

**The Whys and Wherefores of HIPAA**

Office for Civil Rights  
Department of Health and Human Services  
April 15, 2010

1

The Health Insurance Portability & Accountability Act of 1996

- Legislative History:
  - Public Law 104-191 (42 USC §1320d)
  - Signed August 21, 1996
- Title I – Health Insurance Portability
- Title II, Subtitle F--Administrative Simplification

2

Purpose of HIPAA Administrative Simplification Provisions

Improve efficiency and effectiveness of health care system by *standardizing* the electronic exchange of administrative and financial data

3

Purpose of HIPAA Provisions (cont.)

- Encourage development of (electronic) health information technologies (transactions)
- Easier information sharing created the need for standards on security and privacy of health information

4

**HIPAA and Privacy**

- HIPAA required the Secretary to promulgate a regulation protecting the privacy of individually identifiable health information if Congress did not enact such legislation by August 21, 1999
  - Congress did not act
  - The Secretary proposed a health information privacy rule on November 3, 1999

5

HIPAA Privacy Rule

- Final Rule published 12/28/00
- Final modifications published 8/14/02
- Compliance by 4/14/03 for most covered entities

45 CFR Parts 160 and 164

6

## Scope: Who is Covered?

- Limited by HIPAA to:
  - Health care providers who transmit health information in electronic transactions for which the Secretary has adopted standards
  - Health plans
  - Health care clearinghouses

7

## Business Associates

- Agents, contractors, others hired to do work on behalf of covered entity that requires Protected Health Information (PHI)
- Covered entity must obtain satisfactory assurance – usually through a contract --that a business associate will safeguard protected health information, limit use and disclosure

8

## Uses and Disclosures: Authorizations

- Covered entities must obtain an individual's authorization before using or disclosing PHI for purposes other than:
  - Treatment, Payment or Healthcare Operations (TPO)
  - Where opportunity to agree or object required
  - Specified public priorities

45 CFR §§ 164.502, 164.510, 164.512

9

## Scope: What is Covered?

- Protected health information (PHI) is:
  - Individually identifiable health information
  - Transmitted or maintained in any form or medium
- Held or transmitted by covered entities or their business associates
- Not PHI:
  - De-identified information
  - Employment records

10

## Individual's Rights

Individuals have the right to:

- A written notice of information practices from health plans and providers
- Inspect and obtain a copy of their PHI
- Obtain an accounting of disclosures
- Request an amendment to their records
- Request restrictions on uses and disclosures
- Accommodation of reasonable communication requests
- Complain to the covered entity and to HHS

11

## Uses & Disclosures: Key Points

- NO use or disclosure of PHI unless required or permitted by the Rule
- Required disclosures are limited to:
  - Disclosures to the individual who is the subject of information
  - Disclosures to Secretary of HHS to determine compliance
- All other uses & disclosures in Rule are permissive

45 CFR § 164.502

12

### Minimum Necessary

- Covered entities must make reasonable efforts to limit the use or disclosure of PHI to minimum amount necessary to accomplish their purpose
- “Role-based” access limits
- Exceptions

13

### Public Policy Disclosures

- Covered entities may use or disclose PHI without authorization only if the use or disclosure comes within one of the listed exceptions & follows its conditions;
  - As required by law, law enforcement, judicial & administrative proceedings, etc.
  - For research

14

### Selected Research Provisions

- Authorization that satisfies section 164.508
- Reviews preparatory to research 164.512(i)
- Research solely on decedents’ information
- IRB or a Privacy Board has granted a waiver
- PHI has been de-identified
- Limited data set, with certain identifiers removed

15

### Administrative Requirements

Flexible & scalable

- Covered entities required to:
  - Designate a privacy official
  - Develop policies and procedures (including receiving complaints)
  - Provide privacy training to its workforce
  - Implement administrative, technical, and physical safeguards to protect the privacy of PHI

16

### Administrative Requirements (2)

- Develop a system of sanctions for employees who violate the entity’s policies
- Meet documentation requirements
- Mitigate any harmful effect of a use or disclosure of protected health information that is known to the covered entity
- Refrain from intimidating or retaliatory acts
- Not require individuals to waive their rights to file a complaint with the Secretary or their other rights under this rule

17

### HIPAA Compliance and Enforcement

- Technical assistance for voluntary compliance
- Any person or organization can file complaints with OCR (generally within 180 days)
- OCR may investigate complaints and may conduct compliance reviews
- OCR shall attempt to resolve noncompliance by informal means

45 CFR §§ 160.304 & 160.306

18

**OCR Web Site**

<http://www.hhs.gov/ocr/privacy>

[http://privacyruleandresearch.nih.gov/clin\\_research.asp](http://privacyruleandresearch.nih.gov/clin_research.asp)

19