HIPAA Security Rule Compliance

Caryn Reiker

MAXIS360

HIPAA Security Rule Compliance…what is it and why you should be concerned about it

Table of Contents

About HIPAA 2

Who Must Comply 2

The HIPAA Security Rule 3

Security Rule Sections 3

- Security standards: General Rules 3
- Administrative Safeguards 4
- Physical Safeguards 4
- Technical Safeguards 4
- Organizational Requirements 4
- Policies and Procedures and Documentation Requirements 4

A Word About Standards and Implementation Specifications 5

HIPAA Security Rule Standards 5

- Administrative Safeguards 6
- Physical Safeguards 7
- Technical Safeguards 7

HITECH Enacts Significant Changes to the HIPAA Security Rule 8

- The Tiered Civil Monetary Penalty (CMP) System 8

What Should You Do…Steps to Compliance 9

About HIPAA

The Health Insurance Portability and Accountability Act, commonly known as HIPAA, was signed into law on August 21, 1996. Congress passed HIPAA to:

- Improve portability and continuity of health insurance coverage in the group and individual markets
- Combat waste, fraud, and abuse in health insurance and health care delivery
- Promote the use of medical savings accounts
- Improve access to long-term care services and coverage
- Simply the administration of health insurance.

There are a five "titles" in HIPAA, each title being broad in scope and addressing different areas of the overall objective of the HIPAA legislation. The five titles are:

- Title I Healthcare Insurance Access, Portability and Renewability
- Title II Preventing Healthcare Fraud and Abuse, Administrative Simplification and Medical Liability Reform
- Title III Tax-related Health Provisions
- Title IV Application and Enforcement of Group Health Insurance Requirements
- Title V Revenue Offsets

The Security Rule, which this article addresses, falls within the Administrative Simplification Section of Title II.

Who Must Comply

As designated in the legislation, the HIPAA Security Rule applies to the following covered entities:

- Covered Healthcare Providers—Any provider of medical or other health services, or supplies, who transmits any health information in electronic form in connection with a transaction for which the Department of Health and Human Services has adopted a standard.
- Health Plans—Any individual or group plan that provides, or pays the cost of, medical care, including certain specifically listed governmental programs (e.g., a health insurance issuer and the Medicare and Medicaid programs).
- Healthcare Clearinghouses—A public or private entity that processes another entity's healthcare transactions from a standard format to a nonstandard format, or vice versa.

The HIPAA Security Rule

The HIPAA Security Rule specifically focuses on safeguarding electronic protected health information (ePHI.) For covered entities, this requires addressing administrative, physical and technical procedures. This would encompass access to offices, files and computers, as well as the processes a healthcare provider uses to keep electronic health information secure.

The HIPAA Security Rule outlines the steps that covered entities must take to protect ePHI from *unintended* disclosure through breaches of security. This includes any reasonably anticipated threats or hazards, such as a computer virus, network intruders and inappropriate uses and disclosures of electronic health information such as using unencrypted Email to communicate ePHI to persons outside your network. ePHI is vulnerable to and must be protected from:

- Hacker and disgruntled employee abuse
- Untrained personnel mishandling
- Access by personnel not having a "need to know"
- System outages
- Theft
- Disasters, natural and man-made

A fundamental design principal in the Security Rule was that "one size does not fit all". Organizations need to first understand the law, second asses their risks in relation to the law and third take appropriate actions to mitigate their risks in order to comply with the law.

Security Rule Sections

The HIPAA Security Rule consists of six main sections and each of those sections includes standards and implementation specifications that a covered entity must address. The six sections are listed below.

Security standards: General Rules

This section includes the general requirements that all covered entities must meet. It also establishes flexibility of approach, identifies standards and implementation specifications, outlines decisions a covered entity must make regarding addressable implementation specifications and requires maintenance of security measures to continue reasonable and appropriate protection of electronic protected health information. This section also requires that covered entities must:

- Ensure the confidentiality, integrity, and availability of ePHI that it creates, receives, maintains, or transmits;
- Protect against any reasonably anticipated threats and hazards to the security or integrity of ePHI
- Protect against reasonably anticipated uses or disclosures of such information that are not permitted by the Privacy Rule.

In complying with this section of the Security Rule, covered entities must also understand the definitions provided for confidentiality, integrity, and availability as identified in Section164.304:

- **Confidentiality** is "the property that data or information is not made available or disclosed to unauthorized persons or processes."
- **Integrity** is "the property that data or information have not been altered or destroyed in an unauthorized manner."
- **Availability** is "the property that data or information is accessible and useable upon demand by an authorized person."

Administrative Safeguards

Administrative Safeguards are defined in the Security Rule as the "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."

Physical Safeguards

Physical Safeguards are defined as the "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."

Technical Safeguards

Technical Safeguards are defined as the "the technology and the policy and procedures for its use that protect electronic protected health information and control access to it."

Organizational Requirements

This section includes standards for business associate contracts and other arrangements, including memoranda of understanding between a covered entity and a business associate when both entities are government organizations; and requirements for group health plans.

Policies and Procedures and Documentation Requirements

This section requires implementation of reasonable and appropriate policies and procedures to comply with the standards, implementation specifications and other requirements of the Security Rule; maintenance of written (which may be electronic) documentation and/or records that includes policies, procedures, actions, activities, or assessments required by the Security Rule; and retention, availability, and update requirements related to the documentation.

A Word About Standards and Implementation Specifications

The Security Rule establishes standards that covered entities must comply with to ensure that ePHI remains confidential and secure. Each of the sections in the Security Rule includes **standards** and **implementation specifications.**

Important Note: Covered entities are required to comply with All HIPAA Security Rule standards.

Many standards contain implementation specifications. An implementation specification is a more detailed description of the method or approach that can be used to meet the standard. Implementation specifications are either required or addressable.

- A **required** implementation specification is similar to a standard meaning that a covered entity must comply with it.
- **Addressable** implementation specifications must either be implemented, or if not implemented, an assessment to determine whether the implementation specification is reasonable and appropriate for the covered entity's environment must be performed. Following the completion of the assessment, the covered entity must decide to:
    - Implement the addressable implementation specification
    - Implement an equivalent alternative measure that will still ensure that the covered entity complies with the standard
    - Not implement the addressable specification or any alternative measures, if equivalent measures are not reasonable and appropriate within its environment

Covered entities are required to document these assessments and all decisions. We advise both CEs and BAs to treat "required" and "addressable" specifications as "required". Data and information is becoming more and not less vulnerable and privacy and security laws are only going to become more stringent over time.

HIPAA Security Rule Standards

Listed below are the HIPAA Security Rule-required standards, their specific HIPAA Security Rule citation and corresponding implementation specifications.

In addition to these Safeguards, the Security Rule also contains Standards and Implementation Specifications addressing organizational requirements, as well as policies and procedures and documentation requirements.

Administrative Safeguards

The Security Rule defines administrative safeguards as, *"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."*

The Administrative Safeguards comprise over half of the HIPAA Security requirements

164.308(a)(1) Security management process
- Risk Analysis
- Risk Management
- Sanction Policy
- Information System Activity Review

164.308(a)(2) Assigned security responsibility
- Assigned Security Officer

164.308(a)(3) Workforce security
- Authorization and/or Supervision
- Workforce Clearance Procedure
- Termination Procedures

164.308(a)(4) Information access management
- Isolate Healthcare Clearinghouse Functions
- Implement Policies and Procedures for Authorizing Access
- Implement Policies and Procedures for Access Establishment and Modification

164.308(a)(5) Security awareness training
- Security Reminders
- Protection from Malicious Software
- Login Monitoring
- Password Management

164.308(a)(6) Security incident procedures
- Response and Reporting

164.308(a)(7) Contingency plan
- Data Backup Plan
- Disaster Recovery Plan
- Emergency Mode Operation Plan
- Testing and Revision Procedure
- Applications and Data Criticality Analysis

164.308(a)(8) Evaluation
- Periodic Technical and Nontechnical Evaluations

164.308(b)(1) Business associate contracts and other arrangements
- Written Contract or Other Arrangements

Physical Safeguards

The Physical Safeguards standards in the Security Rule were developed to ensure that reasonably appropriate physical controls have been put in place to protect ePHI for information systems and related equipment and facilities.

164.310(a)(1) Facility access controls
- Contingency Operations
- Facility Access Plan
- Access Control and Validation Procedures
- Maintenance Records

164.310(b) Workstation use
- Policies and Practices Governing Workstation Use/Location

164.310(c) Workstation security
- Policies and Practices addressing Physical Security of Workstations

164.310(d)(1) Device and media controls
- Disposal
- Media Reuse
- Accountability
- Data Backup and Storage

Technical Safeguards

Healthcare organizations are challenged to protect ePHI from all internal and external risks. To reduce risks to ePHI, covered entities must implement technical safeguards. Implementation of HIPAA's Technical Safeguards standards represent good business practices for technology and associated technical policies and procedures within a covered entity.

164.312(a)(1) Access control
- Unique User Identification
- Emergency Access Procedure
- Automatic Logoff
- Encryption and Decryption

164.312(b) Audit controls
- Implementation of Technical Process to Record Activities Related to the Creation, Modification and Deletion of ePHI

164.312(c)(1) Integrity
- Implementation of Process to ensure that ePHI is not Improperly Altered or Destroyed
- Implementation of Authentication Mechanisms

164.312(d) Person or entity authentication
- Implementation of Controls that properly authenticate users of ePHI

164.312(e)(1) Transmission security
- Integrity Controls
- Encryption

HITECH Enacts Significant Changes to the HIPAA Security Rule

The Health Information Technology for Economic and Clinical Health (HITECH) Act was enacted as part of the American Recovery and Reinvestment Act of 2009. HITECH is the largest expansion and change to HIPAA Privacy and Security Rules ever. The fifteen change areas comprise new federal privacy and security provisions that will have major financial, operational and legal consequences for all Covered Entities and now their Business Associates as well.

The most significant of the changes are the penalties that HHS can now impose for violations of HIPAA rules. For example, a new Civil Monetary Penalty (CMP) system makes monetary penalties mandatory for violations involving "willful neglect" as of February 17th, 2011. Section 13410(d) of the HITECH Act strengthened the enforcement by establishing tiered ranges of increasing minimum penalty amounts, with a maximum penalty of $1.5 million for violations of an identical provision in a calendar year and the Final Omnibus Rule effective March 26th, 2013 increased the potential per violation fines.

The Tiered Civil Monetary Penalty (CMP) System

- Tier A - violations in which the Covered Entity did not know a violation occurred and by "exercising reasonable due diligence would not have known"
  - $100 to $50,000 fine for each violation, and
  - $1,500,000 maximum imposed per calendar year of an identical provision
- Tier B – violations due to reasonable cause but not "willful neglect"
  - $1,000 to $50,000 fine for each violation, and
  - $1,500,000 maximum imposed per calendar year of an identical provision
- Tier C – violations due to "willful neglect" that the organization ultimately corrected.
  - $10,000 to $50,000 fine for each violation, and
  - $1,500,000 maximum imposed per calendar year of an identical provision
- Tier D – violations of "willful neglect" that the organization did not correct.
  - $50,000 for each violation, and
  - $1,500,000 maximum imposed per calendar year of an identical provision

The new level of Civil Monetary Penalties applies immediately to all violations. HHS will use the CMP proceeds to further enforce the HIPAA Privacy and Security Rule. Subsection 13410(c) of the HITECH Act requires civil penalties for violations to be funneled back into the Department of Health and Human Services' Office of Civil Rights enforcement budget. Additionally HHS must distribute a portion of CMP proceeds directly to harmed individuals which will provide a direct incentive for individuals to report alleged violations to HHS and state attorneys general.

What Should You Do…Steps to Compliance

- Conduct a complete risk assessment. Your assessment should identify all personal health information (PHI) records, both paper and electronic. Determine the risks to PHI security that exist within your organization and spell out all the controls you have in place for safeguarding PHI.
- Conduct a comprehensive HIPAA Security Assessment to determine your current level of compliance with the HIPAA Security Rule.
- Create a plan to mitigate your major risks. Once you have identified your top risks you will need to create a written plan with the appropriate controls to address your risks. Then you will need to implement the controls from your plan into your organization's business practices.
- Update policies and procedures, determine what needs to be updated or enhanced for compliance with HIPAA and HITECH.
- Consider whether all of your uses, disclosures and requests for PHI are in compliance with the "minimum necessary" standard now that a "limited data set" has been defined as compliance with that standard.
- Document all decisions made and risks that are deemed accepted.
- Ensure all employees (including clinicians and upper management) are trained on their roles and responsibilities with respect to the HIPAA Security Rule and the HITECH Act.
- Maintain an ongoing program for monitoring your environment and operational processes for HIPAA Security Rule compliance.