that maintains that information.	
Electronic Prescribing or ePrescribing	*Verb*. The use of electronic devices and programs by physicians and other legally authorized individuals to review drug and formulary coverage and to transmit prescriptions to a pharmacy.	
Encryption	*Noun*. The translation of data into a code that prevents the reading or understanding of that data by unauthorized individuals and other persons.	

TERM	DEFINITION	COMMENTS
Health Information for Economic and Clinical Health (HITECH) Act	*Noun*. Those portions of federal law set forth in Title XIII of Division A and Title IV of Division B of ARRA.	
Health Information Exchange or HIE	*Verb*. The electronic movement of health-related information among organizations according to nationally recognized standards, while maintaining the meaning of the information exchanged thereby.	
Health Information Sharing Effort	*Noun*. Any initiative that supports the electronic exchange of health information between data holders. *Compare:* SNO.	
Health Information Organization or HIO	*Noun*. An organization that facilitates, oversees and/or governs the exchange of health related information among organizations in accordance with specified standards.	
Individually Identifiable Health Information	*Noun*. Information, including demographic information collected from an individual, that (1) is created or received by a healthcare provider, health plan, employer or healthcare clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present or future payment for the provision of healthcare 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.	

TERM	DEFINITION	COMMENTS
Interoperability	*Noun*. The ability of systems components to exchange health information and to use the information that has been exchanged accurately, securely, and verifiably, when and where needed.	
Non-Repudiation	*Noun*. A process of confirming proof of information delivery to the sender and proof of sender identity to the recipient.	
Participant	*Noun*. A person that is a Data Provider or a Data Recipient.	
Protected Health Information or PHI	*Noun*. Individually identifiable health information in any form that has not been de-identified.	
Sub-network Organization (SNO)	*Noun*. A health information sharing effort.	

Acknowledgements

Markle Connecting for Health HIE Advisory Committee

Committee Members

Phyllis Albritton
Colorado Regional Health
Information Organization (past)

Hunt Blair*
Department of Vermont Health Access

Allen Briskin, JD
Pillsbury Winthrop Shaw Pittman, LLP

Jennifer Covich Bordenick
eHealth Initiative

Carol C. Diamond, MD, MPH
Markle Foundation

Joyce Dubow
AARP Office of Policy and Strategy

Vicki Estrin
C3 Consulting, LLC

Lorraine Fernandes
IBM Information Management

Linda Fischetti, RN, MS
United States Veterans Health Administration

Liza Fox-Wylie
Colorado Regional Health
Information Organization

Mark Frisse, MD, MBA, MSc
Vanderbilt Center for Better Health

Melissa Goldstein, JD
The George Washington University
Medical Center

Adrian Gropper, MD
HealthURL

Jim Hansen
Dossia Consortium

Joseph Heyman
OptumInsight

Gerry Hinkley, JD
Pillsbury Winthrop Shaw Pittman, LLP

Zachery Jiwa*
Louisiana Department of Health & Hospitals,
State of Louisiana

Ted Kremer
Greater Rochester Regional Health
Information Organization

Alice Leiter, JD
National Partnership for Women & Families

Patricia MacTaggart
The George Washington University School
of Public Health and Health Services

Linda Malek, JD
Moses & Singer, LLP

Janet Marchibroda
Health Information Technology Initiative,
Bipartisan Policy Center

Deven McGraw, JD, MPH, LLM
Health Privacy Project, Center for Democracy
& Technology

Amanda Heron Parsons,* MD
Primary Care Information Project,
NYC Department of Health & Mental Hygiene

Gina Bianco Perez, MPA
Advances in Management, Inc.

Carol Raphael, MPA
Visiting Nurse Service of New York

Carol Robinson*
Oregon Office of Health Policy & Research

Jan Root
Utah Health Information Network

Will Ross
Redwood Mednet

Scott Schumacher, PhD
IBM Information Management

Raymond Scott
Axolotl Corporation

Randy Sermons

David Sharp
Center for Health Information Technology,
Maryland Health Care Commission

Jenny Smith
Franciscan Missionaries of Our
Lady Health System

Paul Uhrig
Surescripts

Stefaan Verhulst
Markle Foundation

Marcy Wilder, JD
Hogan Lovells

Claudia Williams,* MS
Office of the National Coordinator
for Health Information Technology

Staff

Laura Bailyn, JD
Markle Foundation

Rebekah Rockwood, MPH
Markle Foundation

Jill Schulmann, MS
Markle Foundation

Sam Sheikh, MS
Markle Foundation

Sarah Stewart
C3 Consulting, LLC

Meredith Taylor, MPH
Markle Foundation

**Note: State and Federal employees participate in the Markle HIE Advisory Committee but make no endorsement.*

We thank the members of the Markle Connecting for Health HIE Advisory Committee for providing their time and expertise to the development of the Markle Connecting for Health Common Framework Policies in Practice for Health Information Sharing resources.

We particularly thank Vicki Estrin of C3 Consulting for managing this project, and the lead authors of these resources: Allen Briskin, JD, Pillsbury Winthrop Shaw Pittman, LLP; Alice Leiter, JD, National Partnership for Women and Families; Linda Malek, JD, Moses & Singer, LLP; Deven McGraw, JD, MPH, LLM, Center for Democracy & Technology; and Stefaan Verhulst, Markle Foundation.