Breach Notification for Unsecured Protected Health Information

May 11, 2010

Christina Heide, J.D.
HHS, Office for Civil Rights
Background

- **American Recovery and Reinvestment Act of 2009**

- **Title 13**: Health Information Technology for Economic and Clinical Health Act (HITECH Act)

- **Subtitle D**: Privacy (Privacy Rule and Security Rule)

- **Section 13402 – Breach Notification**
  - Guidance on Unsecured Protected Health Information
  - IFR on Notice Requirements for Covered Entities and Business Associates
Process

• Guidance and Request for Information – April 17, 2009
  – Guidance on Technologies/Methodologies for unusable, unreadable, indecipherable PHI
  – 74 FR 19006

• Interim Final Rule and Guidance – August 24, 2009
  – 45 CFR 164, Subpart D
  – Effective for breaches on/after 9/23/09
  – 60 day public comment period ended 10/23/09
  – Approximately 120 comments received
  – 74 FR 42740
Unsecured Protected Health Information

• Covered entities and business associates must provide notification of breaches of unsecured protected health information

• HHS Breach Notification Guidance: PHI is “unsecured” if it is NOT
  • Encrypted
  • Destroyed
What is a Breach?

- Impermissible use/disclosure which “compromises privacy/security” of PHI
  - Exceptions for inadvertent, harmless mistakes
    - Unintentional access by workforce member and no further impermissible use or disclosure
    - Inadvertent disclosure at same CE/BA/OHCA and no further impermissible use or disclosure
    - Recipient could not reasonably have retained the PHI
Notification to Affected Individuals

- Covered entity must notify each affected individual of breach
- Business associate must notify covered entity of breach
- Notification to be provided without unreasonable delay (but no later than 60 calendar days) after discovery of breach
Notification to Affected Individuals

• Methods
  – First-class mail or if individual agrees, electronic mail
  – If insufficient or out-of-date contact information, substitute notice

• Content
  – What happened
  – Types of PHI involved
  – Steps individuals should take
  – Steps covered entity is taking
  – Contact information
Notification to Media

• Required if more than 500 people affected in state/jurisdiction
• Notification to be provided without unreasonable delay (but no later than 60 calendar days) after discovery of breach
• Same content as in notification to individual
Notification to Secretary

• If 500 or more individuals affected, report to Secretary required contemporaneously with notification to individual
• If fewer than 500 individuals affected, annual report to Secretary permitted
• Reporting done via OCR’s website
• Posting of 500+ breaches on OCR website
Administrative Requirements & Burden of Proof

- Train workforce
- Policies and Procedures
- Documentation
- Covered entity/business associate has burden of proof to demonstrate all notifications were made or no breach occurred
Breach Reports to the Secretary

• Approximately 80 breaches affecting 500+ individuals reported, resulting in over 2,426,562 notifications to individuals (Sept-April).
  – Mostly ePHI that is contained in lost or stolen unencrypted media or portable device

• OCR has also received over 6000 reports of smaller breaches (Sept-April).
  – Mostly paper records sent to wrong fax number, wrong address, wrong individual
More Information

For more information on Breach Notification:

http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html