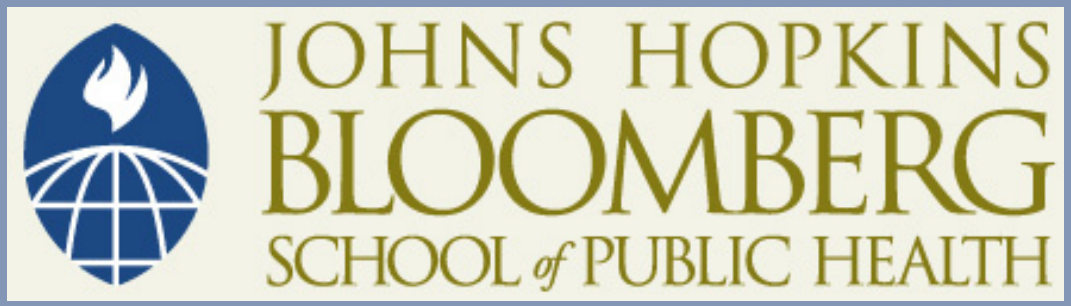
This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike License. Your use of this material constitutes acceptance of that license and the conditions of use of materials on this site.



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

Section B

Health Information Privacy, Part 1

Privacy of Health Information: Current Practices

- HIPAA has generally defined the floor for uses and disclosures of health information

- HIPAA did not require "consent" for uses or disclosures related to treatment, payment, and health care operations
  - "Authorization" required for other specific uses and disclosures

- HIPAA does *not* define requirements for:
  - Electronic consent
  - Granularity of consumer controls
  - Electronic health information exchanges
  - Personal health records

Privacy of Health Information: Current Practices

- HIPAA has generally defined the floor for uses and disclosures of health information

- HIPAA did not require "consent" for uses or disclosures related to treatment, payment, and health care operations
  - "Authorization" required for other specific uses and disclosures

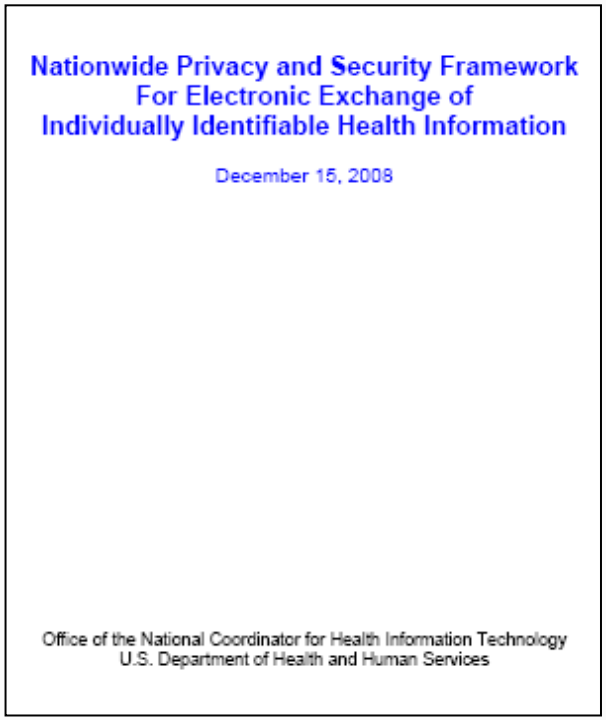
- HIPAA does *not* define requirements for:
  - Electronic consent
  - Granularity of consumer controls
  - Electronic health information exchanges
  - Personal health records

Privacy of Health Information: Current Practices

- Other federal laws define specific use and disclosure requirements (over and above HIPAA) for specific types of data (i.e., substance abuse, mental health, lab data, education records)
- There are also program-specific privacy protection requirements (such as Medicare, Medicaid, SCHIP)
- Many state laws establish additional requirements when privacy consent is needed
  - Some even for treatment, payment, and operations
  - Still mostly silent about electronic consent, granularity, electronic health information exchanges, personal health records
- Existence of a national "framework" on health information privacy —but unenforceable

US Health Information Privacy and Security Framework

- Developed and released in 2008
- Purpose: to provide a clear, understandable, uniform set of principles to support a consistent and coordinated approach to privacy and security for organizations to adhere to and implement
- Document defines a set of principles to serve as a guide (non-enforceable) for public and private organizations
- References to federal laws and



Core Principles

- Individual access
  - Individuals should be provided with a simple and timely means to access and obtain their individually identifiable health information in a readable form and format

- Correction
  - Individuals should be provided with a timely means to:
    - Dispute the accuracy or integrity of their individually identifiable health information
    - Have erroneous information corrected
    - Have a dispute documented if their requests are denied

Core Principles

- Openness and transparency
  - There should be openness and transparency about policies, procedures, and technologies that directly affect individuals and/or their individually identifiable health information

- Individual choice
  - Individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use, and disclosure of their individually identifiable health information

Core Principles

- Collection, use and disclosure limitation
  - Individually identifiable health information should be collected, used, and/or disclosed only to the extent necessary to accomplish a specified purpose(s) and never to discriminate inappropriately

- Data quality and integrity
  - Persons and entities should take reasonable steps to ensure that individually identifiable health information is complete, accurate, and up-to-date to the extent necessary for the person's or entity's intended purposes and has not been altered or destroyed in an unauthorized manner

Core Principles

- Safeguards
  - Individually identifiable health information should be protected with reasonable administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure

- Accountability
  - These principles should be implemented, and adherence assured, through appropriate monitoring and other means and methods should be in place to report and mitigate non-adherence and breaches

Glossary

APPENDIX I: GLOSSARY

Administrative safeguards: Administrative actions, and policies and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic individually identifiable health information and to manage the conduct of the entity's workforce in relation to the protection of that information. Administrative safeguards include policies and procedures, workforce training, risk management plans, and contingency plans.

Collect/Collection: The acquisition or receipt of information, including individually identifiable health information.

Corrective measures: Actions taken to address a security breach or privacy violation, with the intent to counteract the breach or violation and reduce future risks.

Disclose/Disclosure: The release, transfer, exchange, provision of access to, or divulging in any other manner of information outside the person or entity holding the information.

Health Information: Any information that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Individual: A person who is the recipient of health and/or wellness services.

Individually Identifiable Health Information: Health information that identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Open: Actively communicating information through notice or otherwise.

Persons and Entities: Health care professionals, partnerships, proprietorships, corporations and other types of organizations and their agents when acting on their behalf.

Physical safeguards: Physical measures, policies and procedures to protect electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion. Physical safeguards include workstation security and use procedures, facility security plans, data backup and storage, and portable device and media controls.

Privacy: An individual's interest in protecting his or her individually identifiable health information and the corresponding obligation of those persons and entities, that participate in a network for the purposes of electronic exchange of such information, to respect those interests through fair information practices.

Security: The physical, technological, and administrative safeguards used to protect individually identifiable health information.

Technical safeguards: The technology and the policies and procedures for its use that protect electronic individually identifiable health information and control access to it.

Transparent: Making information readily and publicly available.

Use: Is the employment, application, utilization, examination, analysis or maintenance of individually identifiable health information.

Base Requirements and Principles: HIPAA Privacy Rule

- Consumer controls over health information
  - Rights to consumer
- Boundaries of uses and disclosures
  - Limitations on when, how, to whom, and for what purpose entities can use and disclose health information
- General security requirement
  - Further expanded with HIPAA security rule
- Accountability
  - Effects for negligent or criminal actions with health information

Base Requirements and Principles: HIPAA Privacy Rule

- Covered entity and protected health information
  - Applicable *only* to entities covered by HIPAA
  - Applicable to all health information (used/disclosed by covered entities)

- No consent requirement
  - For uses or disclosures of health information for TPO (treatment, payment, health care operations)
  - For 22 types of uses and disclosures, including public health, health oversight, judicial and administrative, victims of abuse and neglect, others
  - Authorization needed for all others

- No preemption of state laws that are more stringent

Base Requirements and Principles: HIPAA Privacy Rule

- Covered entity and protected health information
  - Applicable *only* to entities covered by HIPAA
  - Applicable to all health information (used/disclosed by covered entities)

- No consent requirement
  - For uses or disclosures of health information for TPO (treatment, payment, health care operations)
  - For 22 types of uses and disclosures, including public health, health oversight, judicial and administrative, victims of abuse and neglect, others
  - Authorization needed for all others

- No preemption of state laws that are more stringent

Base Requirements and Principles: Patient Consent

- Patient consent (authorization) in most states
  - Required by other laws
    - For specific types of information
    - Under HIPAA (authorization for certain disclosures)
    - In specific states
  - Determine several factors about health information
    - WHO: can access, use or disclose
    - WHAT: information can be assessed, used, disclosed
    - TO WHOM: can information be disclosed
    - WHY: for what purpose(s)
    - WHEN: time-limited

Base Requirements and Principles: Patient Rights

- Receive a notice of privacy practices
- Access individually identifiable health information for review and/or copy
- Request amendments to health information
- Request an accounting of certain disclosures that a covered entity has made of their PHI
- Request privacy protections to health information
  - Right to request restrictions on the use and disclosure of health information
  - Right to request confidential communications from a entities
- File a complaint about privacy issues

Base Requirements and Principles: Patient Rights

- Receive a notice of privacy practices
- Access individually identifiable health information for review and/or copy
- Request amendments to health information
- Request an accounting of certain disclosures that a covered entity has made of their PHI
- Request privacy protections to health information
  - Right to request restrictions on the use and disclosure of health information
  - Right to request confidential communications from a entities
- File a complaint about privacy issues

Base Requirements and Principles: Organization

- Organization responsibilities
  - Administrative policies and procedures
  - Privacy officer
  - Apply minimum necessary requirements
  - Handle various types of sensitive health information
  - Verify the identity and authority of individual requesting health information prior to disclosure (if not known by the entity disclosing the information), including documentation of such identify and authority
  - Mitigate harm, in the event of a use or disclosure done in violation of privacy requirements or organization's own policies and procedures

American Recovery and Reinvestment Act (ARRA), 2009

- Privacy provisions
  - HIPAA provisions extended to business associates
  - New breach notification requirements
    - FCC rules: entities not covered by HIPAA
    - HHS rules: entities covered by HIPAA
  - Ability to restrict disclosures to a health plan for payment or operations or items/services paid out of pocket
  - Limit uses and disclosures to limited data sets or minimum necessary
  - Accounting of disclosures through EHRs for TPO

American Recovery and Reinvestment Act (ARRA), 2009

- Privacy provisions
  - Provide copy of personal health information in electronic format to individual
  - Study and recommendations to Congress for P&S requirements for non-covered entity PRH vendors
  - Enforcement
    - Extend HIPAA civil penalties to BAs
    - Provides state AGs with authority to enforce HIPAA
    - Employees/individuals can be criminally liable