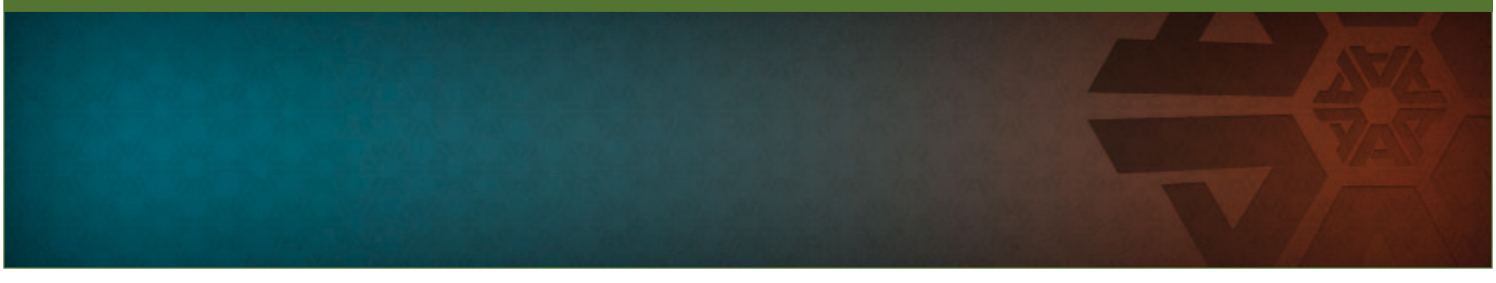
Markle Connecting for Health
Common Framework for Private and
Secure Health Information Exchange

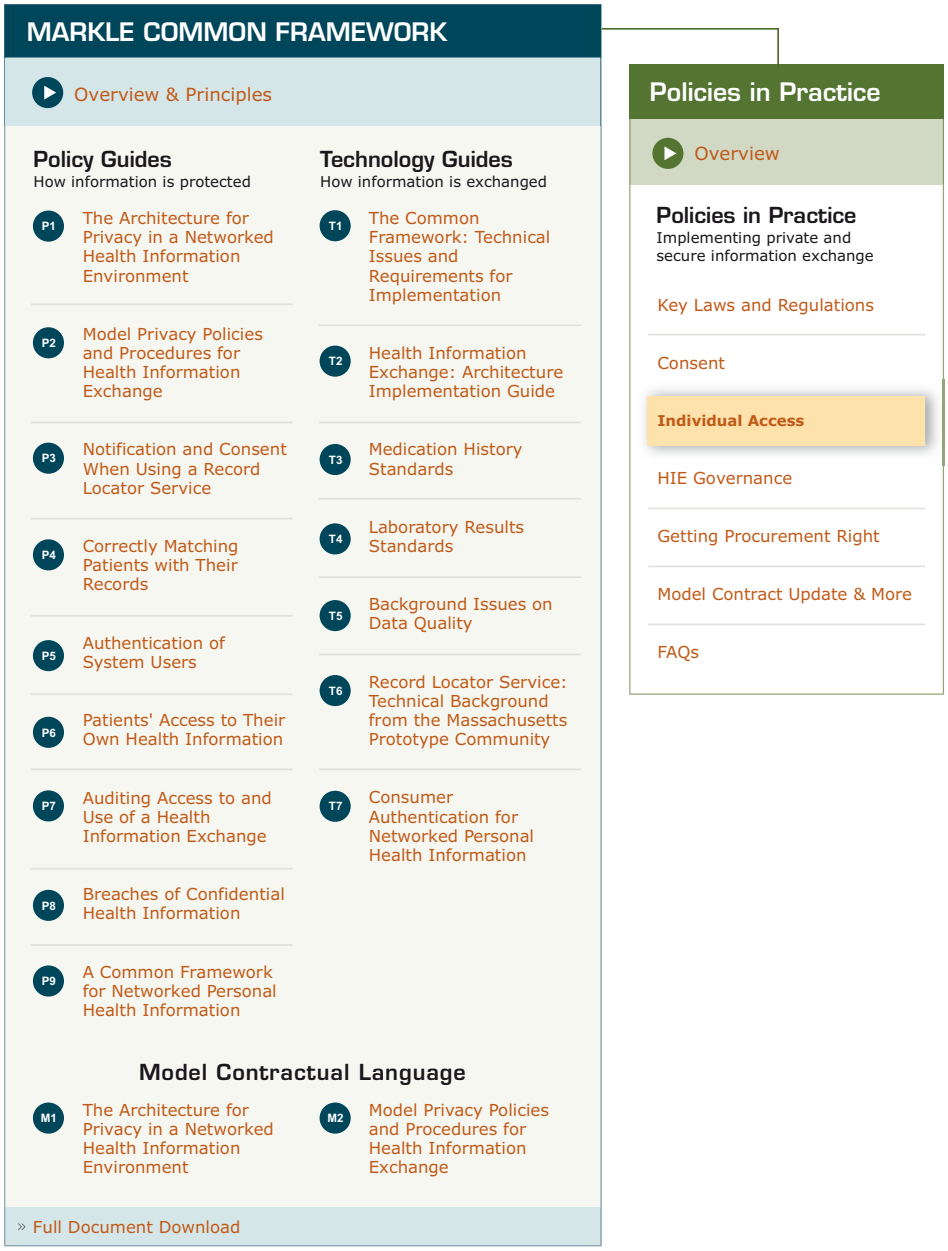
# Policies in Practice

## Individual Access: Connecting Patients with Their Health Information

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

# Individual Access: Connecting Patients with Their Health Information

## Executive Summary

Providing individuals access to their own information is well-rooted in Fair Information Practice Principles (FIPPs) and a basic expectation for health IT. Convenient access to one's own personal health information serves as a building block to helping people lead healthier lives and get higher-quality, more cost-effective care.

The Markle Connecting for Health Common Framework for Networked Personal Health Information recommends practices that encourage appropriate handling of personal health information as it flows to and from electronic personal health records (PHRs) and similar applications or supporting services. It is built upon a set of FIPPs-based core principles that provide the foundation for managing personal health information within consumer-accessible data streams.

Recently adopted laws and related policies have accelerated efforts to connect consumers to their health care providers and their own information. The ability for individuals to log in securely online to view and download pertinent health information is a good starting place for enabling such access.

This Policies in Practice outlines the basic requirements for giving patients access to personal health information through a download capability. It draws upon consensus-based recommendations reflected in the Markle Common Framework for Networked Personal Health Information and the Markle Connecting for Health Policies in Practice: The Download Capability.

---

*Markle Connecting for Health thanks Josh Lemieux, former Director of Personal Health Technology, Markle Foundation, 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.*

## I. What is the Markle Common Framework for Networked Personal Health Information and when does it apply to health information sharing efforts?[1]

The Markle Common Framework for Networked Personal Health Information, published in 2008, was developed and supported by 56 organizations, representing technology companies, health insurers, provider groups and medical professional societies, consumer and patient advocacy groups, and privacy experts.

This broad support reflects a consensus on policy and technology practices for the storage and flow of personal health information into and out of consumer-accessible applications such as electronic personal health records (PHRs).

We use the term "consumer access services" for organizations that provide individuals with online connections to personal health information and services. Consumers may be offered such services by a variety of organizations, ranging from existing health care entities (e.g., providers, payers, pharmacies, self-insured employers) to new entrants to the health sector (e.g., technology companies, employer coalitions, or state or regional health information sharing efforts). The Markle Common Framework for Networked Personal Health Information is intended for any organization providing consumer access services—regardless of whether it is covered by the Health Insurance Portability and Accountability Act (HIPAA), a business associate of a HIPAA-covered entity, or outside of the HIPAA regulatory purview.

The Markle Common Framework approach has been applied to create two bodies of work related to the following specific health information technology (IT) contexts:

| **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. |

[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)."

Health information sharing efforts should implement all the elements of the Markle Connecting for Health Common Framework for Private and Secure Health Information Exchange for electronic exchange of patient information among health professionals and health care entities.

If a health information sharing effort is also going to play a role in helping providers give patients access to their own information, then the policies and practices of the Markle Common Framework for Networked Personal Health Information should also be applied to address the specific function of connecting individuals online to their own information.

As we outline in Questions 2 and 4 below, many health information sharing efforts are contemplating access for individuals through a variety of models, including service models for participating doctors and hospitals, to attain the patient engagement requirements of the Meaningful Use (MU) financial incentives.

## II. Why is consumer access important and how are health information sharing efforts considering a role in helping to provide access for individuals?

Providing individuals with access to information captured about them is well-rooted in Fair Information Practice Principles (FIPPs) and is a basic expectation for health IT. Convenient access to one's own personal health information is a building block to helping people live healthier lives and get higher-quality and more cost-effective care. Roughly two-thirds of the American public and doctors support an individual's ability to view and download his/her personal health information online, according to a recent Markle Survey on Health in a Networked Life.[2]

By giving individuals convenient access to copies of their own information, organizations can help patients communicate better with health care providers and take an active role in transforming health care. Network-enabled efficiencies and safety improvements are more likely to occur if individuals and health care professionals act as partners who share access to and responsibility for updating personal health information. We describe this potential in the Markle Common Framework: Consumers as Network Participants.

> **Juan Alaniz, Washington State:** Just as the goal for providers is not just acquisition of health IT, it's about them using health IT to transform how they deliver health care. For consumers, the goal is not just that they access their health information electronically. The goal is that by putting consumers in the driver's seat, they can become direct participants in their care, in collaboration with their physicians, and they can help direct how their health care will be delivered.

---

[2] Markle Health in a Networked Life, "Public and Doctors Alike Support Allowing Individuals to Download Their Own Health Information," *Markle Foundation*, last modified January 31, 2011. http://www.markle.org/publications/1441-public-and-doctors-alike-support-allowing-individuals-download-their-own-health-in (accessed on February 22, 2012).

In the last few years, several factors have accelerated the effort to connect consumers to their health care providers and their own information. As in other sectors, many health entities such as integrated delivery networks and health insurers recognize the value of and are emphasizing online connections with consumers to improve service, lower administrative costs, and remain competitive. The Health Information Technology for Economic and Clinical Health (HITECH) Act established that individuals have the right to obtain electronic copies of their information held in electronic health records (EHRs). The MU requirements under HITECH also have placed priority on patient access and engagement for providers and hospitals to qualify for federal financial incentives.

Section 13405 (e) of HITECH established an individual's right to request information in electronic format from EHRs and have it sent to a service of the individual's choosing. Although there may be varying interpretations as to whether this provision applies specifically to state or regional health information sharing efforts, it clearly establishes the basic expectation that health IT will help foster individual access to personal health information.

The MU requirements of the EHR Incentives Program include the delivery of electronic copies of personal health information to patients. For Stage 2 of this program, it has been proposed that patients should be able to view and download their information from participating providers and hospitals. Similarly, patient engagement is likely to be a focus for emerging requirements for Accountable Care Organizations (ACOs) within the Medicare Shared Savings Program.

Individual access is also addressed in a March 2012 Program Information Notice titled Privacy and Security Framework Requirements and Guidance for the State Health Information Exchange Cooperative Agreement Program released by the Office of the National Coordinator for Health Information Technology (ONC).

As a result of all of these factors, several health information sharing efforts are seeking ways to help participating providers and hospitals fulfill these MU and health care reform requirements. These health information sharing efforts are contemplating how to enable providers' achievement of these requirements in a variety of ways. For example, some will seek to provide secure access directly to individuals to retrieve information such as medication lists or past lab results from doctors and hospitals. Alternatively, some may supply such information to the providers' EHRs, which, in turn, offer online access to individuals (through secure online patient portals or electronic PHRs). Yet another opportunity to provide individuals with access to their own health information is via secure e-mail. In all cases, the provider would have a primary role in engaging patient participation, which could help satisfy some of the requirements of these programs.

Notably, a health information sharing effort does not have to aggregate an individual's information in order to provide a useful service. Simply providing basic information such as record location services can be useful to both participating providers as well as patients. The information a health information sharing effort is able to make available to patients will reflect its larger structure and organization, and should respect the meaningful decisions individuals have made with the providers or entities with whom they have a relationship about whether and

how to share their health share their information. Regardless of the ways in which consumers may be ultimately given access to their personal health information, such access must be implemented with careful policies and practices in place to protect personal health information and earn the trust of the public and providers.

## III. What are the components of the Framework and how can they be incorporated in the procurement process for personal health information services?

The Markle Common Framework for Networked Personal Health Information is built upon a set of **core principles** that provide the foundation for managing personal health information within consumer-accessible data streams. These principles are based on accepted FIPPs. Each principle must be contextualized into a set of policy and technology practices that together protect privacy and enhance trust. All such policy and technology practice areas must be addressed in a sound and public way to provide adequate protections to consumers and to encourage trust across a network. (See **Appendix A** for the principles and **Appendix B** for the practice areas.)

A useful resource to implement the Markle Common Framework for Networked Personal Health Information is the detailed due diligence Policy and Technology Checklists for Procurers and Implementers. These tools were derived by analyzing the recommendations of each practice area, then developing a set of detailed questions that can be used as a checklist of recommended policy practices which may be used in requests for information (RFI), requests for proposals (RFP), procurement requirements or policy development discussion guides.

## IV. What is a good starting point for individual access?

The ability for individuals to log in securely online to view and download pertinent health information, such as what is required for patient engagement under Meaningful Use, is a good starting place for enabling individual access.

The Markle Connecting for Health public-private collaboration has emphasized the download capability as a critical building block for patient engagement and market innovation.[3]

Implementing the online view and download capability for patients is not the same as developing and implementing a fully functional PHR. The basic requirements begin with **secure online access**, meaning that the identity of each individual given credentials to access his or her own data must be proofed to an acceptable level of accuracy, and the individual must present an acceptable token (e.g., unique username and password combination) upon login to get access to the data for view and/or to download.

---

[3] Markle Connecting for Health Work Group on Consumer Engagement, "Policies in Practice: The Download Capability," *Markle Foundation*, last modified August 31, 2010. http://www.markle.org/publications/1198-policies-practice-download-capability (accessed on February 22, 2012).

Establishing an individual's identity and issuing authentication tokens for network access can be a significant barrier for health information sharing efforts or any entity that does not have a direct relationship with the patient. The solutions will depend on the relationship that the entity has with patients, or whether it can "bootstrap" identity proofing performed at participating provider organizations or other organizations that may have a relationship with the consumers.

The CT2 guide of the Markle Common Framework for Networked Personal Health Information has a detailed set of recommendations regarding identity proofing and monitoring, authentication tokens, and reliance on third parties for such services.

The second basic requirement is that logged-in individuals be able to **view and download** key information about themselves in human-readable formats. The MU patient engagement data sets are a good place to start, such as problem and medication lists, allergies, laboratory results, and clinical visit summaries (from eligible providers) and hospital discharge instructions (from eligible hospitals). Any entity offering the download capability should obtain **independent confirmation** from the individual (i.e., such as a "yes" response to a question) that the individual wants to download a copy of personal health information. Such independent confirmation should be obtained after presenting the individual with, at a minimum, the following **clearly stated information:**

> *Health records can contain sensitive information.*
>
> *If you download sensitive information to a shared or unsecured computer or device, others might see it.*
>
> *You are responsible for protecting the information that you download, and for deciding with whom to share it.*
>
> *Are you sure you want to download a copy of your personal health information to the computer or device you are using?*

With respect to download formats, **human-readability** is the minimum requirement. Additionally, if the data are available in the standardized clinical summary formats endorsed as MU standards (i.e., CCD or CCR), the patient should have an option to download that data in those formats. The bottom-line requirement for human readability ensures that people will not need to use a specific application or service to see their own health information. They should have the option of viewing and downloading their information in human-readable form through ubiquitous Internet browsers and common software formats (e.g., text, spreadsheet, or PDF).

By "human-readable," we mean information viewable and downloadable online should be in English or other language common to a provider's majority population of patients. It is ideal for the terminology to be as patient-friendly and free of medical jargon as possible, as well as translated into languages common to a provider's patient population. However, we do not recommend strict requirements for how understandable the information must be to patients at this time. It is more important to make the information available securely and conveniently online.

The important distinction of a basic view and download capability is that the entity providing it does not also necessarily have to do the hard work of developing applications that allow consumers to use or manipulate their own health information. Once individuals download their information, they have the opportunity to choose from a variety of different services or offerings to manage and use the information further. The experience at the U.S. Department of Veterans Affairs (VA), and with the Medicare and TRICARE programs, demonstrate that the basic capability has value to patients and can spur private sector innovation. When the VA enabled patients to download their information, the private sector responded by demonstrating a wide range of applications that made that information useful to patients (making it easier to know when to take medications, storing medical images, and connecting with peers who have similar health conditions). As the download capability becomes a common feature, individuals may have a need for proxy services to organize and regularly update their personal health information.

The Markle Common Framework Policies in Practice: The Download Capability provides specific recommendations for health information sharing efforts and other data holders to enable patients to download their information, as well as policy considerations for enabling secure automated downloads through a variety of services.

## Appendix A

The Markle Common Framework for Networked Personal Health Information consists of Consumer Policy (CP) and Consumer Technology (CT) guides; it is a hallmark of the approach that policy and technology work together interdependently.

Here are the nine principles and their corresponding guides:

| CORE POLICY PRINCIPLES | MARKLE COMMON FRAMEWORK FOR NETWORKED PERSONAL HEALTH INFORMATION PRACTICE AREAS |
|---|---|
| 1. **Openness and transparency:** Consumers should be able to know what information has been collected about them, the purpose of its use, who can access and use it, and where it resides. They should also be informed about how they may obtain access to information collected about them and how they may control who has access to it. | • CP2: Policy Notice to Consumers |
| 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. | • CP2: Policy Notice to Consumers<br>• CP3: Consumer Consent to Collections, Uses, and Disclosures of Information<br>• CT4: Limitations on Identifying Information |
| 3. **Collection limitation and data minimization:** Personal health information should only be collected for specified purposes and should be obtained by lawful and fair means. The collection and storage of personal health data should be limited to that information necessary to carry out the specified purpose. Where possible, consumers should have the knowledge of or provide consent for collection of their personal health information. | • CP2: Policy Notice to Consumers<br>• CP3: Consumer Consent to Collections, Uses, and Disclosures of Information<br>• CT4: Limitations on Identifying Information |

| CORE POLICY PRINCIPLES | MARKLE COMMON FRAMEWORK FOR NETWORKED PERSONAL HEALTH INFORMATION PRACTICE AREAS |
|---|---|
| 4. **Use limitation:** Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified. | • CP2: Policy Notice to Consumers<br>• CP3: Consumer Consent to Collections, Uses, and Disclosures of Information<br>• CP7: Discrimination and Compelled Disclosures<br>• CT3: Immutable Audit Trails<br>• CT4: Limitations on Identifying Information |
| 5. **Individual participation and control:** Consumers should be able to control access to their personal information. They should know who is storing what information on them, and how that information is being used. They should also be able to review the way their information is being used or stored. | • CP3: Consumer Consent to Collections, Uses, and Disclosures of Information<br>• CP5: Notification of Misuse or Breach<br>• CP7: Discrimination and Compelled Disclosures<br>• CP8: Consumer Obtainment and Control of Information<br>• CT3: Immutable Audit Trails<br>• CT5: Portablility of Information |
| 6. **Data quality and integrity:** All personal data collected should be relevant to the purposes for which they are to be used and should be accurate, complete, and up-to-date. | • CP6: Dispute Resolution<br>• CP8: Consumer Obtainment and Control of Information<br>• CT2: Authentication of Consumers<br>• CT3: Immutable Audit Trails |
| 7. **Security safeguards and controls:** Reasonable safeguards should protect personal data against such risks as loss or unauthorized access, use, destruction, modification, or disclosure. | • CP5: Notification of Misuse or Breach<br>• CT2: Authentication of Consumers<br>• CT4: Limitations on Identifying Information<br>• CT6: Security and Systems Requirements<br>• CT7: An Architecture for Consumer Participation |

| CORE POLICY PRINCIPLES | MARKLE COMMON FRAMEWORK FOR NETWORKED PERSONAL HEALTH INFORMATION PRACTICE AREAS |
|---|---|
| 8. **Accountability and oversight:** Entities in control of personal health information must be held accountable for implementing these principles. | • CP4: Chain-of-Trust Agreements<br>• CP5: Notification of Misuse or Breach<br>• CP6: Dispute Resolution<br>• CP9: Enforcement of Policies<br>• CT3: Immutable Audit Trails |
| 9. **Remedies:** Remedies must exist to address security breaches or privacy violations. | • CP5: Notification of Misuse or Breach<br>• CP6: Dispute Resolution<br>• CP9: Enforcement of Policies |

## Appendix B

Consumers as Network Participants: Explains why consumer participation can be transformative in health care as it has been in other sectors; why networked personal health records (PHRs) are a vital tool to empowering consumers, and how policies can help guide an emerging industry.

CP1: Policy Overview: Describes the policy landscape, including how the Health Information Portability and Accountability Act (HIPAA) as well as state and contract laws apply to emerging consumer data streams. Explains unregulated and regulated areas of the current environment, and argues for a voluntary common framework of policies.

CP2: Policy Notice to Consumers: Recommends preferred practices for giving consumers access to the policies for collection, use, and disclosures of personal health information, including privacy and security practices, terms and conditions of use, and other relevant policies.

CP3: Consumer Consent to Collections, Uses, and Disclosures of Information: Describes mechanisms to capture the consumer's agreement prior to any collection, use, or disclosure of personal data; explains why notice and consent are not sufficient by themselves in providing adequate protection for consumers.

CP4: Chain-of-Trust Agreements: Describes the merits and limitations of contractual mechanisms among parties exchanging personal health information; recommends important limitations to place on unaffiliated third parties, including vendors, service providers, and others who receive personal data or de-identified data.

CP5: Notification of Misuse or Breach: Discusses what to do if something goes wrong. Recommends that consumers be individually informed if their personal information was, or is reasonably believed to have been, disclosed or acquired by an unauthorized person or party in a form that carries significant risk of compromising the security, confidentiality, or integrity of personal information.

CP6: Dispute Resolution: Recommends that consumers be provided a clear and logical pathway to resolve disputes such as over breach or misuse, data quality or matching errors, allegations of unfair or deceptive trade practices, etc.

CP7: Discrimination and Compelled Disclosures: Recommends policies to bar discrimination and "compelled disclosures," such as when the consumer's authorization for release of data is required in order to obtain employment, benefits, or other services.

CP8: Consumer Obtainment and Control of Information: Covers several areas to facilitate the consumer's ability to electronically collect, store, and control copies of personal health information, including requesting data in an electronic format, allowing for proxy access to an account, requesting amendments, or disputing entries of data. Also covers appropriate retention of information in inactive accounts, and consumer requests to "delete" data and terminate their accounts.

CP9: Enforcement of Policies: Raises the issue of how policies and practices should be enforced on the network; describes the pros and cons of several different enforcement mechanisms, including: enforcing current laws, amending and expanding HIPAA, creating new law to govern Consumer Access Services, encouraging self-attestation with third-party validation, and encouraging consumer-based ratings.

CT1: Technology Overview: Describes the complexity of emerging digital health data streams; explains how information can be combined to build revealing profiles of individuals; depicts how health care entities and consumer technology innovators operate under different cultures that can clash without basic rules of the road.

CT2: Authentication of Consumers: Provides a framework for establishing and confirming the identity of individual consumers so that they may participate on a network.

CT3: Immutable Audit Trails: Recommends that audit trails be a basic requirement of PHRs and supporting services; explains the value of providing consumers with convenient electronic access to an audit trail as a mechanism to demonstrate compliance with use and disclosure authorization(s).

CT4: Limitations on Identifying Information: Recommends strong limitations on disclosures of identifying data to third parties. Supports disclosures only of those data that are reasonably necessary to perform the limited function(s) to which the third parties are authorized. Provides a caveat about considering data "de-identified."

CT5: Portability of Information: Highlights the importance of the consumer's ability to export and import information in industry-standard formats as they become available.

CT6: Security and Systems Requirements: Provides a brief outline on basic security protections. Recommends continuous monitoring of industry practices and threats, as well as personnel training and strict policies regarding who can access consumer data, and consequences for security violations.

CT7: An Architecture for Consumer Participation: Provides a view on how Consumer Access Services can fit within the Connecting for Health approach to architecture for a Nationwide Health Information Network (NHIN).

# 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.