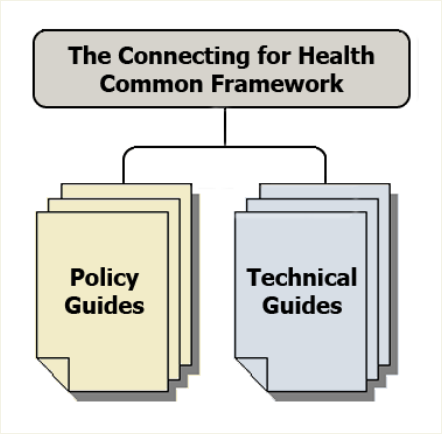

Americans are eager to see the cost and quality improvements that will result from health information technology.

A coordinated and common information policy framework is critical to the success and sustainability of health IT efforts.

Privacy is a critical enabler of information sharing and health IT adoption.

Our approach to privacy must reflect the evolving market and health care environment.

The Connecting for Health Common Framework provides a flexible 21st century privacy approach, articulating clear national expectations for health IT:

- Core privacy principles
- Sound network design
- Oversight and accountability

Both public and private entities will have a role in implementing and using such a framework.

Connecting for Health Policy Brief: September 2008

We need a 21st century privacy approach allowing Americans to protect and share health information to improve quality

Americans are eager to see the cost and quality improvements that will result from health information technology (health IT). Improving health care quality is dependent on health IT to enable information sharing. Information must be shared to improve continuity of care, enable robust decision support tools for providers and patients, and support e-prescribing systems that alert physicians to harmful drug interactions. We urgently want and need these developments and they are within our reach.

Privacy is a critical enabler of information sharing and health IT adoption. It is clear that Americans are eager to reap the benefits of health IT if appropriate safeguards are in place to protect their personal information. We need to earn and keep the public's trust that personal health information will be protected as it is shared.

Our approach to privacy must reflect the evolving market and health care environment. We need a 21st century privacy approach that establishes common information policy expectations. The expectations apply broadly to the myriad of health IT efforts from e-prescribing to health information exchange (HIE) and drug safety reporting and to the many and evolving entities sharing health information.

The Connecting for Health Common Framework provides a 21st century privacy approach. Since 2002, the Markle-led Connecting for Health collaborative has brought together key organizations from all sectors to develop a common approach to information policies.

Our Common Framework[1] articulates clear national expectations for health IT in three areas, summarized in this brief:

1. **Core privacy principles**
2. **Sound network design**
3. **Oversight and accountability**

The Common Framework can be used by any health IT effort to think through critical information policy issues. It provides consistent policies for disparate health IT activities while allowing flexibility to tailor specific practices (e.g., patient consent, breach notification, or audit practices) to the demands of specific health IT uses.

Implementation of this framework is possible today. It has been adopted by providers, e-health companies and HIE entities across the country to foster trusted information sharing.

[1] See www.connectingforhealth.com

Both public and private entities will have a role in implementing and using such a framework. The shared framework will foster public trust, an investment as significant as standards for advancing information sharing.

- **Federal policymakers –** Can make the key attributes of the framework a condition of any federally-funded health IT effort.
- **State policymakers –** Can build the framework into all state procurement and state health IT roadmaps.
- **HIE entities** – Can require that all participants satisfy the key attributes of framework.
- **Private industry** – Can adopt policies and build information-protective technology tools into products and business relationships.
- **Consumer groups** – Can use the framework to track and monitor health IT developments and evaluate policy proposals.

In the context of federal health IT initiatives, Congress, Federal agencies and participants would all use the framework, but in different ways.

- Congress would use the framework to "set the bar," establishing the broad expectations for any health IT effort without detailing one-size-fits-all national policies.
- Agencies would use the framework to develop the policies and rules for any health IT effort, tailored to the specifics of the initiative envisioned.
- Participants, including recipients of federal grants, would be required to document how they would achieve the elements of the framework.

1. Core Privacy Principles

Health IT efforts must be built around the core privacy principles that protect information and enhance trust

- The nine core privacy principles are: *openness and transparency, purpose specification, collection and use limitation, individual participation and control, data integrity and quality, security safeguards and controls, accountability and oversight, and remedies.*
- The principles require that limits be set on data collection and use, that patients have access to and reasonable control over their health information, and that security safeguards be adopted.
- Health IT initiatives must achieve privacy protection through both policy and technology tools.
- No one principle, including individual control or consent, is adequate on its own. Meaningful safeguards are achieved by applying these principles together. Applying some and not others can weaken the overall approach.

Connecting for Health Common Framework Requirements

CORE PRIVACY PRINCIPLES – Every information-sharing effort must provide:

Openness and Transparency
- Communicate policies to participants and individuals
- Provide privacy notices to consumers
- Involve stakeholders in developing information sharing policies

Purpose Specification
- Specify the purpose of the data collection effort clearly and make it narrowly suited to the need

Collection Limitation and Minimization
- Assure that only data needed for specified purposes are being collected and shared

Use Limitation
- Establish processes to ensure that data are only used for the agreed upon and stated purposes
- Establish what data access is permitted for each user

Individual Participation and Control
- Allow individuals to find out what data have been collected and who has access, and exercise meaningful control over data sharing
- Give individuals access to information about them, and the ability to request corrections and see audit logs

Data Integrity and Quality
- Provide that data are relevant, accurate, complete and up-to-date

Security Safeguards and Controls
- Establish tools and mechanisms to provide that data are secured against breaches, loss or unauthorized access
- Establish tools and approaches for user authentication and access

Accountability and Oversight
- Establish who monitors compliance with policies and procedures for handling breach
- Produce and make available audit logs

Remedies
- Establish mechanisms for complaints
- Establish remedies for affected parties to compensate for harm caused by breach

2. Sound Network Design

Health IT efforts should use sound network design that protects information while it is shared

- Health IT efforts should enable information sharing or "interoperability"—supporting many applications and using secure, open web standards.
- The internet is the network and is independent of actual applications. The "NHIN", or any health information exchange, is not a new network, but rather a way of using the existing Internet for private and secure health information exchange based on a set of common policies, standards and practices.
- Information need not be centralized in order to be shared.
- Data should stay as close as possible to where it's captured, and shared as needed.

3. Oversight and Accountability

Health IT efforts must establish oversight and accountability, including critical governance and enforcement mechanisms

- A consistent framework and appropriate oversight and accountability mechanisms will empower industry to innovate and experiment within clear parameters.
- A policy framework is only effective if it is subject to mechanisms that enforce it. The needed structures and processes to assure oversight and accountability cannot be developed in a "one-size-fits-all" fashion and applied across all efforts. Rather, they will need to be thought through and specified based on the needs and scope of the particular initiative. Some uses of health IT will lend themselves to contractual enforcement within the parameters of existing state and federal laws; others will require a combination of mechanisms, some existing and some new, to establish adequate oversight and accountability.
- Governance models should anticipate future participants who may collect, transport or otherwise use patient data and be readily adaptable to evolving business models.

Connecting for Health Common Framework Requirements

SOUND NETWORK DESIGN – Every information sharing effort must:

- **Incorporate technical tools that facilitate trusted use**: audit, access, authorization, authentication and accuracy
- **Promote technological choices that limit the potential for abuse and mitigate risks of large breaches**, including distributed architecture
- **Focus on interoperability and flexibility**, supporting a diversity of applications
- **Use secure, open web standards** that facilitate information sharing

OVERSIGHT & ACCOUNTABILITY – Every information sharing effort must:

- **Have inclusive participation of all affected** in the development of approaches and policies
- **Have processes, responsibility and timelines for ensuring that the framework and its attributes are adopted**
- **Include clear mechanisms of enforcement for the information policies** that are appropriate to the specific activity, such as contractual agreements in the case of information exchange activities or government oversight in the case of government-funded initiatives
- **Designate responsibility for monitoring and oversight against the framework**, including effective enforcement and accountability to stakeholders