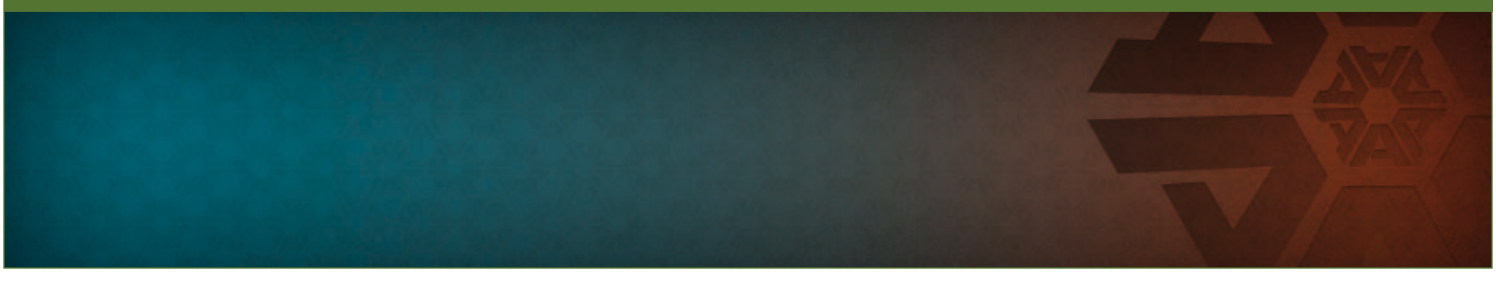
Markle Connecting for Health
Common Framework for Private and
Secure Health Information Exchange

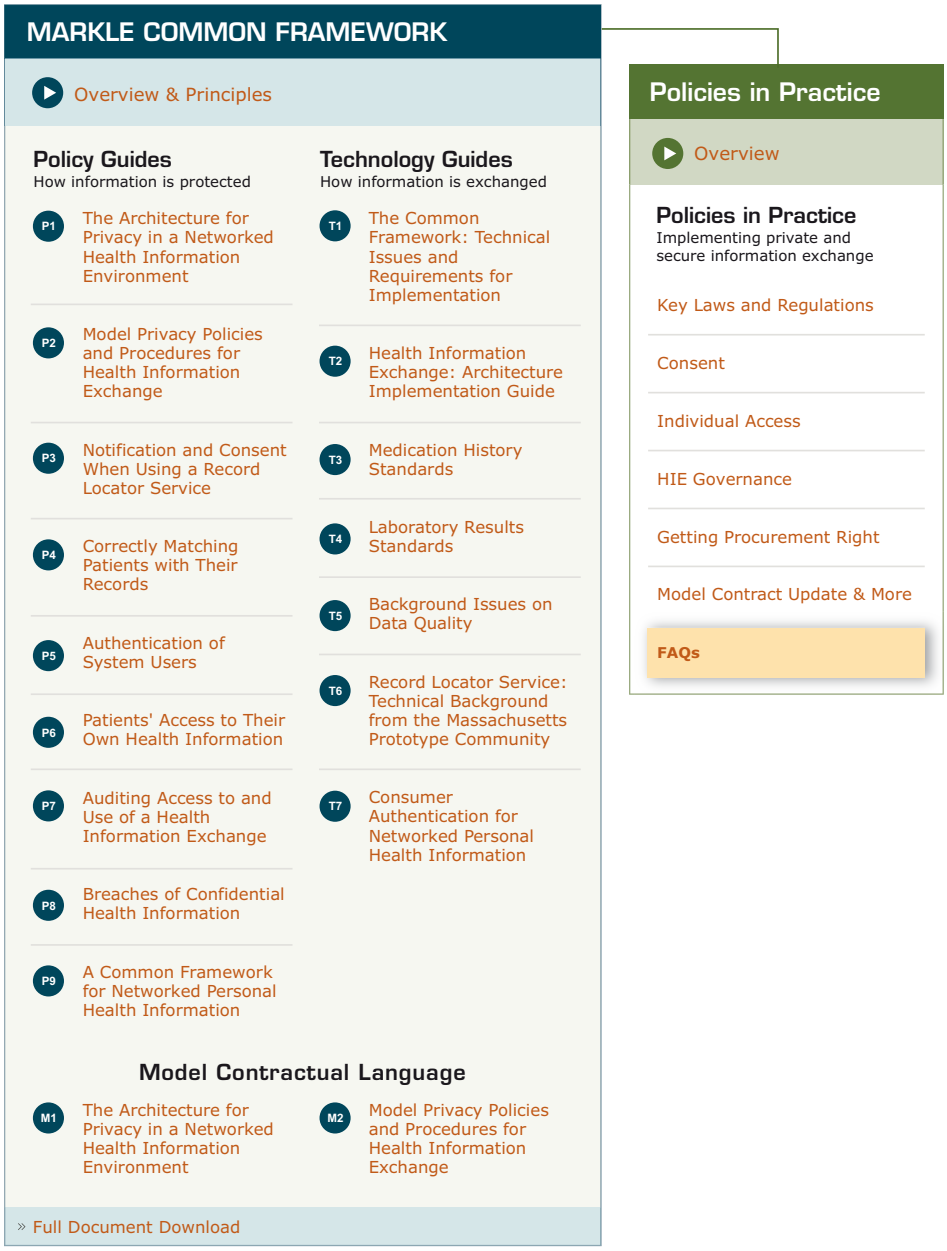
Policies in Practice

Frequently Asked Questions

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

Frequently Asked Questions About the Markle Common Framework

The following are answers to frequently asked questions about the Markle Connecting for Health Common Framework for Private and Secure Health Information Exchange (Markle Common Framework).

How does the Markle Common Framework apply Fair Information Practice Principles?

Information sharing depends on trusting relationships among entities and institutions, not machines. Our experience suggests that any health information sharing effort must adopt a framework of trust and then translate it into practice by specifying the policies, practices, and technology choices necessary for implementation. The specific policies and practices of the Markle Common Framework benefited greatly from their grounding in nine policy principles from the U.S. Fair Information Practice Principles (FIPPs)[1] and the Organization for Economic Cooperation and Development's (OECD) Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.[2] In the U.S., FIPPs have been recognized for decades at the state and national levels. Recently, both the Commerce Department and the Federal Trade Commission have recognized FIPPs as important foundational elements of a nationwide privacy framework to address privacy in a digital age.[3, 4]

---

[1] "A Review of the Fair Information Principles: The Foundation of Privacy Public Policy," *Privacy Rights Clearinghouse*. Last modified July 2010. http://www.privacyrights.org/ar/fairinfo.htm (accessed on February 22, 2012).

[2] "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," OECD. http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00&&en-USS_01DBC.html (accessed on February 22, 2012).

[3] "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers; Preliminary FTC Staff Report," Federal Trade Commission. Last modified December 2010. http://www.ftc.gov/os/2010/12/101201privacyreport.pdf (accessed on February 22, 2012).

[4] "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework," Department of Commerce Internet Policy Task Force. Last modified December 16, 2010. http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf (accessed on February 22, 2012).

Based on FIPPs, the Markle Common Framework policy principles include openness and transparency, purpose specification, collection limitation and minimization, use limitation, individual participation and control, data integrity and quality, security safeguards and controls, accountability and oversight, and remedies.[5] No single principle is adequate on its own. Meaningful safeguards are achieved by applying these principles together: applying some and not others can weaken the overall approach. In Appendix A, we provide tables that identify how the Markle Common Framework Policy and Technology Guides and the Policies in Practice address each of the core policy and technology principles.

How does the Markle Common Framework support population health activities?

As health information becomes increasingly networked, opportunities are growing to support health and health care not only for individuals, but for entire populations as well. Aggregation and analysis of population-level data can address important research questions related to quality, clinical effectiveness, public health, and safety. The Markle Connecting for Health First Principles for Population Health Data Sharing and Decision Making apply the key attributes of the Markle Common Framework to population health initiatives. The First Principles emphasize a distributed "network of networks" approach where data on individual patients remain with local data holders, while only summarized, anonymous data are aggregated for large-scale analysis. The First Principles outline an initial set of policy and technical principles to enable broad-scale information sharing, while protecting individual patient privacy.

Some technical challenges need to be addressed to allow for broad scale implementation of this model. For example, it is difficult to find and delete duplicate "anonymized" records that may be counted unintentionally in multiple summary statistics. However, there is promising research in the area of distributed models, as well as compelling examples of successful models that address a range of population health questions.[6, 7] Due to the enormous potential for societal benefit, further research and development is warranted.

---

[5] "P1: The Architecture for Privacy in a Networked Health Information Environment," *Markle Connecting for Health*, last modified April 2006. http://www.markle.org/sites/default/files/P1_CFH_Architecture.pdf (accessed on February 22, 2012).

[6] Carol C. Diamond, Clay Shirky and Farzad Mostashari, "Collecting and Sharing Data for Population Health: A New Paradigm." Health Affairs, 28, no. 2, (2009): 454–466. http://www.markle.org/publications/1463-collecting-and-sharing-data-population-health-new-paradigm (accessed on February 22, 2012).

[7] JS Brown, et al, "Distributed Health Data Networks: A Practical and Preferred Approach to Multi-institutional Evaluations of Comparative Effectiveness, Safety, and Quality of Care." *Med Care*, 48, no. 6, (2010): 45–51. http://journals.lww.com/lww-medicalcare/Fulltext/2010/06001/Distributed_Health_Data_Networks__A_Practical_and.9.aspx (accessed on February 22, 2012).

Does the Markle Common Framework address the sustainability of health information sharing efforts?

The Markle Common Framework is rooted in the premise that sustainability cannot be achieved unless efforts are grounded in clear and explicit health goals, and improvements in health care quality and cost-effectiveness are valued and supported.[8]

Although federal spending under the Health Information Technology for Economic and Clinical Health (HITECH) Act of the American Recovery and Recovery Act of 2009 (ARRA) has resulted in an unprecedented level of federal funding to foster the application of health IT and health information sharing, long-term sustainability will depend on aligning improvements in health care quality and cost-effectiveness with financial and non-financial incentives. In addition, the private sector needs to demonstrate clear and substantial support for these types of improvements in order to sustain health information sharing. A true return on investment can only be realized when this happens.

What is the Markle Common Framework's network approach?

The Markle Common Framework offers an approach to information sharing that is predicated on a 'network of networks', like the Internet, and designed to enable health information sharing with a policy and technology framework that promotes innovation and protects privacy.

The Markle Common Framework is built on the assumption that all health information sharing decisions are best made between the patient and the provider with whom the patient has a relationship. The network of networks design is distributed, allowing information to be kept at its source and transmitted when authorized to appropriate recipients. In this model, patients and the doctors they trust can decide with whom to share personal health information and for what purposes.

'Finding' the location of a patient's health information is described in the Markle Common Framework using an index called the Record Locator Service (RLS) that points users to the authorized records they are requesting. The RLS does not contain actual clinical data or clinical metadata. After identifying where the clinical information is stored, each provider holding records has the discretion to disclose those records, depending on the decisions the providers have made with their patients. Transfers of health information may then be accomplished via fax or secure e-mail, or by secure computer-to-computer transfers over the Internet, depending on the level of information sharing available. Providers and sources that routinely collaborate may exchange data automatically and electronically. Thus, there are two decisions to be made locally: whether to index and whether to share.

---

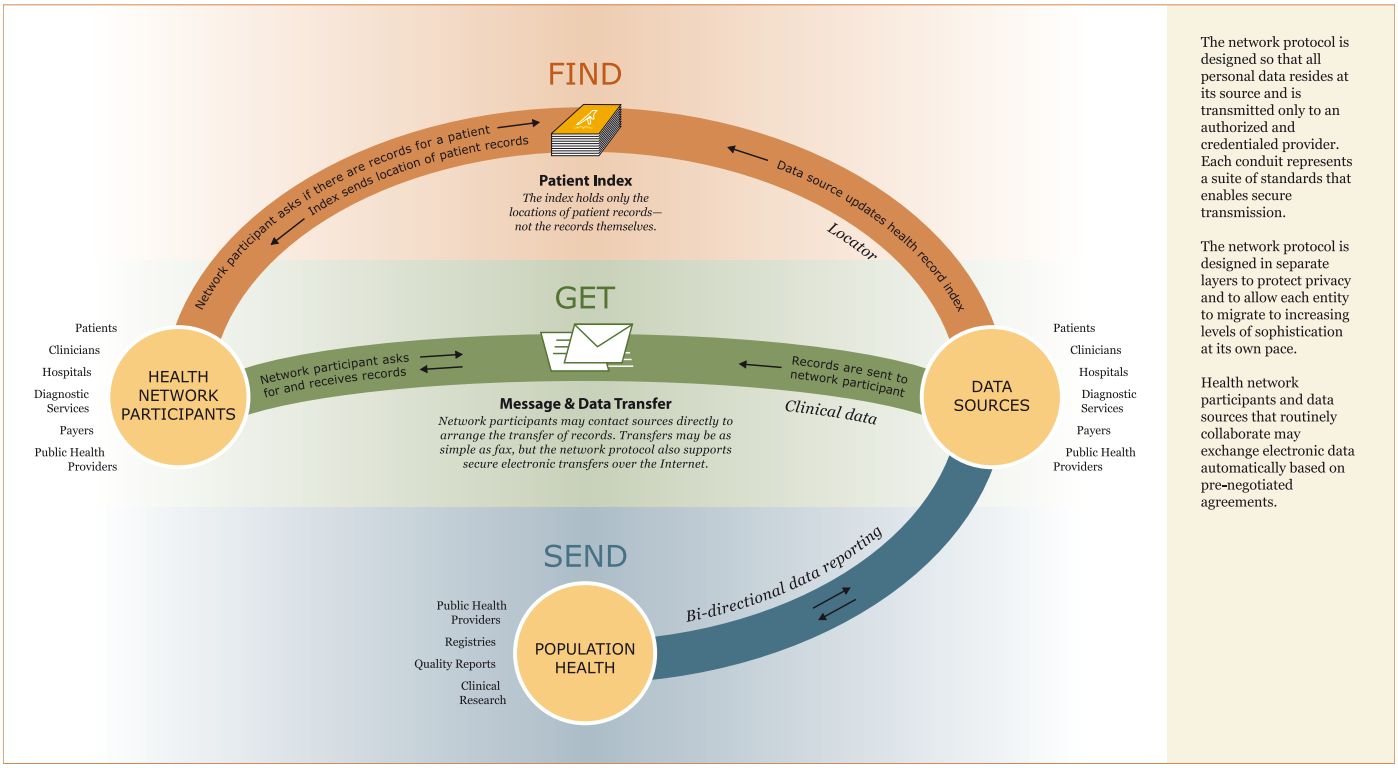
[8] Center for American Progress, Engelberg Center for Health Care Reform, and Markle Foundation, "Key Themes." Paper presented at the Aligning Health IT and Health Reform: Achieving an Information-Driven Health Care System Forum at the Center for American Progress, Washington, DC, July 15, 2009. http://www.markle.org/publications/899-aligning-health-it-and-health-reform-achieving-information-driven-health-care-syste (accessed on February 22, 2012).

This two-step process helps ensure that the system does not increase exposure of personal health information, while making record location fast and efficient, even in environments where electronic records are not fully available.

NETWORK PROTOCOL

MARKLE CONNECTING FOR HEALTH

(Updated January 2012)



The network protocol is designed so that all personal data resides at its source and is transmitted only to an authorized and credentialed provider. Each conduit represents a suite of standards that enables secure transmission.

The network protocol is designed in separate layers to protect privacy and to allow each entity to migrate to increasing levels of sophistication at its own pace.

Health network participants and data sources that routinely collaborate may exchange electronic data automatically based on pre-negotiated agreements.

Additional information on the RLS can be found in T1: The Markle Common Framework: Technical Issues and Requirements for Implementation.

As reflected in the Markle Common Framework, policies must be crafted in parallel with the design and deployment of technology and in an ongoing manner. Both policy and technology evolve with new information sharing needs and objectives, and therefore will remain important objectives.

How has the landscape changed since release of the Markle Common Framework?

The health information sharing landscape has changed dramatically since release of the Markle Common Framework in 2006. Over recent years, the level of federal leadership, new regulation, and public investment around health information sharing have increased substantially. In addition, use of health IT has grown among providers and individuals alike.

Early efforts to establish an infrastructure for health information sharing were bolstered in 2004 through an Executive Order which established the Department of Health and Human Services' (HHS) Office of the National Coordinator for Health Information Technology (ONC) and made possible efforts for standards harmonization, use case development, and the certification of electronic health record (EHR) products. By 2006, the health care sector was struggling to overcome challenges of policy, technology and capital investment to advance health information sharing.

Adoption of health IT in clinical settings was weak. In 2006, only 29.2 percent of physicians reported any electronic medical record (EMR) or EHR in their office-based practice.[9] (An EMR/EHR is a medical or health record system that is either all or partially electronic, excluding systems solely for billing.) That same year, 26 health information exchanges (HIEs) reported being operational and transmitting data for use by their health care stakeholders.[10]

Enactment of the HITECH Act in February 2009 marked a new level of federal leadership, regulation and investment for health information sharing. Aiming to address many of the challenges facing the health care sector, the HITECH Act codified into law the U. S. Department of Health and Human Services' (HHS) Office of the National Coordinator for Health Information Technology (ONC), established federal advisory committees to advise ONC on policy and standards decisions, invested in state HIE, set forth an EHR incentives program for Medicare and Medicaid providers, established new initiatives to support the education and training of the health IT workforce, modified particular aspects of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and established new programs to foster individual engagement with health IT.

On the heels of the HITECH Act, broad-scale health care reform legislation, the Patient Protection and Affordable Care Act of 2009 (ACA), was enacted. Aspects of ACA aim to further leverage health IT in efforts to transform health care. For example, it calls for the creation of a "Shared Savings Program" to deliver seamless, high-quality care for Medicare beneficiaries through Accountable Care Organizations (ACOs), which must apply health IT in order to meet care coordination requirements.

---

[9] Chun-Ju Hsiao, et al, "Electronic Medical Record/Electronic Health Record Use by Office-based Physicians: United States, 2008 and Preliminary 2009," *Centers for Disease Control and Prevention*. Last modified December 23, 2009. http://www.cdc.gov/nchs/data/hestat/emr_ehr/emr_ehr.htm#figures (accessed on February 22, 2012).

[10] "Migrating Toward Meaningful Use: The State of Health Information Exchange," *eHealth Initiative*. http://www.sftvision.com/2009SurveyReportFINAL.pdf (accessed on February 22, 2012).

Recent investments have recognized health IT and health information sharing as critical to improving the quality and efficiency of health care in the U.S., as reflected by rising adoption rates. Preliminary data indicate that 43.9 percent of physicians reported any EMR/EHR in their office-based practice in 2009.[11] By 2011, 85 HIEs were reported to be operational.[12]

A recent Markle Survey on Health in a Networked Life uniquely compares the core values of physicians and patients on deployment of IT in health care. Seventy-four percent of doctors surveyed said that they would prefer computer-based means (electronic networks, secure email, or portable storage devices) to paper and fax, when sharing patient information with each other. Up to 74 percent of doctors agreed that patients should be able to share information with their doctors electronically. At least 59 percent of the public agreed with this statement. The survey results also indicate that personal health record (PHR) adoption is on the rise, with 10 percent of the surveyed public reporting having a PHR in 2010, compared to 3 percent in 2008.[13]

How does the Markle Common Framework align with state and federal efforts?

Since its release in 2006, health information sharing efforts have used the Markle Common Framework to develop architecture, specifications, and policies for the private and secure sharing of health information. Many states cite the Markle Common Framework in their operational and strategic plans to ONC as part of the State HIE Cooperative Agreement Program. States also refer to the Markle Common Framework in their online policy and technology materials.[14]

The Markle Common Framework is also closely aligned with federal policy efforts. For example, the EHR incentive program reflects many elements of the Markle Common Framework; setting forth minimum necessary standards to allow for flexibility and innovation within the marketplace, as well as requiring the submission of aggregate quality data to minimize risk of exposing patient

---

[11] Chun-Ju Hsiao, et al, "Electronic Medical Record/Electronic Health Record Use by Office-based Physicians: United States, 2008 and Preliminary 2009," *Centers for Disease Control and Prevention*. Last modified December 23, 2009. http://www.cdc.gov/nchs/data/hestat/emr_ehr/emr_ehr.htm#figures (accessed on February 22, 2012).

[12] "2011 Report on Health Information Exchange: Full Report," *eHealth Initiative*. http://www.ehealthinitiative.org/store.html?page=shop.product_details&flypage=flypage.tpl&category_id=8&product_id=67 (accessed on February 22, 2012).

[13] "The Public and Doctors Overwhelmingly Agree on Health IT Priorities to Improve Patient Care," *Markle Foundation*, (last modified January 2011). http://www.markle.org/publications/1461-public-and-doctors-overwhelmingly-agree-health-it-priorities-improve-patient-care (accessed on February 22, 2012).

[14] Through an environmental scan of state HIE websites, we found that the following states have cited the Markle Common Framework in their State HIE Strategic or Operational plans or online materials: AZ, MD, SC, IL, AL, FL, RI, MN, NY, CO, ID, MO, MT, NJ, NC, VT, MA, VA, WI, MD, and WV.

data.[15, 16] In the area of population health, ONC recently announced new efforts to explore and further the application of distributed networks.[17]

The important role of foundational principles, policies, and practices, like those of the Markle Common Framework, in supporting the trusted sharing of health information, is recognized by the federal government. For example, the Health IT Task Force, a joint initiative of the ONC and Office of Management and Budget, called for select federal agencies to coordinate health IT investments around a shared set of policy and technology principles, to maximize the benefits of health IT. In September 2010, Vivek Kundra, the Federal Chief Information Officer, and David Blumenthal, the National Coordinator for Health IT, articulated a set of policy and technology principles for agencies to use as a guide in planning for and using health IT investments that emphasized five principles:

1. Improve health and health care;
2. Promote open government and provide patients with a secure, timely, electronic copy of their own information;
3. Share health information between providers;
4. Protect privacy and security, aligning with FIPPs; and
5. Use a distributed data architecture versus centralized data warehouses.[18]

---

[15] "Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology; Final Rule." *Federal Register* 75 (July 28, 2010). http://edocket.access.gpo.gov/2010/pdf/2010-17210.pdf (accessed on February 22, 2012).

[16] "Medicare and Medicaid Programs; Electronic Health Record Incentive Program; Final Rule." *Federal Register 75* (July 28, 2010). http://edocket.access.gpo.gov/2010/pdf/2010-17207.pdf (accessed on February 22, 2012).

[17] Doug Fridsma, "Join Query Health in Developing National Standards for Population Queries," *HealthITBuzz* (blog), September 23, 2011 (11:29 p.m.), http://www.healthit.gov/buzz-blog/from-the-onc-desk/queryhealth/ (accessed on February 22, 2012).

[18] Vivek Kundra and David Blumenthal to Selected Heads of Executive Departments and Agencies, memorandum, "Health Information Technology Guidance," September 17, 2010, Chief Information Officers Council. http://www.cio.gov/documents/Health-Information-Technology-Guidance.pdf (accessed on February 22, 2012).

How does the Markle Common Framework for Private and Secure Health Information Exchange relate to the Markle Common Framework for Networked Personal Health Information?

The Markle Common Framework approach, based on Fair Information Practice Principles (FIPPs), has been applied to create two bodies of work. These two frameworks share the same foundational attributes and principles. The variation in the frameworks is how these principles are specifically applied in two different information-sharing contexts as outlined below.

The Markle Common Framework for Private and Secure Health Information Exchange (released in 2006)	**The Markle Common Framework for Networked Personal Health Information** (released in 2008)
Purpose: Helps health information networks to share information among their members and nationwide while protecting privacy and allowing for local autonomy and innovation.	**Purpose:** Recommends practices that encourage appropriate handling of personal health information as it flows to and from electronic PHRs and similar applications or supporting services.
Focus: Specific to the context of the electronic exchange of patient information among health professionals and health care entities.	**Focus:** Specific to the context of connecting individuals online to their own information, such as via electronic PHRs, or to other health-related services and applications that use the individual's personal health information.

Appendix A

Each of the Policies in Practice and the Policy and Technology Guides of the Markle Common Framework for Private and Secure Information Exchange (Markle Common Framework) addresses a subset of relevant core policy and technology principles. The tables in this Appendix identify each resource and its corresponding core policy and technology principles.

Markle Connecting for Health Core Policy Principles

Markle Connecting for Health has published a set of policy principles that provide the foundation for privacy and health information technology (IT) in a networked environment. The Markle Connecting for Health approach dictates that these nine principles be balanced together and considered as part of one package. Elevating certain principles over others would weaken any overall architectural solution to privacy protection in a networked health information environment.

In brief, the principles and the corresponding resources are as follows:

CORE POLICY PRINCIPLES	MARKLE COMMON FRAMEWORK PRACTICE AREAS	POLICIES IN PRACTICE
1. **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.	• 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 • 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	• Consent: Implementing the Individual Choice and Control Principle • Getting Procurement Right: Policy Aware Procurement Strategies and Practices • Mechanisms for Oversight, Accountability, and Enforcement: The Model Contract and More • Governance of Health Information Sharing Efforts: Achieving Trust and Interoperability with Meaningful Consumer Participation • Individual Access: Connecting Patients with Their Health Information

CORE POLICY PRINCIPLES	MARKLE COMMON FRAMEWORK PRACTICE AREAS	POLICIES IN PRACTICE
2. Purpose specification: 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.	• 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	• Consent: Implementing the Individual Choice and Control Principle
3. 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.	• 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	• Consent: Implementing the Individual Choice and Control Principle • Getting Procurement Right: Policy Aware Procurement Strategies and Practices • Mechanisms for Oversight, Accountability, and Enforcement: The Model Contract and More
4. Use limitation: Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified.	• 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 • P7: Auditing Access to and Use of a Health Information Exchange	• Getting Procurement Right: Policy Aware Procurement Strategies and Practices • Mechanisms for Oversight, Accountability, and Enforcement: The Model Contract and More

CORE POLICY PRINCIPLES	MARKLE COMMON FRAMEWORK PRACTICE AREAS	POLICIES IN PRACTICE
	• T1: The Common Framework: Technical Issues and Requirements for Implementation • T6: Record Locator Service: Technical Background from the Massachusetts Prototype Community	
5. 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.	• 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 • P6: Patients' Access to Their Own Health Information • P8: Breaches of Confidential Health Information • P9: A Common Framework for Networked Personal Health Information • T5: Background Issues on Data Quality • T6: Record Locator Service: Technical Background from the Massachusetts Prototype Community	• Consent: Implementing the Individual Choice and Control Principle • Getting Procurement Right: Policy Aware Procurement Strategies and Practices • Mechanisms for Oversight, Accountability, and Enforcement: The Model Contract and More • Governance of Health Information Sharing Efforts: Achieving Trust and Interoperability with Meaningful Consumer Participation • Individual Access: Connecting Patients with Their Health Information

CORE POLICY PRINCIPLES	MARKLE COMMON FRAMEWORK PRACTICE AREAS	POLICIES IN PRACTICE
6. 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.	• P1: The Architecture for Privacy in a Networked Health Information Environment • P2: Model Privacy Policies and Procedures for Health Information Exchange • P5: Authentication of System Users • P6: Patients' Access to Their Own Health Information • T5: Background Issues on Data Quality • T6: Record Locator Service: Technical Background from the Massachusetts Prototype Community • T7: Consumer Authentication for Networked Personal Health Information	• Mechanisms for Oversight, Accountability, and Enforcement: The Model Contract and More • Governance of Health Information Sharing Efforts: Achieving Trust and Interoperability with Meaningful Consumer Participation
7. 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.	• P1: The Architecture for Privacy in a Networked Health Information Environment • P2: Model Privacy Policies and Procedures for Health Information Exchange • P4: Correctly Matching Patients with Their Records • P5: Authentication of System Users • 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	• Consent: Implementing the Individual Choice and Control Principle • Getting Procurement Right: Policy Aware Procurement Strategies and Practices • Mechanisms for Oversight, Accountability, and Enforcement: The Model Contract and More • Governance of Health Information Sharing Efforts: Achieving Trust and Interoperability with Meaningful Consumer Participation • Individual Access: Connecting Patients with Their Health Information

CORE POLICY PRINCIPLES	MARKLE COMMON FRAMEWORK PRACTICE AREAS	POLICIES IN PRACTICE
	• T1: The Common Framework: Technical Issues and Requirements for Implementation • T2: Health Information Exchange: Architecture Implementation Guide • T6: Record Locator Service: Technical Background from the Massachusetts Prototype Community • T7: Consumer Authentication for Networked Personal Health Information	
8. Accountability and oversight: Entities in control of personal health data must be held accountable for implementing these information practices.	• P1: The Architecture for Privacy in a Networked Health Information Environment • P2: Model Privacy Policies and Procedures for Health Information Exchange • P5: Authentication of System Users • P7: Auditing Access to and Use of a Health Information Exchange • P8: Breaches of Confidential Health Information • T1: The Common Framework: Technical Issues and Requirements for Implementation • T7: Consumer Authentication for Networked Personal Health Information	• Consent: Implementing the Individual Choice and Control Principle • Getting Procurement Right: Policy Aware Procurement Strategies and Practices • Mechanisms for Oversight, Accountability, and Enforcement: The Model Contract and More • Governance of Health Information Sharing Efforts: Achieving Trust and Interoperability with Meaningful Consumer Participation

CORE POLICY PRINCIPLES	MARKLE COMMON FRAMEWORK PRACTICE AREAS	POLICIES IN PRACTICE
9. Remedies: Legal and financial remedies must exist to address any security breaches or privacy violations.	• P1: The Architecture for Privacy in a Networked Health Information Environment • P2: Model Privacy Policies and Procedures for Health Information Exchange • P4: Correctly Matching Patients with Their Records • P8: Breaches of Confidential Health Information	• Consent: Implementing the Individual Choice and Control Principle • Getting Procurement Right: Policy Aware Procurement Strategies and Practices • Mechanisms for Oversight, Accountability, and Enforcement: The Model Contract and More • Governance of Health Information Sharing Efforts: Achieving Trust and Interoperability with Meaningful Consumer Participation

Markle Connecting for Health Core Technology Principles

In addition to the set of policy principles, Markle Connecting for Health has published a set of technology principles. Together, these principles have guided the specific, practical decisions about the architecture, specifications, and policies that support private and secure sharing of health information across the nation.

In brief, the technology principles and corresponding resources are as follows:

CORE POLICY PRINCIPLES	MARKLE COMMON FRAMEWORK PRACTICE AREAS	POLICIES IN PRACTICE
1. Make it "Thin": Only the minimum number of rules and protocols essential to widespread sharing 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 to allow for information sharing among subordinate networks.	• T1: The Common Framework: Technical Issues and Requirements for Implementation • T6: Record Locator Service: Technical Background from the Massachusetts Prototype Community	• Governance of Health Information Sharing Efforts: Achieving Trust and Interoperability with Meaningful Consumer Participation
2. Avoid "Rip and Replace": Any proposed model for health information sharing must take into account the current structure of the health care 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.	• T1: The Common Framework: Technical Issues and Requirements for Implementation • T6: Record Locator Service: Technical Background from the Massachusetts Prototype Community	

CORE POLICY PRINCIPLES	MARKLE COMMON FRAMEWORK PRACTICE AREAS	POLICIES IN PRACTICE
3. 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.	• 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	
4. 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.	• P1: The Architecture for Privacy in a Networked Health Information Environment • P3: Notification and Consent When Using a Record Locator Service • T1: The Common Framework: Technical Issues and Requirements for Implementation • T2: Health Information Exchange: Architecture Implementation Guide • T6: Record Locator Service: Technical Background from the Massachusetts Prototype Community	

CORE POLICY PRINCIPLES	MARKLE COMMON FRAMEWORK PRACTICE AREAS	POLICIES IN PRACTICE
5. 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 health information sharing.	• P2: Model Privacy Policies and Procedures for Health Information Exchange • P8: Breaches of Confidential Health Information • T1: The Common Framework: Technical Issues and Requirements for Implementation • T6: Record Locator Service: Technical Background from the Massachusetts Prototype Community	• Governance of Health Information Sharing Efforts: Achieving Trust and Interoperability with Meaningful Consumer Participation
6. Flexibility: Any hardware or software can be used for health information sharing 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.	• T1: The Common Framework: Technical Issues and Requirements for Implementation • T2: Health Information Exchange: Architecture Implementation Guide	
7. Privacy and Security: All health information sharing, 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.	• 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 • P7: Auditing Access to and Use of a Health Information Exchange • P8: Breaches of Confidential Health Information	• Consent: Implementing the Individual Choice and Control Principle • Getting Procurement Right: Policy Aware Procurement Strategies and Practices • Mechanisms for Oversight, Accountability, and Enforcement: The Model Contract and More • Governance of Health Information Sharing Efforts: Achieving Trust and Interoperability with Meaningful Consumer Participation

CORE POLICY PRINCIPLES	MARKLE COMMON FRAMEWORK PRACTICE AREAS	POLICIES IN PRACTICE
	• P9: A Common Framework for Networked Personal Health Information • T1: The Common Framework: Technical Issues and Requirements for Implementation • T2: Health Information Exchange: Architecture Implementation Guide • T5: Background Issues on Data Quality • T6: Record Locator Service: Technical Background from the Massachusetts Prototype Community	• Individual Access: Connecting Patients with Their Health Information
8. Accuracy: Accuracy in identifying both a patient and his or her records with little tolerance for error is an essential element of health information sharing. There must also be feedback mechanisms to help organizations fix or "clean" their data in the event that errors are discovered.	• P4: Correctly Matching Patients with Their Records • P5: Authentication of System Users • T1: The Common Framework: Technical Issues and Requirements for Implementation • T2: Health Information Exchange: Architecture Implementation Guide • T5: Background Issues on Data Quality • T6: Record Locator Service: Technical Background from the Massachusetts Prototype Community	

Acknowledgements

Markle Connecting for Health HIE Advisory Committee

Committee Members

Phyllis Albritton
Colorado Regional Health Information Organization

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
MedCommons

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
Louisiana Health Care Quality Forum

Paul Uhrig
Surescripts

Stefaan Verhulst
Markle Foundation

Marcy Wilder, JD
Hogan Lovells

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.