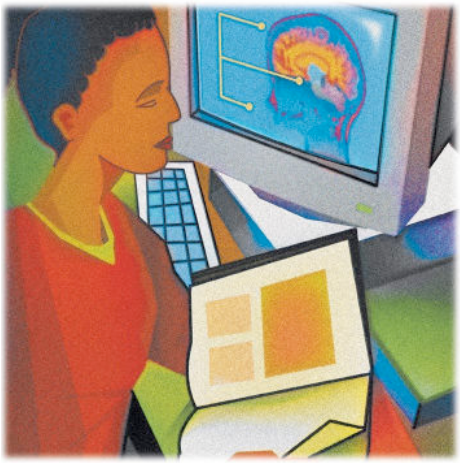
CENTER FOR DEMOCRACY & TECHNOLOGY



Connecting for Health Policy Brief: February, 2008

Beyond Consumer Consent: Why We Need a Comprehensive Approach to Privacy in a Networked World

A privacy approach that rests solely on obtaining consumer consent can provide weak protection for consumers.

A complementary package of privacy and security polices—rooted in Fair Information Practices—is needed to provide meaningful protection to consumers.

The policies needed are practical and common sense. They address setting limits on data collection and use, ensuring patients' access to information, and providing rigorous user authentication and other appropriate mechanisms to address data security and breach.

Consumer consent has long been seen as the privacy pillar for networked health information.

But a privacy approach that rests solely on obtaining consumer consent can provide weak protection for consumers. While consumers should be informed about and agree with how health information is being collected and used, consent alone cannot be a substitute for a comprehensive approach to privacy that protects consumers and builds trust.

A complementary package of privacy and security polices—rooted in Fair Information Practices—is needed to provide meaningful protection to consumers. Fair Information Practices are the interrelated principles to protect privacy used worldwide since 1973 (see *core privacy principles* on page 2 of this brief).

The policies needed are practical and common sense. They address setting limits on data collection and use, ensuring patients' access to information, and providing rigorous user authentication and other appropriate mechanisms to address data security. It is critical that they be applied as a cohesive package, as applying some and not others can have the unintended consequence of weakening the overall approach.

Technology approaches can also protect privacy by minimizing the risks of data spills. Distributed models of information sharing do not require the creation of large-scale databases, and thus reduce the risks of unintended disclosure or breach. These distributed models leave information in the hands of entities that have a direct relationship with the patient, allowing it to be shared with authorized parties when needed.

Using a comprehensive approach to privacy means that consumer consent does not have to bear the full weight of privacy protection. When the full array of privacy policies is put in place to protect information, different approaches to consent might emerge. For example, "opt-out" consent might be appropriate when offered in conjunction with an easy-to-use audit function that allows consumers to monitor and adjust who is accessing their information.

Relying on consumer consent without a broader framework of privacy policies and technology can have unintended consequences.

- **Consent to what?** Consumers can only provide meaningful consent when they are fully informed about what information is being collected, under

CENTER FOR DEMOCRACY & TECHNOLOGY

what circumstances it will be shared, and how it will be protected, as established in the other necessary information policies.

- **Weaker consumer protections.** Relying solely on consent places an unfair burden on consumers—and overlooks the importance of systems, rules, and processes—to protect and safeguard personal health information.
- **"All or nothing" blanket consents.** Placing too much reliance on consent often leads to the use of comprehensive blanket consents. These mechanisms offer consumers "all-or-nothing" choices and little meaningful ability to control how they want to share information, and with whom, over time.
- **Reduced use of privacy-protective technology.** The use of one-time blanket consents as an isolated approach to privacy can have the unintended consequence of creating a sense of immunity for the many holders of a patient's data, reducing their motivation to address the full complement of Fair Information Practices, and diminishing their demand for privacy-protective technologies and services.

A comprehensive approach to privacy will yield tangible rewards. A clear policy framework integrating all the principles outlined below will provide guidance to groups participating in information exchange and meaningful protection to consumers. It will also have marketplace benefits; stimulating innovation, stabilizing risk for new entrants, and providing greater market certainty for investment.

Core Privacy Principles – derived from Fair Information Practices

Openness and Transparency (Is it easy to understand what policies are in place, how they were determined, and how to make inquiries or comment? Is it clear who has access to what information for what purpose?)

Purpose Specification and Minimization (What is the purpose of gathering these data? Are the purposes narrowly and clearly defined?)

Collection Limitation (Are only those data needed for the specified purposes being collected, and are subjects fully informed of what is being collected?)

Use Limitation (Will the data only be used for the purposes stated and agreed to by the subjects?)

Individual Participation and Control (Can an individual find out what data has been collected and exercise control over whether and with whom it is shared?)

Data Integrity and Quality (How are the data kept current and accurate?)

Security Safeguards and Controls (How are the data secured against breaches, loss, or unauthorized access?)

Accountability and Oversight (Who monitors compliance with these policies? How is the public informed about violations?)

Remedies (How will complaints be handled? Will consumers be able to respond to or be compensated for mistakes in decisions that are based upon the data?)

__Connecting for Health__ is a collaborative of more than 100 leading private and public organizations including experts in clinical medicine, information technology, public policy, and patient privacy. The collaborative is led by the Markle Foundation and funded by both Markle and the Robert Wood Johnson Foundation.

WANT MORE DETAILS? SEE:

Connecting for Health
Common Framework: Resources for Implementing Private and Secure Health Information Exchange

Policy Guides

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

P5: Authentication of System Users

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

Technical Guides

T1: The Common Framework: Technical Issues and Requirements for Implementation

Find these and other policy and technical resources at:
www.connectingforhealth.org