

United States Department of  
**Health & Human Services**  
Office of the Secretary  
Office for Civil Rights (OCR)

## **HIPAA Privacy and Security Rule And Breach Notification Overview**

*Health Data Security Training  
October 25, 2012  
Susan Pezzullo Rhodes, Deputy Regional Manager, Region I*



## **45 CFR parts 160, 164**

- 160 General Administrative Requirements
  - Definitions
  - State law preemption
  - Compliance and enforcement
- 164 Security and Privacy
  - Definitions
  - Organizational requirements
  - Subpart E – Privacy
    - Uses and disclosures
    - Related requirements
    - Individual rights
    - Administrative requirements

**OCR**

2



## Scope: Who is Covered?

- Limited by HIPAA to:
  - Health care providers who transmit health information electronically in connection with a transaction for which there is a HIPAA standard
  - Health plans
  - Health care clearinghouses
- Business Associate Relationships

OCR

3

§160.301



## Business Associates

- Agents, contractors, and others hired to do the work of, or to work for, the covered entity, and such work requires the use or disclosure of protected health information (“PHI,” see next slide).
- The Privacy Rule requires “satisfactory assurance,” which usually takes the form of a contract, that a BA will safeguard the PHI, and limit its use and disclosure.

OCR

4

§160.301



## Scope: What is Covered?

- Protected Health Information (“PHI”):
  - 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
  - FERPA records

OCR

5

§160.301



## Uses and Disclosures: Key Points

- No use or disclosure of PHI unless permitted or required by the Privacy Rule.
- *Required* Disclosures:
  - To the individual who is the subject of the PHI.
  - To the Secretary of HHS in order to determine compliance.
- All other uses and disclosures in the Privacy Rule are *permissive*.
- Covered Entities may provide greater protections.

OCR

6

§164.502



## Permissive Uses and Disclosures

- To the individual or personal representative
- For treatment, payment, and health care operations (TPO)
- With the opportunity to agree or object
- For specific public priorities
- “Incident to”
- Limited data sets
- As authorized by the individual

§164.502

OCR

7



## To Individuals

- Besides making required disclosures, Covered Entities may also disclose PHI to their patients or enrollees. For example:
  - Health plans may contact their enrollees.
  - Providers may contact or speak with their patients.
- Covered Entities must treat a personal representative -- person who has authority to make decision related to health care -- as an individual

OCR

8





## Treatment, Payment, Health Care Operations (TPO)

- What is “treatment?”
- What is “payment?”
- What are “health care operations?”
- Using and disclosing for TPO §164.506
- Using and disclosing for TPO of another Covered Entities

§164.502

OCR

9



## Opportunity to Agree or Object

- To use PHI in facility directories (name, location, general condition, religious affiliation to clergy)
- To disclose PHI to persons involved in care or payment for care and for notification purposes. For example:
  - Friends may pick up prescriptions.
  - Hospitals may notify family members of a patient’s condition.
  - Covered entities may notify disaster relief agencies.

§164.510

OCR

10



## Public Priorities

- Covered Entities may use or disclose PHI without authorization only if the use or disclosure comes within one of the listed exceptions and follows its conditions. Some examples:
  - As required by law
  - For public health activities
  - For judicial and administrative proceedings
  - For specialized government functions

§164.512

OCR

11



## Incidental Uses and Disclosures

- The Privacy Rule permits uses and disclosures incidental to an otherwise permitted use or disclosure, provided minimum necessary and safeguard standards (discussed following) are met.
  - Examples: talking to a patient in a semi-private room; talking to other providers if passers-by are present; waiting-room sign-in sheets; patient charts at bedside.
- Allows for common practices if reasonably performed

§164.502

OCR

12



## Minimum Necessary Standard

- Covered entities must make reasonable efforts to use, disclose, or request the minimum necessary ("MN") PHI based on purpose.
- Exceptions to the MN standard: e.g., disclosure of PHI for the purpose of treatment
- Covered entities must identify classes of workforce members who need access to PHI to do their jobs.
- Covered entities must develop criteria to limit disclosures of and requests for PHI to the MN.

OCR

13

§164.502



## Authorizations

- Covered Entities *must* obtain an individual's authorization before using or disclosing PHI for purposes other than:
  - TPO;
  - Where the opportunity to agree or object is required;
  - Specified public priorities.
- Authorizations *must* be obtained for marketing (with limited exceptions).

OCR

14

§164.508



## Marketing

- Covered Entities *must* obtain an individual's authorization to use PHI for marketing.
- Exceptions are for:
  - Face-to-face communications;
  - Promotional gifts of nominal value.
- Marketing excludes treatment-related communications.
- Marketing includes arrangements where the Covered Entity discloses PHI for remuneration to a third party for that party to market its own products or services to individuals.

OCR

15

§164.501



## Administrative Requirements

- Covered Entities must:
  - Designate a Privacy Officer;
  - Designate a contact person or office to receive complaints and provide further information;
  - Provide privacy training to all workforce members;
  - Develop and apply sanction policy for workforce members who fail to comply;
  - Implement policies and procedures designed to comply with standards.

OCR

16

§164.530





## Administrative Requirements (cont.)

- Covered Entities must:
  - Implement administrative, technical and physical safeguards to protect privacy of PHI;
  - Mitigate any harmful effect of a violation known to the covered entity to the extent practicable;
  - Provide an internal complaint process for individuals;
  - Refrain from intimidating and retaliatory acts;
  - Not require individuals to waive their rights.

OCR

17

§164.530



## Individual Rights

- Notice of Privacy Practices
- Access: inspect and copy
- Amendment
- Accounting
- Alternative communications
- Request restriction
- Complaints to Covered Entity and Secretary

OCR

18



## Notice

- Individual has the right to written notice of the uses and disclosures of PHI that may be made by CE, CE's legal duties with regard to PHI, and individual rights.
- Required elements in Privacy Rule
- In most cases, Covered Entity must post and provide a copy to the individual on first contact with providers and upon enrollment with health plan and upon request.
- Covered provider must document "good faith effort" to obtain acknowledgement.

§164.520

OCR

19




## Access

- Individual has a right to inspect and obtain a copy of PHI about the individual in a designated record set ("DRS") for as long as the DRS is maintained.
- CE must act on the request within 30 days.
- CE must provide access in the form or format requested
- Reasonable fees are allowed for copying and postage only (no retrieval fees allowed).

§164.524

OCR


20



## Amendment

- Amendment:  
An individual has the right to request that a CE amend PHI about the individual in a DRS as long as the DRS is maintained.

OCR 21 §164.526



## Accounting

- Accounting:  
An individual has the right to receive an accounting of disclosures of PHI made by a CE in the six years or less prior to the request.

OCR 22 §164.528



## Alternative Communication

- Alternative Communication

A covered health care provider must permit the individual to request and must accommodate reasonable requests to receive communications of PHI by alternative means and at alternative locations. The requirement applies to health plans if the individual clearly states that the disclosure could endanger the individual.

§164.522(b)

OCR

23



## Request Restrictions

- Request Restrictions

CE must permit the individual to request that the CE restrict uses and disclosures of PHI for TPO. CE not required to agree to the request.

§164.522(a)

OCR

24





## Security Rule

- *Preamble and Definitions (45 CFR §164.304)*
- *General Rules – (45 CFR §164.306)*
- *Administrative Safeguards – (45 CFR §164.308)*
- *Physical Safeguards – (45 CFR §164.310)*
- *Technical Safeguards – (45 CFR §164.312)*
- *Organizational Requirements – (45 CFR §164.314)*
- *Policies and Procedures and Documentation Requirements – (45 CFR §164.316)*

OCR

25



## Security Rule Continued

- General Rules
  - Establishes the requirements covered entities (and business associates) must meet
  - Includes the consideration for a flexibility of approach
  - Defines the required standards and implementation specifications (both required and addressable)
  - Requires the maintenance of security measures implemented to support the reasonable and appropriate protection of electronic protected health information

OCR

26



## Security Rule continued.

- **Organizational Requirements**
  - Contains the standards for business associate contracts and other arrangements
  - Contains the requirements for group health plans
- **Policies and Procedures and Documentation Requirements**
  - Requires the implementation of reasonable and appropriate policies and procedures
  - Requires the maintenance of documentation (written or electronic)
  - Establishes the retention, availability, and update conditions for documentation

OCR

27



## Safeguards

- **Administrative Safeguards**
  - “...are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity’s workforce in relation to the protection of that information.” (*Definitions - 45 CFR §164.304*)
- **Physical Safeguards**
  - “...are physical measures, policies, and procedures to protect a covered entity’s electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.” (*Definitions - 45 CFR §164.304*)

OCR

28



## Safeguards continued

- Technical Safeguards
  - “...means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.” (*Definitions - 45 CFR §164.304*)

OCR

29




## Examples of Challenges

- Workstation Security
  - Many operating system and application versions have reached end of official support
  - Monthly security patches may be needed to ensure CIA
  - Vulnerabilities can be introduced by supporting applications like Java, PDF readers, and others (Shockwave, Flash)
- Access Control
  - Changes in workforce status (new, transfer or terminated)
  - Locations of the workforce
  - Motivations of the workforce

OCR

30




## Breach

- **Subpart D – Notification in Case of Breach of Unsecured PHI**
- **45 C.F.R. §§ 164.400-164.414**
- **(74 FR 42740)**

OCR

31



## Provisions

- 164.400 – Applicability
- 164.402 – Definitions
- 164.404 – Notification to individuals
- 164.406 – Notification to media
- 164.408 – Notification to Secretary/OCR
- 164.410 – Notification by business associates
- 164.412 – Law enforcement delay
- 164.414 – Administrative requirements and burden of proof

OCR

32





## Breach Overview

- Covered entities must:
  - notify each affected individual of breach of “unsecured protected health information.”
  - Notice to media if more than 500 people affected.
  - Notice to Secretary of breach through OCR website.
  - Most notifications must be provided without unreasonable delay (but no later than 60 days) of discovery of breach.
- Business associate must notify covered entity of breach and identify individuals affected.
- Effective date – September 23, 2009.
- No CMPs/sanctions imposed for failure to provide notification for 180 days after publication date for violations of Subpart D.

OCR

33



## What is a Breach?

- An impermissible acquisition, access, use or disclosure of PHI in a manner not permitted under Subpart E which compromises the security or privacy of the PHI.
- To compromise the security or privacy means to poses a *significant risk* of financial, reputational, or other harm to the individual.
- Uses or disclosures of limited data sets in which all dates of birth and zip codes have also been removed are not considered to compromise the security or privacy of PHI

OCR

34



## What is a “Significant Risk” of Harm

- Determined by the covered entity through a risk assessment once it learns of a possible breach.
- In determining the level of risk, the covered entity should make a fact-based evaluation of factors such as the recipient of the PHI, the nature of PHI itself, any mitigation that can be taken to lessen potential harm, and the number of identifiers contained within the PHI.

OCR

35



## Significant Risk of Harm-Examples

- Covered entity mistakenly discloses PHI to the wrong pharmacy. Since the pharmacy is also a covered entity and obligated to comply with the Security and Privacy Rules, this may not pose a significant risk of harm to the individual.
- Covered entity loses an unencrypted laptop containing PHI. However, it is recovered the next day and a forensic analysis reveals that the information contained was not opened, altered, transferred, or otherwise compromised. This may not pose a significant risk of harm to the individual.

OCR

36



## Breach Checklist for Covered Entities

1. Has there been an impermissible use or disclosure of PHI?
2. Perform risk assessment - determine and document whether the impermissible use or disclosure compromised the security or privacy of PHI and whether any financial, reputational, or other harm to the individual resulted.
3. Determine if the incident falls under any of the exceptions to the definition of breach
4. Was the PHI unsecured?

OCR

37



## OCR Web Site

[www.hhs.gov/ocr](http://www.hhs.gov/ocr)

Susan.Rhodes@hhs.gov

Privacy: [www.hhs.gov/ocr/hipaa/](http://www.hhs.gov/ocr/hipaa/)

OCR

38