Privacy and Security Standards

Walter G. Suarez, MD, MPH
Director, Health IT Strategy, Kaiser Permanente
Past President, Public Health Data Standards Consortium
Section A: overview: basic concepts and underlying realities

Section B: privacy of health information, part 1
  - Framework
  - Current practices

Section C: privacy of health information, part 2

Section D: health information security
  - Framework
  - Current practices
Section A

Overview: Basic Concepts and Underlying Realities
HITSP Standards Categorization

1. Information exchange standards
   - E.g., messaging standards

2. Information content standards
   - E.g., reference information models (RIMS)

3. Data standards (vocabularies and terminologies)

4. Identifiers standards
   - E.g., provider, plan, individual

5. Privacy and security standards

6. Functional standards
   - E.g., workflow/dataflow standards

7. Other
   - E.g., IT standards
Basic Concepts

- What is *privacy* (of health information)?
  - An individual's (or organization's) right to determine whether, what, when, by whom and for what purpose their personal health information is collected, accessed, used or disclosed

- What is *security* (of health information)?
  - A defined set of administrative, physical and technical actions used or taken to protect the confidentiality, availability and integrity of health information

Source: HITSP vocabulary—modified and expanded from 45 CFR 164.304.
Health Information Privacy and Security: Realities

- Medical records are among the most sensitive information about a person

- Health care is an information-driven field
  - Everything about the health care system involves information
  - Information is much more complex than other industries (amount, type, frequency)

- Health information is central to the doctor-patient relationship

- Privacy and security of health information are central to the doctor-patient relationship
Health Information Privacy and Security: Realities

- Health care is a complex system when it comes to health information
  - Many actors (patient, provider, health plan, employer, government, public health, researchers, vendor, etc.)
  - Various types of information (demographic, clinical, financial)
  - Many processes related to health information (collection, creation, maintenance, access, use, disclosure)
  - Different purposes (treatment, payment, operations, public health, research, judicial, legal, etc.)
  - Many places where health information resides
  - Lack of common identifiers and other standards
Health Information Privacy and Security: Realities

- Many laws
  - Federal laws: include HIPAA, Privacy Act, Education Records Law, Mental Health Records Laws, Public Health information laws
  - State laws: patchwork of varying types and levels of state privacy laws; few address health privacy and security in a comprehensive fashion

- Different policies and practices created and used by organizations
  - Many go above and beyond what federal/state laws require
Increasing complexities
- Expanded use of electronic health records
- Increased electronic communications between patients and the health care system (i.e., Web sites, email)
- Electronic networks (Regional Health Information Exchanges, NHIN)
- Evolving personal health records
Federal Agencies Work: Office for Civil Rights

Source: www.hhs.gov/ocr
The Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information

The principles of the Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information establish a single, consistent approach to address the privacy and security challenges related to electronic health information exchange through a network for all persons, regardless of the personal or organizational exchange. The goal of this effort is to establish a policy framework for electronic health information exchange that can guide the nation’s adoption of health information technologies and help improve the availability of health information and health care quality. The principles have been designed to establish the roles of individuals and the responsibilities of those who hold and exchange electronically identifiable health information through a network.

- The Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information (PDF - 821K)

The Health IT Privacy and Security Toolkit

As part of a Privacy and Security Toolkit to implement the Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information (Privacy and Security Framework) the Office of the National Coordinator for Health Information Technology (ONC) and the Office for Civil Rights (OCR) developed a number of materials and guidance, respectively. The Privacy and Security Toolkit includes:

- Draft Model Personal Health Record (PHR) Privacy Notice & Facts At A Glance
- HIPAA Privacy Rule Guidance Related to the Privacy and Security Framework and Health IT

Source: www.hhs.gov/healthit
Advisory Committees

SUBCOMMITTEE ON PRIVACY, CONFIDENTIALITY AND SECURITY

Charge

The Subcommittee on Privacy, Confidentiality and Security monitors major developments with regard to health information privacy, confidentiality and security on behalf of the National Committee on Vital and Health Statistics, and identifies issues and opportunities for investigation. The Subcommittee also makes recommendations to the full Committee and assists the Department in its administration of the privacy and security provisions of the Health Insurance Portability And Accountability Act Of 1996 (P.L. 104-191).

Privacy & Security Tiger Team

The Office of the National Coordinator for Health IT (ONC) has organized a workgroup (subcommittee) under the auspices of the HIT Policy Committee to move forward on a range of privacy and security issues. A new Privacy & Security Tiger Team (composed of members from the HITPC and the HITSC, as well as NCVHS) will work over the next few months to address the requirements of HITECH and the needs of many new organizations created under that law. We expect the work of the Tiger Team to be completed by late fall 2010.

Privacy & Security Standards Workgroup

The Privacy & Security Standards Workgroup will make recommendations to the HIT Standards Committee on privacy and security requirements that should be included in standards, certification criteria, and implementation specifications.

Specific Charge

- Make recommendations to the HIT Standards Committee on specific privacy and security safeguards that should be included in the definition of Meaningful Use, with a specific focus on the eight (8) areas listed in Section 1102(b)(2)(B), within two (2) months of the workgroup's first meeting.

Beacon Community Highlights and Videos Now Available

Learn more about how ONC’s Beacon Communities are using Health IT to improve health care quality and efficiency in their communities.