Introduction

- Title II of HIPAA mandated the creation of rules to address how electronic healthcare transactions are transmitted and stored.
- The resulting HIPAA Security Rule establishes a standard for the security of electronic protected health information, or ePHI.
- The following legislation has modified and expanded the scope and requirements of the Security Rule
  - 2009 Health Information Technology for economic and Clinical Health Act (HITECH Act)
  - 2009 Breach Notification Rule
  - 2013 Modification to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under HITECH Act and the Genetic Information Nondiscrimination Act; Other Modifications to HIPAA Rules (known as the Omnibus Rule)

The HIPAA Security Rule

The HIPAA Security Rule focuses on safeguarding ePHI:

- Any individually identifiable health information (IIHI) that is stored, processed, or transmitted electronically or digitally
- Applies to covered entities (CEs) and business associates
- CEs include healthcare providers, health plans, healthcare clearinghouses, and certain business associates

What Is the Objective of the HIPAA Security Rule?

Main goal of HIPAA Security Rule is to protect the

- Confidentiality
- Integrity
- Availability

of all electronic protected health information

What Is the Objective of the HIPAA Security Rule? Cont.

The standards are intentionally nonspecific and scalable.

Covered entities choose the appropriate technology and controls for their own unique environment, taking into consideration

- Their size and capabilities
- Their technical infrastructure
- The cost of the security measures
- The probability of risk

Enforcement and Compliance

- DHHS Office and Civil Right (OCR) Authority is responsible for investigating violations and enforcing the Security Rule
  - Fines for noncompliance are up to $1,500,000 per violation per year
  - Criminal charges can be brought with penalties of
    - Up to $50,000 and 1 year in prison for knowing violations
    - Up to $100,000 and 5 years in prison for violations committed under false pretense
    - Up to $250,000 and 10 years in prison for offenses committed for commercial or personal gain

How Is the HIPAA Security Rule Organized?

Administrative Safeguards:

The documented policies and procedures for

- Managing operations
- Conduct and access of workforce to ePHI
- Selection, development, and use of security controls

Physical Safeguards:

- Requirements for protecting ePHI from unauthorized physical access

How Is the HIPAA Security Rule Organized? Cont.

Technical Safeguards:

- The use of technology to control access to ePHI

Organizational Requirements:

- Includes standards for business associate contracts and requirements for group health plans

Documentation Requirements:

- Includes policies and procedures regarding documentation and records and their retention and availability

Implementation Specifications

- Many of the standards contain implementation specifications
- Specifications can be
  - Required
  - Addressable
    - It does not mean optional or that it can be ignored

What Are Administrative Safeguards?

Incorporates nine standards focusing on internal organization, policies, procedures, and maintenance of security measures that protect patient health information

The Security Management Process includes:

- Conducting a risk assessment
- Implementing a risk management program; identifying all threats to ePHI
- Developing and implementing a sanction policy for security violations; applies to employees, contractors, and vendors
- Developing and deploying an information system activity review

What Are Administrative Safeguards? Cont.

Assigned Security Responsibility:

- Appoint a responsible security official to oversee compliance

Workforce Security:

- Implement procedures for authorization and supervision of workforce members
- Establish a workforce clearance procedure for hiring and assigning tasks
- Establish termination procedures

What Are Administrative Safeguards? Cont.

Information Access Management:

- Isolate healthcare clearinghouse functions
- Implement policies and procedures to authorize access
- Implement policies and procedures to establish access

What Are Administrative Safeguards? Cont.

Security Awareness and Training:

- Establish a security awareness program to remind users of potential threats
- Provide training on recognizing malicious software (malware)
- Provide training on login monitoring procedures
- Provide training on password management

What Are Administrative Safeguards? Cont.

Security Incident Procedures:

- Addresses reporting of and responding to security incidents
  - Training users to recognize incidents
  - Implementing a reporting system
  - Follow through with investigations and report back to the user

What Are Administrative Safeguards? Cont.

Contingency Plans:

- Conduct an application and data criticality analysis
- Establish and implement a data backup plan
- Establish and implement a disaster recovery plan
- Establish an emergency mode operation plan
- Test and revise procedures

What Are Administrative Safeguards? Cont.

Evaluation:

- All covered entities must develop criteria and metrics for evaluating their own compliance

Business Associate Contracts and Other Agreements:

- Business associates and third parties must also comply
- Based on written contract or other form of agreement

What Are Physical Safeguards?

Facility Access Controls include:

- Create a facility security plan; prevent unauthorized access, tampering, and theft
- Implement access control and validation procedures
- Keep maintenance records, including modifications to doors, locks, and so on
- Establish contingency operations

What Are Physical Safeguards? Cont.

Workstation Use:

- Covers proper use of workstations, particularly laptops

Workstation Security:

- Covers restricting workstation access to authorized users

What Are Physical Safeguards? Cont.

Device and Media Controls:

- Implement disposal policies and procedures
- Implement reuse policies and procedures
- Maintain accountability for hardware and electronic media
- Develop data backup and storage procedures

What Are Technical Safeguards?

Access Control:

- Require unique user identification
- Establish emergency access procedures
- Implement automatic logoff procedures that terminate a session after a period of inactivity
- Encrypt and decrypt information at rest

What Are Technical Safeguards? Cont.

Audit Controls:

- Organizations must monitor system activity

Integrity Controls:

- To protect ePHI from improper alteration or destruction
- Includes antivirus and antispyware, firewalls, and e-mail scanning

What Are Technical Safeguards? Cont.

Person or Entity Authentication:

- Requires unique user identification, such as password, PIN, biometric ID, and so on

Transmission Security:

- Implement integrity controls
- Implement encryption

What Are the Organizational Requirements?

Business Associates Contracts:

- Contracts must meet specific requirements to ensure the confidentiality, integrity, and availability of ePHI
- Covered entities, business associates, and their agents must protect ePHI and report security incidents or risk termination

What Are the Policies and Procedures Standards?

Policies and Procedures to ensure that:

- Standards and implementation specifications are met
- Actual activities of the covered entity are reflected

What Are the Policies and Procedures Standards? Cont.

Documentation:

- Retain documentation for 6 years
- Make documentation available to necessary personnel
- Update documentation as necessary to reflect changes that may affect the security of ePHI

The HITECH Act and the Omnibus Rule

- The HITECH Act is part of the American Recovery and Reinvestment Act of 2009
  - Amended the Public Health Service Act (PHSA) with a focus on improving healthcare quality, safety, and efficiency through the promotion of health information technology
  - Widened the scope of privacy and security protections available under HIPAA
- The Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the HITECH Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules (known as the Omnibus Rule) was published January 25, 2013

What Changed for Business Associates?

- Original description
  - A person or organization that performs certain functions or activities that involve the use or disclosure of PHI on behalf of, or provides services to, a CE
- Revised description
  - A person or entity that creates, receives, maintains, transmits, or accesses PHI to perform certain functions or activities on behalf of a CE
- Subcontractors of business associates that create, receive, maintain, transmit, or access PHI are considered business associates
- Civil penalties for violations were increased
- Criminal penalties were not changed but criminal charges can be brought against anyone who wrongly discloses PHI, not just CEs

What Are the Breach Notification Requirements?

- HITECH established several notification requirements for CEs and business associates
  - Safe Harbor Provision
  - Breach Notification Requirements
    - CEs must notify individuals in case of a breach even if the breach occurred through a business associate
    - The notification must be done within 60 days of the discovery of the breach
    - If the breach affects more than 500 individuals in a state or jurisdiction, a notice to “prominent media outlets” must be done
    - DHHS must be notified of all breaches