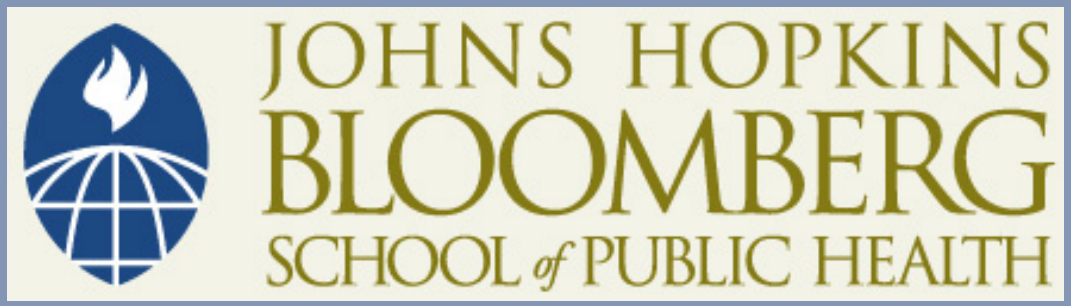
This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike License. Your use of this material constitutes acceptance of that license and the conditions of use of materials on this site.



Copyright 2011, The Johns Hopkins University and Walter Suarez. All rights reserved. Use of these materials permitted only in accordance with license rights granted. Materials provided “AS IS”; no representations or warranties provided. User assumes all responsibility for use, and all liability related thereto, and must independently review all materials for accuracy and efficacy. May contain materials owned by others. User is responsible for obtaining permissions for use from third parties as needed.

JOHNS HOPKINS
UNIVERSITY

Privacy and Security Standards

Walter G. Suarez, MD, MPH
Director, Health IT Strategy, Kaiser Permanente
Past President, Public Health Data Standards Consortium

Outline

- 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

JOHNS HOPKINS
UNIVERSITY

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

Health Information Privacy and Security: Realities

- 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

U.S. Department of Health & Human Services

HHS.gov *Improving the health, safety, and well-being of America*

Search | Search: OCR All HHS

HHS Home | HHS News | About HHS | Font Size | Print | Download Reader

Health Information Privacy

Office for Civil Rights | Civil Rights | Health Information Privacy

OCR Home > Health Information Privacy

HIPAA
- Understanding HIPAA Privacy
- HIPAA Administrative Simplification Statute and Rules
- Enforcement Activities & Results
- How to File a Complaint
- News Archive
- Frequently Asked Questions

PSQIA
- Understanding PSQIA Confidentiality
- PSQIA Statute & Rule
- Enforcement Activities & Results
- How to File a Complaint

Health Information Privacy

The Office for Civil Rights enforces the HIPAA Privacy Rule, which protects the privacy of individually identifiable health information; the HIPAA Security Rule, which sets national standards for the security of electronic protected health information; and the confidentiality provisions of the Patient Safety Rule, which protect identifiable information being used to analyze patient safety events and improve patient safety.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules

Learn about the Rules' protection of individually identifiable health information, the rights granted to individuals, OCR's enforcement activities, and how to file a complaint with OCR.

The Patient Safety and Quality Improvement Act of 2005 (PSQIA) Patient Safety Rule

Learn about the Patient Safety Rule's protection of confidential patient safety work product, the permitted disclosures of patient safety work product, OCR's enforcement activities, and how to file a complaint with OCR.

OCR Privacy Listserv

Learn more about the Privacy Rule! Sign up for the OCR Privacy Listserv.

What's New
- Psychotherapy Notes & Testing Data Study
  - in Chicago, IL on Oct.7th - 09/07/10
  - in Los Angeles, CA on Nov.18th - 10/15/10
- Breach Notification Final Rule Update - 7/28/10
- Resolution Agreement with Rite Aid Corporation - 7/27/10
- Risk Analysis Final Guidance - 7/14/10
- HITECH Notice of Proposed Rulemaking - 7/08/10
- Updated Web Page: Posted Breaches Affecting 500 or More Individuals - 7/08/10
- HITECH Accounting of Disclosures Request for Information - 5/03/10
- OCR & NIST: HIPAA Security Conference, May 11th & 12th, Conference Presentations - 3/18/10
- HITECH Act Rulemaking and Implementation Update - 03/15/10
- Workshop on the HIPAA Privacy Rule's De-Identification Standard, March 8-9, 2010. View the web cast - 03/19/10

Source: www.hhs.gov/ocr

Federal Agencies Work: ONC

U.S. Department of Health & Human Services — www.hhs.gov

The Office of the National Coordinator for Health Information Technology

Search GO

Get email updates | Follow us on | Contact us

- Health IT Home
- HITECH & Funding Opportunities
- HITECH Programs
- Federal Advisory Committees
- Regulations & Guidance
  - ONC Regulations FAQs
  - Meaningful Use
  - Privacy and Security
    - » Privacy & Security Framework
    - Anti-fraud
    - HIPAA & Health IT
    - State-Level Resources
    - Model PHR Privacy Notice
    - Medical Identity Theft
    - Federal Laws and Regulations
  - Standards and Certification
- ONC Initiatives
- Outreach, Events, & Resources
- About ONC

Home > Regulations & Guidance > Privacy and Security > Privacy & Security Framework

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 below 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 legal framework that may apply to a particular organization. The goal of this effort is to establish a policy framework for electronic health information exchange that can help 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 electronic individually identifiable health information through a network.

- The Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information [PDF – 80K]

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
- Reassessing Your Security Practices in a Health IT Environment: A Guide for Small Health Care Practices (PDF)
- HIPAA Privacy Rule Guidance Related to the Privacy and Security Framework and Health IT

Feature

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.

Quick Links

- ATCBs
- HITECH Programs
- Certification Programs
- Privacy & Security
- Meaningful Use
- HIT Policy Committee
- HIT Standards Committee

Source: www.hhs.gov/healthit

Advisory Committees