United States Department of Health & Human Services

Office of the Secretary
Office for Civil Rights (OCR)

Overview of the HIPAA Security Rule

Office for Civil Rights
Region IX
Alicia Cornish, EOS
Sheila Fischer, Supervisory EOS

Topics

Upon completion of this session, you will be able to:

- Understand some of the basic requirements of the:
  - HIPAA Security Rule
  - HITECH Breach Notification Rule
  - HIPAA Audit Program
  - Key Areas for Compliance

A Culture of Compliance

- OCR aggressively enforcing the HIPAA Privacy, Security, and Breach Notification Rules
- Covered entities and business associates should have robust HIPAA Privacy and Security compliance programs
- A robust compliance program includes employee training, vigilant implementation of policies and procedures, regular internal audits, and a prompt action plan to respond to incidents

Who is Covered?

- HIPAA specifies that only Covered Entities are required to comply with the Privacy and Security Rules
- Covered Entities (CE) are defined as:
  - Health care providers who transmit health information electronically in connection with a transaction for which there is a HIPAA standard
  - Health plans
  - Healthcare clearinghouses

Business Associates

- Agents, contractors, and others hired to do the work of, or to work for, the CE, and such work requires the use or disclosure of protected health information (PHI)
- The Privacy and Security Rules require a CE to receive “satisfactory assurance”
  - Assurance usually takes the form of a contract
  - Business associates (BA) only use or disclose PHI as permitted by agreement
  - Safeguard PHI from unauthorized disclosure

HIPAA Security Rule

- Security Standards: General Rules
- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards
- Organizational Requirements
- Policies and Procedures

The Guiding Principles of the Security Rule

- Ensure Electronic Protected Health Information (ePHI) is used, stored, transmitted or received with:
  - **Confidentiality**
    - only the right people see it
  - **Integrity**
    - the information is what it is supposed to be – no unauthorized alteration or destruction
  - **Availability**
    - the right people can see the ePHI when needed

Security Standards: General Rules

- Applies to Electronic Protected Health Information (ePHI)

- That a Covered Entity
  - Creates
  - Receives
  - Maintains
  - Transmits electronically

The Security Rule Requires CE's to Protect ePHI

- Protect ePHI against reasonably anticipated threats or hazards to the security or integrity of information
- Protect against reasonably anticipated uses and disclosures not permitted by the Privacy Rule or Security Rule
- Establish policies and procedures to ensure compliance by workforce

HHS Approach to HIPAA Security

- Standards to assure the confidentiality, integrity, and availability of ePHI
- Thorough, reasonable, and appropriate safeguards
- Addressing vulnerabilities identified through analysis and management of risk
- Appropriate to the size and complexity of the organization and its information systems
- Technology neutral

General Implementation Approach

- Conduct (and document) risk analysis
- Determine how to implement each standard and implementation specification of the rule (document the analysis) based on risk analysis
- Develop security policies/procedures (document)
- Implement security policies/procedures
- Train workforce
- Periodic evaluation
- Have business associate agreement
- Have contingency plans in place

Key Administrative Safeguards

- Risk analysis
- Risk management
- Designated security official
- Workforce security
- Information access management
- Information security awareness and training
- Incident procedures and contingency plans
- Evaluation
- Business associate agreements

Key Physical Safeguards

- Facility access
- Workstation use
- Workstation security
- Device and media controls

Key Technical Safeguards

- Access control
- Audit controls
- Integrity
- Person or entity authentication
- Transmission security

Key Technical Safeguards Cont.'

- Implement reasonable and appropriate safeguards to ensure the CIA (confidentiality, integrity, and availability) of data on systems that create, transmit or store ePHI
  - Encryption at rest
  - Encryption during transmission
  - Automatic logoff
  - Strong authentication
- Properly configure wireless network access

What is a Breach?

Impermissible use/disclosure which "compromises privacy/security" of PHI

Poses a significant risk of harm

- Financial
- Reputational
- Other harm
- Determined through risk assessment

Breach Notification IFR

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

Breach Notification Requirements

Covered entity must:

- Notify each affected individual of breach
- Notify Secretary via OCR's website
- Notify media if more than 500 people affected in state/jurisdiction without unreasonable delay after discovery of breach – can report "small" breaches annually

Appropriate Safeguards Prevent Breaches

- Evaluate the risk to ePHI when at rest on removable media, mobile devices and computer hard drives
- Take reasonable and appropriate measures to safeguard ePHI
  - Store all ePHI to a network
  - Encrypt data stored on portable/movable devices & media
  - Employ a remote device wipe to remove data when lost or stolen
  - Train workforce members on how to effectively safeguard data and timely reporting of incidents

Breach Notification Highlights September 2009 through March 2012

- 409 reports involving a breach of over 500 individuals
  - Theft and loss are 65% of large breaches (about 70% of these incidents involved ePHI)
  - Laptops and other portable storage devices account for 37% of large breaches
  - Paper records are 24% of large breaches
- 50,000+ reports of breaches of under 500 individuals

Business Associates

- Under HITECH Act, business associates (BA) will be directly liable under HIPAA
- May not use or disclose PHI in violation of BA agreement or Privacy Rule
- Must fully comply with Security Rule, including risk analysis/mgmt, training of staff, limiting access to ePHI, etc.
- Must report breaches of PHI to covered entities

Audits as Part of OCR Compliance Oversight

- Enforcement
  - Investigation of complaints
  - Compliance reviews
- Audit
  - More systematic approach to compliance
  - Preventative (rather than reactive) to close vulnerabilities before they can be exploited
  - Risk-based considerations to selection
  - Increased potential for learning from others

Background

- Section 13411 of the HITECH Act requires HHS to provide for periodic audits to ensure covered entities and business associates are complying with the HIPAA Privacy and Security Rules and Breach Notification standards
- OCR is piloting a program to perform up to 115 audits by 12/2012 of covered entities to assess HIPAA privacy and security performance

Program Objective

- Audits present a new opportunity to:
  - Examine mechanisms for compliance
  - Identify best practices
  - Discover risks and vulnerabilities that may not have come to light through complaint investigations and compliance reviews
  - Encourage renewed attention to compliance activities

Elements of Audits

- Objective selection criteria for entities
- Standard protocols adapted to entity size/ type
- Advance notice
- Preliminary desk review and onsite components
- Reports drafting with findings, recommendations
- Reporting on corrective or other actions

Who Will be Audited?

- Every covered entity is eligible for an audit
- OCR seeks to audit as wide a range of types and sizes of covered entities as possible which includes:
  - Health plans of all sizes
  - Health care clearinghouses
  - Individual and organizational providers
  - Business associates in later audit wave

Compliance Tools

- Risk Analysis Guidance
  - OCR website July 2010
  - http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidance.html
- NIST Security Rule Tool
  - http://scap.nist.gov/hipaa/
- Small Provider Guidance
  - http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/smallprovider.pdf

NIST HIPAA Security Rule Toolkit

- A toolkit to help covered entities and their business associates
  - Better understand the requirements of the HIPAA Security Rule
  - Implement those requirements
  - Assess those implementations in their operational environments
  - A self-contained, desktop based application that can support various operating environments (e.g. Microsoft Windows, Apple OS-X, Linux)
- **http://scap.nist.gov/hipaa**

Want More Information?

The OCR website, http://www.hhs.gov/ocr/privacy/ offers a wide range of helpful information about health information privacy including educational information, FAQ's, rule text and guidance for the Privacy, Security, and Breach Notification Rules.

Questions