



HIPAA

Health Insurance Portability and
Accountability Act

Introduction

- **Health Insurance Portability and Accountability Act (HIPAA)**
 - Became effective on April 3, 2003
 - Four major components:
 - ❖ Health insurance portability
 - ❖ Standardization of electronic transmission of common administrative and financial transactions (such as billing and payments)
 - ❖ Privacy regulations, known as The Privacy Rule (effective 4-14-2003).
 - ❖ Security Regulations, known as The Security Rule (effective 2005)
 - HIPAA does not replace State, Federal or any other law that provides individuals added protection for their medical information
- Full text can be found at <http://www.hhs.gov/ocr/hipaa>

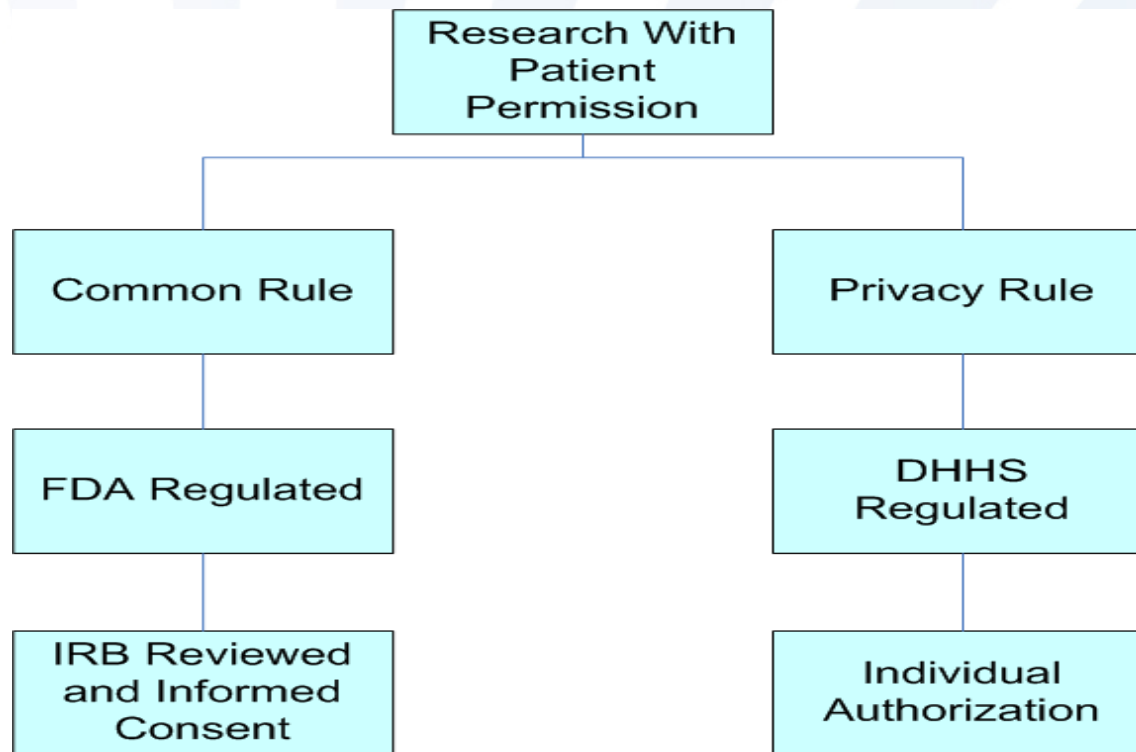
Introduction

- The Privacy and Security Rules were enacted to:
 - Reassure patients of safeguards to keep their health information private
 - Hold violators accountable through criminal penalties
 - Give patients control over their health information

Introduction

- The Privacy Rule regulates how patient information may be used or disclosed by Covered Entities.
- The Security Rule addresses the security of Protected Health Information in any form that is transferred or maintained by Covered Entities.

Common Rule* vs. Privacy Rule



* 45 CFR Part 46 Subpart A

DHHS – Department of Health and Human Services

Definitions

- **Covered Entity**

- A health plan, a health care clearinghouse, or a health care provider who transmits health information in electronic form in connection with a transaction for which DHHS has adopted a standard.

Business Associate

- **Business Associate**
 - assists in or performs HIPAA related activities for a Covered Entity that involve the use or disclosure of individually identifiable health information; or
 - provides certain services to a Covered Entity that involve the use or disclosure of Individually Identifiable Health Information.

Definitions

■ Health Information

- Any information, whether oral or recorded in any form or medium, that:
 - (1) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
 - (2) 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

Definitions

- **Individually Identifiable Health Information**
 - Is created or received by a health care provider, health plan, employer, or health care clearinghouse;
 - 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; and
 - Either identifies the individual, or, with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Definitions

- **Protected Health Information (PHI)**
 - A subset of **Individually Identifiable Health Information** that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.

Protected Health Information (PHI)

PHI includes all of the following (does not need to include diagnosis):

- License or VIN Numbers
- Account Numbers
- Biometric Identifiers/ Device Identifiers
- Full Face Photos
- Any other unique Identifier
- Names
- Addresses and Zip Codes
- All Dates
- Contact Info
- Social Security Numbers
- Medical Record Numbers
- Health Plan/Insurance ID Numbers

What does the Privacy Rule mean for individuals?

- Individuals have the right to:
 - A notice of privacy describing individuals' rights
 - Access to and ability to inspect and make copies of their own PHI
 - Make changes to their own PHI
 - Patient permission or “Authorization” is needed to use or share PHI for certain marketing or forecasting activities
 - Request who can have access to their PHI
 - Make complaints to Covered Entity and DHHS

What is HIPAA's impact on research at covered entities?

- Affects how covered entities provide access to or disclose PHI for use in research
- Places limits on clinicians who use PHI they collect for research purposes
- Types of data collection
 - Clinical trials
 - Merging patient information databases
 - Patient surveys
 - Retrospective chart reviews
 - Copying specific information from medical records

Permissible Use of PHI for Clinical Research

- Pursuant to the subject's written authorization.
- Subject to approval from an IRB or a Privacy Board granting a waiver of the authorization requirement or an altered authorization.
- If the PHI has been de-identified in accordance with accepted standards.
- For reviews preparatory to research with required representations obtained from the researcher .
- For research solely on decedents' information with certain representations and, if requested, documentation obtained from the researcher.

Written Authorization

- An individual's signed permission that allows a Covered Entity to use or disclose the individual's PHI for the purpose(s) and to the recipient(s) stated in the Authorization.
- Must pertain to a specific study.
- Covered Entity's use and disclosure of PHI must be consistent with Authorization.

Elements of an Authorization to Use or Disclose PHI

Core Elements

- Description of PHI to be used or disclosed:
- Person(s) authorized to make the requested use or disclosure.
- Person(s) to whom the Covered Entity may disclose PHI.
- Each purpose for the use or disclosure.
- Expiration date or event (e.g. "end of the research study" or "none").
- Participant Signature and Date

Statements

- Right to revoke Authorization plus exceptions and process
- Ability/Inability to condition treatment, payment, or enrollment/eligibility for benefits on Authorization
- PHI may no longer be protected by Privacy Rule once it is disclosed by the Covered Entity

Required Documentation of a Waiver or Alteration of Authorization Includes:

- A brief description of the PHI for which use or access has been determined by the IRB or Privacy Board to be necessary in connection with the specific research activity.
- A statement that the waiver or alteration was reviewed and approved under either normal or expedited review procedures.
- The required signature of the IRB or Privacy Board chair or the chair's designee.

De-Identified Health Information

- Health information that does not contain enough information to identify an individual
- Achieved by either:
 - A formal determination by a qualified statistician
 - The removal of specified identifiers of the individual and of the individual's relatives, household members, and employers. This method is adequate only if the Covered Entity has no actual knowledge that the remaining information could be used to identify the individual

»

»

Activities Preparatory to Research

- Covered entities may use or disclose PHI for purposes preparatory to research, such as to aid study recruitment.
- An employee of a Covered Entity workforce can use PHI to contact prospective research participants for purposes of seeking their Authorization to use or disclose PHI for a research study.
- PHI can be disclosed to an outside researcher who has made required representations regarding the use of PHI.

Activities Preparatory to Research

- Researcher Representations (required in writing):
 - the use or disclosure is requested solely to review PHI as necessary to prepare a research protocol or for similar purposes preparatory to research
 - the PHI will not be removed from the Covered Entity in the course of review, and
 - the PHI for which use or access is requested is necessary for the research

Business Associates

- Business Associate Agreement
 - Must be executed by Covered Entity and Business Associate prior to disclosure of PHI.
 - Business Associate must provide assurances that it will:
 - use the PHI only for the purposes for which it was engaged by the Covered Entity,
 - safeguard the information from misuse, and
 - help the Covered Entity comply with some of the Covered Entity's duties under the Privacy Rule.

Privacy Practices

- Designate a Privacy Officer
- Develop a Privacy Policy
- Provide subjects with a Notice of Privacy Practices (filed signed copy)
- Maintain private locations to discuss health information with individuals (Do not discuss private information in a public waiting room)
- Enact policies that prohibit staff from discussing individual health information in a general conversation with persons not directly involved in patient care
- Execute Business Associate agreements as necessary

Privacy Officer

- Privacy Officer is responsible for overseeing compliance with HIPAA.
- The Privacy Officer's duties include:
 - Development of a Privacy Policy
 - Providing and tracking Privacy Notices
 - Developing policies on how to handle complaints
 - Ensuring all employees are trained on HIPAA
 - Implementing technical and physical safeguards to protect PHI

Notice of Privacy

- The Notice of Privacy may include:
 - How subject PHI will be shared
 - Who PHI may be shared with
 - The subject's rights regarding PHI
 - Contact information to discuss PHI
 - The Covered Entity's responsibilities regarding PHI

Minimum Necessary Requirement

- Covered entities limit permissible use and disclosure of PHI to the minimum necessary to accomplish the intended purpose.
- The Minimum Necessary Requirement does not apply to disclosures:
 - To HHS
 - To the subject
 - Mandated by law
 - Authorized by subject
 - To health care providers for treatment

The Security Rule

- Addresses the methods used by Covered Entities to protect electronic-PHI.
- Covered entities must implement electronic, physical and procedural methods to protect PHI.
- Does not apply to PHI transmitted orally or in writing.
- Enforced by the Office for Civil Rights (OCR) of the DHHS.

Security Practices

- Maintaining a firewall-protected database with anti-virus software.
- Electronic signatures
- Administrative procedures
- Use of passwords
- Encryption
- Staff Training
- Inform Vendors of HIPAA requirements

Breach Notification Rule

- Addresses the Breach or unauthorized acquisition, use or disclosure of unsecured PHI which can be read by unauthorized persons
- Notice of breach must be provided to affected individuals and reported to DHHS.
- For breaches of unsecured PHI which affect more than 500 notice must also be provided through major media outlets.
- All employees must be trained on Breach Notification Rule.

What are the consequences of non-compliance with HIPAA?

- Possible harms to individual whose PHI is improperly disclosed (e.g., loss of insurance; distress)
- Potential loss of public trust in:
 - Covered Entity
 - Clinical Research
- Civil and criminal penalties
 - Fines up to \$250,000
 - Imprisonment up to 10 years

Summary

- The HIPAA Privacy Rule regulates the way covered entities may use and disclose protected health information the circumstances under which PHI can be used for clinical research.
- The HIPAA Security Rule addresses how covered entities must safeguard PHI.
- Covered Entities must develop processes for the disclosure and protection of PHI.

References

- Title 21 CFR Part 50: Protection of Human Subjects, FDA.
- Title 21 CFR Part 56: Institutional Review Boards, FDA.
- Title 45 CFR Part 46: Common Rule, DHHS
- Title 45 CFR Part 160. HIPAA Administrative Simplification: Enforcement, DHHS
- Title 45 CFR Part 164: Final Rule. Subpart E. FDA.
- OCR Privacy Brief: Summary of the HIPAA Privacy Rule. U.S. DHHS.
- IRB Review of Stand-Alone HIPAA Authorizations Under FDA Regulations. U.S. DHHS.