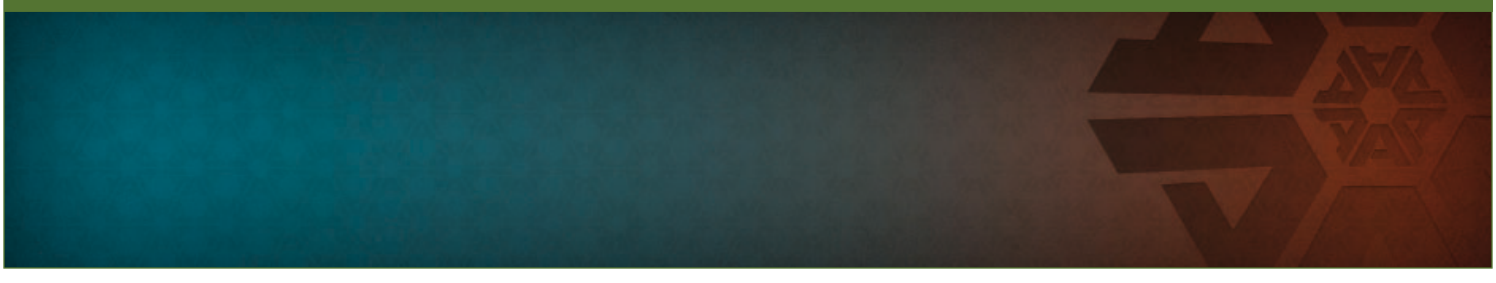
Markle Connecting for Health
Common Framework for Private and
Secure Health Information Exchange

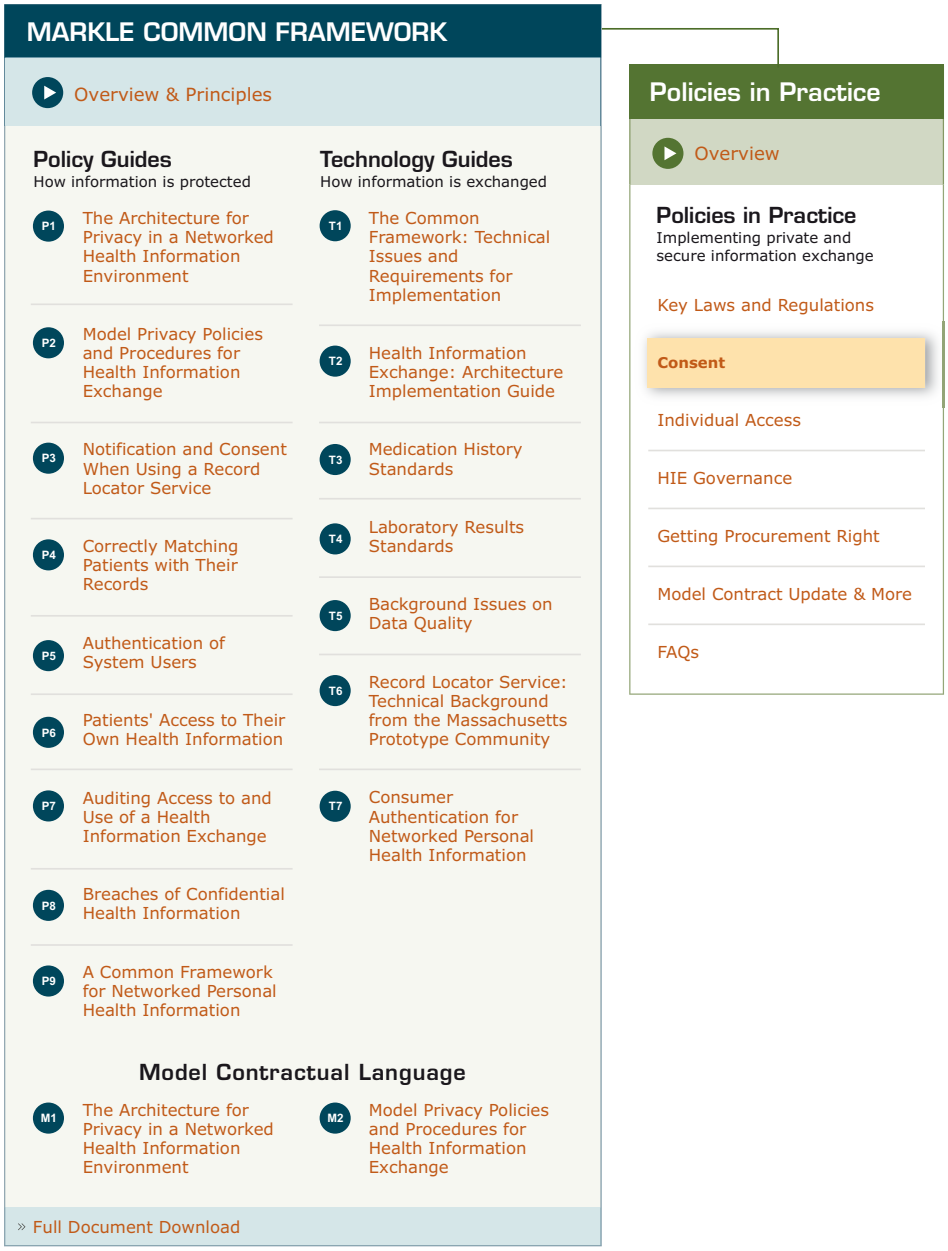
Policies in Practice

Consent: Implementing the Individual Participation and Control Principle in Health Information Sharing

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

Consent: Implementing the Individual Participation and Control Principle in Health Information Sharing

I. Introduction

When building systems for electronic health information sharing, implementers face many tough questions. One of the most challenging involves whether—and if so, how—individuals should be provided with choices about permitting their personal health information to be made part of, or accessible through, the system. This is often the first issue implementers seek to resolve, but paradoxically, it is nearly impossible to resolve first or to resolve in a vacuum.

Providing individuals with meaningful and well informed choice about information sharing is completely dependent on several other attributes of information sharing—such as who can access the information, for what purposes, which security practices are in place, and how data holders are held accountable for their stewardship of data. Health information sharing efforts must consider the entirety of the circumstances of health information sharing and the way those circumstances affect the risks and benefits of information sharing. These issues must be decided before implementers can consider the issue of choice.

This Policies in Practice resource supplements the Markle Connecting for Health Common Framework for Private and Secure Health Information Exchange (Markle Common Framework). It is meant to provide implementation context for the Individual Participation and Control principle and suggest ways for health information sharing efforts to establish their own policies and best practices on this issue, including a sequence to inform consideration of consent policies. This resource benefits from the implementation experience and the legal and policy developments that have occurred since the Markle Common Framework was issued in 2006.

Markle Connecting for Health thanks Deven McGraw, Center for Democracy & Technology, 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.*

II. Background and Definition of Terms

Historically, frameworks for protecting privacy begin with Fair Information Practice Principles (FIPPs), established in the 1970s and still relevant today. Most U.S. privacy law today is based on FIPPs, as described in P1: The Architecture for Privacy in a Networked Health Information Environment. FIPPs continue to be the backbone for establishing workable privacy and security policies for all types of sensitive personal information.

As explained in more detail in P2: Model Privacy Policies and Procedures for Health Information Exchange, focusing on consent policy without addressing the other FIPPs often provides only very weak privacy protection in practice.[1] Relying on consent as the sole or most significant privacy policy shifts the burden of protecting health information to the individual, who then has only the option of saying "yes" or "no" to information sharing that may not be subject to a full complement of protective policies and practices. When individuals are provided with choices about electronic health information exchange, making those choices understandable and meaningful is dependent on implementation of policies that address all of the FIPPs. The decision to engage in health information sharing is not "is it opt-in or opt-out." Instead, the choice is more complex, ideally made with full transparency about how information will be shared and the risks and benefits that come with making the choice to—or not to—participate.

The Markle Common Framework articulates a robust complement of privacy principles originally based on FIPPs and the Organization for Economic Co-operation and Development (OECD) principles. In 2008, the federal Office of the National Coordinator for Health Information Technology (ONC) adopted its own set of FIPPs-based principles (the "The Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information") based in part on Markle's version.

The Markle Common Framework's nine FIPPs-based privacy principles are explained fully in P2: Model Privacy Policies and Procedures for Health Information Exchange and set forth below.

- *Openness and Transparency*: There should be a general policy of openness about developments, practices, and policies with respect to personal data. Individuals should be able to know what information exists about them, the purpose of its use, who can access and use it, and where it resides.
- *Purpose Specification and Minimization*: The purposes for which personal data is 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.

---

[1] See Markle Connecting for Health, "Beyond Consumer Consent," *Markle Foundation*. Last modified February 1, 2008. http://www.markle.org/publications/852-beyond-consumer-consent (accessed on February 22, 2012). It describes the dangers of singling out consent.

- *Collection Limitation*: Personal health information should only be collected for specified purposes, should be obtained by lawful and fair means and, where possible, with the knowledge or consent of the data subject.
- *Use Limitation*: Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified.
- *Individual Participation and Control*:
  - Individuals should have access to their personal health 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 change, 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 a denial;
    - Challenge data relating to them and have it rectified, completed, or amended.
- *Data Integrity and Quality*: All personal data collected should be relevant to the purposes for which they are to be used and should be accurate, complete and current.
- *Security Safeguards and Controls*: Personal data should be protected by reasonable security safeguards against such risks as loss, unauthorized access, destruction, use, modification or disclosure.
- *Accountability and Oversight*: Entities in control of personal health data must be held accountable for implementing these information practices.
- *Remedies*: Legal and financial remedies must exist to address any security breaches or privacy violations.

Ultimately, the goal of enacting a comprehensive set of privacy and security policies is to **build and maintain public trust** in electronic health information sharing. Health information sharing efforts must implement policies necessary to achieve the goals of exchange, thereby maintaining an environment of trust in their communities.

The Markle Common Framework Network Approach

For individuals, trust in health information sharing emanates from trust in their health care providers' legal and ethical duties to keep information confidential. A key recommended practice of the Markle Common Framework is that **decisions about what to share and when to share remain with the person or entity that has the relationship with the patient**.

The role of protecting privacy and security does not rest solely with policy. Technology also plays a critical role in enabling privacy by the way it is designed. The interdependence of policy and technology is a paradigm described in the Markle Common Framework.

For example, to achieve health information sharing, the Markle Common Framework describes a "network of networks" distributed approach where data does not have to be centralized in order to be shared. From a technology perspective, access to patient data involves an intentional two-step process. The requester:

1. Uses a record locator service index (RLS index) to find where the patient's data is located.
2. Makes the request for the patient's data, at which point the data holder determines how to respond.

Refer to P3: Notification and Consent When Using a Record Locator Service and T1: The Markle Common Framework: Technical Issues and Requirements for Implementation.

A hallmark of the RLS system is that the RLS index has no clinical data or metadata. The index has only demographic information and pointers to the location of the patient's information. This separation of clinical and demographic data is a technical requirement that was developed specifically to fulfill a policy objective: to leave decisions about what to share at the edges of the network with the entity that has the relationship with the patient rather than technical models where the decision about what to share is made centrally.

This structure leaves intact the foundation for trust in health information sharing, i.e. the relationship between the patient and health care provider. The data holder ultimately implements the patient's choices with respect to sharing information, consistent with law and policy, and the data holder's relationship with the patient.

III. Where and How to Start

Federal and State Law Compliance

As a threshold matter, health information sharing efforts must comply with federal privacy laws and the laws of the state in which they are located or doing business. The Health Insurance Portability and Accountability Act (HIPAA) does not require individual consent for many routine collection, use and disclosure of health information activities (defined as "treatment, payment and health care operations"), but several states impose consent requirements that apply to collection, use and/or disclosure of health information, some pertaining to all health information and some only to specific types of health information.[2] Further, federal regulations governing federally assisted substance abuse treatment facilities and governing certain educational institutions impose stricter consent requirements and may apply to some health care data holders.

Implementers will need to keep up to date with all relevant laws and regulations that apply to them. Relevant changes to HIPAA as amended by HITECH are covered in Key Laws and Regulations: Changes to the Markle Common Framework.<link to PiP that covers changes in law>. As federal regulators continue to respond to programmatic efforts (such as the Meaningful Use program) through the promulgation of regulations and policy guidance, implementers should also be aware of activities underway among relevant federal policy advisory bodies regarding health information sharing and their suggested policies and practices. In addition, key federal agencies with jurisdiction over consumer privacy have begun to suggest policy options and best practices that can inform health information sharing efforts.

For some health information sharing efforts, applicable state law will set explicit consent policy that must be followed. However, for some states there are no additional legal requirements requiring individual consent to be obtained. In either case, health information sharing efforts will need to determine whether to adopt a policy on consent that goes beyond what the law may require.

> **Jenny Smith, Louisiana Health Care Quality Forum**: Addressing consent is more complex than we expected it to be. We discovered many layers to state laws that surfaced technical and legal questions. For example, we learned that under Louisiana law, consumers have the right to consent. But, we needed to understand what that means. Does the law require consent to share the data or consent to use the data? Can we aggregate data in a health information exchange without individual patient consent or do we need consent before this data is aggregated? The process to address the complexity of this topic requires a very significant level of legal expertise, financial resources and time.

---

[2] Implementers should seek expert advice to determine which laws are applicable to them. Many health information privacy laws apply only to certain entities or certain types of information; further, a health care provider in one state likely will not be legally bound by health privacy laws in other states, even if that provider is receiving information across state lines.

Developing a consent policy based on FIPPs: A three-step process

Consent policy development:

- must account for other important technical and policy attributes of information sharing; and
- is effective only when considered within the entirety of the circumstances of exchange that occur in any particular health information sharing effort.

Consequently, setting effective policy on individual consent will be nearly impossible if the issue is taken up first, before the basic boundaries, objectives and model of information sharing have been established.

This Policies in Practice recommends a sequence for developing privacy and security policy:

1. **Initiate a policy-setting process based on sound governance principles.**
2. **Consider all of the FIPPs-based privacy principles together to develop a set of specific, baseline policies.**
3. **Address the FIPPs-based privacy principles of "Individual Participation and Control" and "Openness and Transparency" last when determining policies with respect to consent.**

Consent is last in the sequence above because this set of policies—what choices people will have and how they will exercise them—should only be made once the circumstances of the health information sharing and the other key data sharing policies are considered. Thus, its placement in the sequence reflects its innate dependency on other foundational policy decisions.

This sequence also describes a process that can be deployed to re-evaluate decisions on consent as circumstances change. Consent policy development is not a one-time process. Such policies must be revisited or refreshed from time to time, such as in response to changes in:

- law or policy,
- technology decisions (for example, an expansion of acceptable uses of the network or the addition of new technical functionalities), or
- the scope or purpose of information sharing.

The expectations of individuals about the uses of their data may also change over time based on increased participation in health information sharing by providers. Individuals may also change their data sharing preferences in response to changing life circumstances, for example health status or marriage status. Implementation at both the policy and technology levels needs to accommodate the ability for individuals to change their choices over time and have them prospectively honored.

IV. Sequencing of Decisions—Getting to the Details

Step 1: Initiate a Policy-Setting Process Based on Sound Governance Principles.

Coming to agreement on workable information sharing policies requires broad, objective and inclusive involvement from various participants and the public at large in order to get appropriate and relevant feedback and to secure early buy-in as well as ongoing support.

Public trust will occur through both sound policies and an inclusive process, which also includes having consumers at the decision-making table. For more information on policies and practices for trust and interoperability with meaningful consumer participation, see Governance of Health Information Sharing Efforts: Achieving Trust and Interoperability with Meaningful Consumer Participation. [<link to governance PiP>]

Step 2: Consider all of the FIPPs-based privacy principles together to develop a set of specific, baseline policies.

"Purpose Specification and Minimization" principle

Determining the purposes for sharing heath information is the critical first step in determining the appropriate data sharing policies that will accomplish those purposes. Many initiatives start by information sharing for individual treatment purposes only and limiting information sharing to those who are involved in the individual's treatment. Some initiatives broaden the permissible uses to include other lawful purposes for data sharing, such as for payment, operations, public health, and other research.

In addition, the types of entities permitted to participate in information sharing may broaden as the purposes for information sharing expand. Still other initiatives permit sharing for any lawful purpose without additional policy limitations.

Regardless of whether the permitted purposes for information sharing are broad or more confined, this information is part of the risk/benefit calculus for information sharing and will be critical to determining whether and to what extent individuals will have choices with respect to whether their information is part of or shared through a health information sharing effort.

"Collection and Use Limitation" principles

The minimization principle is reflected to some extent in the HIPAA "minimum necessary" standard and will likely vary depending on the purposes for which data is to be collected, accessed or disclosed. For example, the information needed in order to treat an individual who seems to be suffering from flu symptoms will be different from the information needed to report a case of the flu to public health authorities.

In the Markle Common Framework Policy Guide P2: Model Privacy Policies and Procedures for Health Information Exchange, SNO Policy 400 describes potential purposes for information sharing and policies for data minimization; SNO Policy 600 specifically addresses the policy of "minimum necessary."

Joe Heyman, solo gynecologist, Wellport Health Information Exchange Steering Committee member, Massachusetts: To start the consent policy conversation, we began by identifying what data would be available through the health information exchange. This took months. Ultimately, we decided that we would exchange the shared health summary or CCR. We had a lot of hearty discussion and conversation about whether to share just the CCR, or whether more information should be shared in addition to the CCR. For example, we debated whether we should include smoking status and alcohol use, and certain sensitive categories of information. There was a lot of discussion, which took time. But it was all with an eye toward how we were going to address consent. In addition to addressing what data would be shared, critical decisions were made about purpose specification and minimization including permitting use for only treatment and sharing demographic and clinical information. We decided to only permit users to view patient information when they were taking care of that patient. We explained these permitted uses to the patient when we sought consent. The consent form, which is presented to patients, details the purposes for use of the data and makes clear that the information won't go beyond the medical community, i.e., those providers directly involved in the patient's care.

Once participants have determined the permissible purposes for sharing of health information, policies and technology must be implemented to limit the collection and use of information to those purposes. Implementing the principle of collection and use limitations also includes establishing internal policies regarding which individuals and entities have the right to access information consistent with the permissible purposes. In P2: Model Privacy Policies and Procedures for Health Information Exchange, SNO Policy 400 describes the use and disclosure policies; SNO Policy 700 describes policies with respect to workforce, agents and contractors.

"Security Safeguards and Controls" principle

Once the policies are set regarding (i) permissible purposes for information sharing and (ii) collection and use limitations that are limited to those purposes, the next step is to consider the security policies and protocols that will support compliance with those policies. For example, participants in a health information sharing initiative can deploy technical tools like role-based access and audit logs to ensure access to information only by persons who are authorized to do so. Encryption can help protect information from theft or loss. Individuals will want to understand the reasonable security safeguards that will be in place to protect their information. P5: Authentication of System Users, P7: Auditing Access to and Use of a Health Information Exchange, and P8: Breach of Confidential Health Information provide examples of security policy issues to be addressed.

"Data Integrity and Quality" principle

The quality of health care depends on accurate health information. Accurately matching individuals with their health information is critical to maintaining data quality. Inaccurate health information can also adversely affect an individual's benefits and protections.

Does Consumer Control Lead to Incomplete Information?

Often, providers are concerned that patients may choose to withhold important information, and that without "complete" information the system will be less useful. In reality, however, complete information about any patient is an aspiration at best. No one can assume that any information derived from a fragmented delivery system used by patients over many years can ever provide an absolutely complete patient record, whether on paper or electronically.

Clinicians know well that in the analog world information is often missing. Sometimes patients withhold information from new providers until they establish a relationship. This basic paradigm will be true in the digital world as well. Using technology to override this, or any policy expectation that individuals may have, can quickly erode trust. <link to Markle CF policies on this> Giving individuals some informed control over how their information is shared is critical to building trust among patients and providers.

Within P2: Model Privacy Policies and Procedures for Health Information Exchange, see SNO Policy 300 ("Individual Participation and Control of Information Posted to the RLS"). In addition, implementers should consult T5: Background Issues on Data Quality, and P4: Correctly Matching Patients with Their Records for further assistance.

Providing individuals with a way to review and request corrections to their health information also can improve data integrity and quality. Policies regarding individual access to health data and requesting amendments to health data can be found at P6: Patients' Access to their Own Health Information and P2: Model Privacy Policies and Procedures for Health Information Exchange, SNO Policy 800 ("Amendment of Data").

"Accountability and Oversight" and "Remedies" principles

Privacy and security policies have little effect if violators are not held accountable for compliance failures. Employee training, privacy and security audits, and other oversight tools can help to identify and address violations and breaches by holding accountable those who violate privacy requirements and by identifying and correcting weaknesses in security systems. In addition, remedies must exist to help hold violators accountable and to make recompense to persons who are aggrieved by privacy violations.

Relevant model policies in P2: Model Privacy Policies and Procedures for Health Information Exchange include SNO Policies 100 ("Compliance with Law and Policy"), 700 ("Workforce Agents, and Contractors"), and 1000 ("Mitigation"); also relevant are P7: Auditing Access to and Use of a Health Information Exchange, and P8: Breach of Confidential Health Information.

Step 3: Address the FIPPs-based privacy principles of "Individual Participation and Control" and "Openness and Transparency" last when determining policies with respect to consent.

"Individual Participation and Control" principle

Once implementers have established policies defining the context for sharing information, including how individuals and entities will be held accountable for complying with such policies, implementers can meaningfully consider whether and how individuals should be provided with choices regarding information sharing.

Relevant model policies in P2: Model Privacy Policies and Procedures for Health Information Exchange include SNO Policy 300 ("Individual Participation and Control of Information Posted to the RLS"); P3: Notification and Consent When Using a Record Locator Service also provide details on consent policy when using a Record Locator Service model for health information exchange. This principle also addresses individual access to health information and the right to request an amendment.

Consent for Patient-mediated Exchange

This Policies in Practice focuses on whether and how to implement consent with respect to the sharing of electronic health information– typically among health care professionals, health care institutions like hospitals, and health plans.

However, the implementation of the Health Information Technology for Economic and Clinical Health (HITECH) is likely to facilitate even greater sharing of health information directly with and by patients. HITECH amended the HIPAA Privacy Rule to make it clear that patients have the right to receive an electronic copy of their health information when their health information is maintained in electronic form. Refer to Key Laws and Regulations: Changes to the Markle Common Framework. [link to legal update PiP]

In addition, the Meaningful Use program requires some affirmative sharing of health information with patients, and these requirements may increase in later stages of that incentive program. At present, the Department of Veterans Affairs, Centers for Medicare and Medicaid Services, Department of Defense, and an increasing number of private-sector entities are offering individuals the opportunity to view and download electronic copies of their health information. This capability can facilitate patient-initiated health information sharing.

Markle Connecting for Health has developed a set of consensus policies specifically for the download capability that build on the Markle Common Framework for Networked Personal Health Information. See also Individual Access: Connecting Patients with Their Information. [link to individual access PiP]

What Granularity of Choice to Offer?

Implementers deciding to provide individuals with choices regarding information sharing will need to consider how granular those choices should be. For example, choice can be "all in or all out" or at the more granular level, choice of health information sharing participation may be by individual provider or type of provider, or by type of data.

State and federal law varies with regard to requirements related to granularity. For example, some states require granularity on the level of individual choice because they require specific consent for certain types of information. Similarly, federal law requires explicit consent for substance abuse treatment data in some circumstances, and requirements enacted by Congress in 2009 provide individuals with the right to restrict disclosures to health plans. See Key Laws and Regulations: Changes to the Markle Common Framework. [link to legal update]

Other policy recommending bodies have called for more granular choice. For example, in Recommendations Regarding Sensitive Health Information, the National Committee on Vital and Health Statistics recommended that electronic health records have the capability to sequester or segregate data in specific sensitive categories. Relevant model policies in P2: Model Privacy Policies and Procedures for Health Information Exchange include SNO Policy 500 ("Information Subject to Special Protection") and SNO Policy 900 ("Requests for Restrictions").

Yet, there is a limit to how granular consent can be implemented in today's complex environment. Health information streams are complex and involve an ever-growing number of users. Even medical professionals are unlikely to understand the full scope of information sharing that occurs in day-to-day health care delivery. For example, CT1: Technology Overview (Appendix: A Data Flow Scenarios) follows the data trail of a single drug prescription, the most common clinical transaction. Just to put the pills in the bottle, under the "simple" scenario, there are 10 different electronic copies of the information stored in various databases.[3]

In addition, greater innovation and development of technology is needed to allow for consent at the more granular levels. ONC's Health IT Policy Committee conducted a hearing on consent technologies and concluded that promising models were in development, but not necessarily in widespread use. We may be years away from widely deployed, reliable solutions. In the meantime, policies on choice need to reflect both what is desirable and what can be accomplished. HHS is piloting more granular consent technologies.

---

[3] As another example, almost 150 different people (including doctors, nursing staff, X-ray technicians, and billing clerks) access at least part of a patient's health record during a single hospital visit, and that there are roughly 600,000 entities with the ability to access at least some part of a patient's information. Judy Foreman, "At risk of exposure: In the push for electronic medical records, concern is growing about how well privacy can be safeguarded," *Los Angeles Times*. Last modified June 26, 2006. http://articles.latimes.com/2006/jun/26/health/he-privacy26 (accessed on January 8, 2011).

But is it "Opt-in" or "Opt-out"?

Many discussions about consent policy options become focused on the sole question of whether health information sharing entities should require "opt-in" or "opt-out" by individuals.

Unfortunately, this paradigm is a gross oversimplification of the complex data sharing decisions that provide the foundation for policies on individual consent. It doesn't reflect how the context of data sharing can influence appropriate and effective consent policy.

Merely saying "opt-in" or "opt-out" says nothing about the context of data sharing. For example, providing individuals with choices based on whether or how much of their information can be accessed or queried, for what purposes, with what protections, whether and how its made available for sharing with other providers, and whether a database that contains copies or summaries of provider records is used is essential to consider and a much more complex decision than a binary choice.

In addition, "opt-in" or "opt-out" also says nothing about whether meaningful choice is provided or presented in a way that individuals understand.

The choice provided should be meaningful and understandable to individuals, including informing them about the data sharing practices and discussing the benefits and risks of participating or not participating. The federal Health IT Policy Committee recommended that individuals be provided with meaningful choice when their information is made accessible through certain types of exchange structures. The elements of meaningful choice include:

- Allows the individual advance knowledge/time to make a decision (e.g., outside of the urgent need for care.)
- Is not compelled, or is not used for discriminatory purposes (e.g., consent to participate in a centralized HIO model or a federated HIO model is not a condition of receiving necessary medical services.)
- Provides full transparency and education (i.e., the individual gets a clear explanation of the choice and its consequences, in consumer-friendly language that is conspicuous at the decision-making moment.)
- Is commensurate with the circumstances (i.e., the more sensitive, personally exposing, or unexpected the activity, the more specific the consent mechanism. Activities that depart significantly from patient reasonable expectations require greater degree of education, time to make decision, opportunity to discuss with provider, etc.)

- Must be consistent with reasonable patient expectations for privacy, health, and safety;
- Must be revocable (i.e., patients should have the ability to change their consent preferences at any time. It should be clearly explained whether such changes can apply retroactively to data copies already exchanged, or whether they apply only "going forward.")

The Appendix includes a brief description of how the Committee's recommendations are consistent with the Markle Common Framework.

Joe Heyman, solo gynecologist, Wellport Health Information Exchange Steering Committee member, Massachusetts: In our consent process, we knew it would be critical for individuals to understand both the benefits and risks of participation as part of the consent process. In my practice, we describe to patients the potential benefits of participation in any health information sharing network or infrastructure:

- The potential for providers to be able to access information about you in advance of a visit, including but not limited to emergencies;
- Possible elimination of duplicate tests or office visits;
- Ability to update information more easily;
- Greater ability to obtain copies of your health information, or information about loved ones.

Potential risks of participation in any health information sharing network or infrastructure may include:

- Although the information is protected with security controls and participation is limited to treating providers, it is possible that someone with whom you would not want to share information may see or infer something about your health from your records.
- Information disclosed to other providers with your consent may be subject to different laws and policies when it is incorporated into the records of other providers.
- Your record may contain errors that are then shared with other members of the medical community.
- Though unlikely, unauthorized electronic access to large health care databases may occur.

"Openness and Transparency" principle

In order to achieve this principle, individuals must be advised how their health data can be accessed, used and disclosed in a way that is easy to read, understandable, and brief—a difficult challenge indeed. Often consent forms err on the side of trying to cover everything. But sacrificing brevity often means a long document that individuals do not understand or do not have time to digest. Forms that err on the side of brevity risk providing individuals with insufficient information to prepare them to make a meaningful choice about information sharing.

Blanket consent forms that provide little real information about actual data sharing, its specific purposes and information uses do little to protect an individual's privacy.[4] Recent reports from FTC[5] and the Department of Commerce[6] also discuss the ongoing challenges of providing full transparency to individuals about data practices and consent rights and the importance of clear and understandable communication with the public.

Openness and transparency about data sharing is essential for trust even in circumstances where explicit consent of the individual is not required or sought as a matter of policy. Individuals should never be surprised about what happens to their health information. The absence of a consent policy or requirement should never be interpreted as permission for information sharing that is beyond what individuals would reasonably expect.

Layered Notice

A promising way to achieve the balance between readability and full transparency is to provide "layered notice." In a "layered notice" approach, individuals are provided with a brief statement of the essential data sharing elements, with the ability to link to (or otherwise easily obtain) more details.

The Markle Common Framework for Networked Personal Health Information includes recommendations for how to fulfill the openness and transparency principle with respect to consumer-based health tools that may be instructive for implementing patient choice with respect to health information sharing. For example, it recommends that general consent be sought initially, when the consumer first voluntarily signs up for the service. Such consent would cover the uses of health information that are consistent with consumers' reasonable expectations in signing up for the service, such as routine maintenance or uses necessary to facilitate opening

---

[4] See Markle Connecting for Health, "Beyond Consumer Consent," *Markle Foundation*. Last modified February 1, 2008. http://www.markle.org/publications/852-beyond-consumer-consent (accessed on February 22, 2012). It discusses the dangers of overreliance on consent and blanket consent.

[5] "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).

[6] "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework," *The Department of Commerce*. http://www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf (accessed on February 22, 2012).

the account. However, independent specific consent should be sought for uses that would not be reasonably expected or involve more sensitive data, as described in CP3: Consumer Consent to Collections, Uses, and Disclosures of Information. The Federal Trade Commission's (FTC) report, Protecting Consumer Privacy in an Era of Rapid Change, also recommends that companies seek independent consent for data uses that go beyond consumers' reasonable expectations (see pages 76-77).

In addition, the FTC report, Protecting Consumer Privacy in an Era of Rapid Change (pages 52–79) sets out recommendations for how to make consent (particularly on the Internet) more understandable and meaningful to individuals. This information may be helpful to implementers who deploy on-line mechanisms for securing patient consent.

Even when the consent form follows the recommended layered notice approach, openness and transparency can rarely (if ever) be effectively achieved solely through written documentation. Individuals must be able to discuss these issues with the providers they trust (or their staff); the written documentation can provide the back-up support for that conversation, offering links to more details and providing the necessary proof, in circumstances where affirmative consent is required to be obtained in advance, that the individual has provided that consent.

Gina Perez, Delaware: We take a multi-pronged approach to informing patients about the Delaware Health Information Network (DHIN). We give a toolkit to the providers that includes information they need to educate their patients. We emphasize the importance of the patient-provider relationship to building trust in health information sharing. We have an informative website and brochures for provider offices. The provider offices also have stickers for their window that say, "We proudly participate in the DHIN". Each practice also receives talking points for the staff to use with their patients. With all that being said, it's at the point of care that patients learn about the DHIN. When a patient walks into a provider's office, the provider's office may have brochures and the sticker. Some doctors actually say, "You know, I'm looking at your information. It came from the Delaware Health Information Network. I'm seeing this lab that you had done by Dr. Smith", and they'll then speak to the patient about the DHIN.

Conclusion

Determining policies around individual consent is often a significant policy challenge for implementers. But it can be addressed effectively if done within the context of the full complement of policies that govern information sharing.

Before establishing consent policies, implementers should first work to set the basic parameters of information sharing, such as, who can access and use health information and for what purposes, what basic security measures are followed, and how participants are held accountable. Once these issues have been addressed, implementers can consider the issue of choice.

Appendix

The HITPC Tiger Team Recommendations are consistent with the Markle Common Framework.

- Policy choices on consent may vary depending on the circumstances. The Health IT Policy Committee, in work initiated by its Privacy and Security Tiger Team, recognized that the foundation of trust in health information exchange is the patient-provider relationship; they subsequently recommended that point-to-point exchange between providers should not necessarily require additional consent (beyond what current law might already require) just because the exchange of information is electronic. However, before setting policy on consent, the Policy Committee had already assumed an exchange environment that involved only exchange for treatment, public health and aggregate quality reporting for meaningful use stage 1. The Committee also recommended clear limits on how intermediaries who help facilitate the exchange of health information, can access, use and disclose that data. This helped the Committee to conclude, with confidence, that individual consent would not be required in this set of circumstances. (They noted, however, that not requiring consent did not eliminate the responsibility for openness and transparency about data sharing practices with patients.)

- The Policy Committee did recommend that additional, meaningful consent should be provided if an individual's health information is shared in ways that they would not reasonably expect, or that subject their data to being accessed without the intervention of their trusted providers. Examples offered were a centralized health information sharing entity, where the patient's data is sent to, and accessible from, a centralized database, or some federated models where the data can be accessed from the provider's records (such as through an edge server) without an individualized decision to disclose being made by the patient's provider. In these circumstances, the context for sharing data had changed – and therefore the Committee reasoned that individuals should have some meaningful choice before their information would be included in those types of exchange arrangements.

Health IT Policy Committee recommendations consistent with the Markle Common Framework.

- The federal Health IT Policy Committee addressed consent in 2010, starting with two core values:

    1. the trust individuals typically place on their providers to be good stewards of their health information, and

    2. that individuals should not be surprised to learn about how their information is shared.

The Committee determined that merely digitizing the type of provider-to-provider information exchange that occurs today on paper need not require additional consent beyond what may be required by law. This is particularly the case when the purposes for information sharing are limited to those the individual or patient would reasonably expect, like treatment, care coordination, and sending information to payers for billing purposes.

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.