HIPAA Compliance White Paper

EQUILIBRIUM
IT SOLUTIONS, INC.

This document provides an overview of HIPAA regulation requirements. This includes privacy, security, enforcement and breach notifications related to HIPAA compliance.

Author: Todd Bey, Managing Consultant

Overview

Businesses and organizations today need to have a basic understanding of the Health Insurance Portability and Accountability Act (HIPAA), regardless if they are operating inside or outside of the healthcare industry. The main focus of HIPAA regulations is towards Covered Entities (CE) and Business Associates (BA). These designations relate to businesses and organizations that are directly involved in healthcare or provision of services to healthcare entities.

There are four areas/rules associated with Health Insurance Portability and Accountability Acct (HIPAA) that businesses need to be familiar with and understand how they apply to business operations:

- HIPAA Privacy Rule
- HIPAA Security Rule
- HIPAA Enforcement Rule
- HIPAA Breach Notification Rule

Businesses need to follow the HIPAA Privacy Rule and the HIPAA Security Rule, and to understand HIPAA enforcement procedures. Additionally, businesses need to provide the appropriate notifications following a breach of unsecured protected health information.

This White Paper is aimed at business decision makers and IT managers at Covered Entities and their Business Associates. It provides a brief overview of regulation requirements.

HIPAA Privacy Rule

The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

Business Associates are directly liable for uses and disclosures of PHI that are not covered under their BAA or the HIPAA Privacy Rule itself. The Privacy Rule requires Business Associates to do the following:

- Do not allow any impermissible uses or disclosures of PHI.
- Provide breach notification to the Covered Entity.
- Provide either the individual or the Covered Entity access to PHI.
- Disclose PHI to the Secretary of HHS, if compelled to do so.
- Provide an accounting of disclosures.
- Comply with the requirements of the HIPAA Security Rule.

HIPAA Security Rule

The HIPAA Security Rule requires appropriate Administrative, Physical, and Technical Safeguards to ensure the confidentiality, integrity, and security of protected health information (PHI).

There are three parts to the Security Rule:

- Technical Safeguards
- Physical Safeguards
- Administrative Safeguards.

Each of the three Safeguards have implementation specifications, and are either designated as "required" or "addressable." Required implementation specifications must be implemented. Addressable implementation specifications must be implemented if it is reasonable and appropriate to do so. It is important for businesses to maintain documentation supporting the choice to address. Addressable implementation specifications are not considered optional, and if it is possible business should implement the addressable implementation specification.

Technical Safeguards

The Technical Safeguards focus on the technologies that protect and control access to PHI. The standards of the Technical Safeguards do not require the use of any specific technologies, and are meant to be technology-neutral.

There are five standards under Technical Safeguards, including:

- Access Control
- Audit Controls
- Integrity
- Authentication
- Transmission Security

When considering these five standards, businesses need to address nine specific areas for implementation.

Access Control - Unique User Identification (required)

Users should be assigned a unique identifier such as a name or number for tracking and identifying user identity.

Emergency Access Procedures (required): Establish and implement procedures for gaining access to necessary PHI during an emergency.

Automatic Logoff (addressable): Implement electronic procedures for termination of electronic sessions after a predetermined period of inactivity.

Encryption and Decryption (addressable): Implement a mechanism for encryption and decryption of PHI.

Audit Controls (required)

Implement hardware, software, and procedural mechanisms to record and examine activities within information systems that utilize or contain PHI.

Integrity - Mechanism to Authenticate PHI (addressable)

Implement electronic mechanisms to verify whether PHI has been altered or destroyed in an unauthorized manner.

Authentication (required)

Implement procedures to verify that the person or entity seeking to access PHI is the actual person or entity seeking access.

Transmission Security

Integrity Controls (addressable): Implement security measures to ensure electronically transmitted PHI is not modified without detection.

Encryption (addressable): Implement encryption mechanisms for PHI as necessary and appropriate.

Physical Safeguards

Physical Safeguards are a set of rules and guidelines that focus on the physical access to PHI.

There are four standards under Physical Safeguards, including:

- Facility Access Controls

- Workstation Use
- Workstation Security
- Device and Media Controls

When considering these four standards, businesses need to address ten specific areas for implementation:

Facility Access Controls

Contingency Operations (addressable): implement procedures that allow facility access during an emergency for restoration of lost data according to disaster recovery and business continuity plans.

Facility Security Plan (addressable): Implement policies and procedures for protection of facilities and equipment within those facilities from theft, tampering, and unauthorized physical access.

Access Control and Validation Procedures (addressable): Implement procedures to validate and control access to facilities based on individual roles and functions, including visitor access, and control of access to software program testing and revisioning.

Maintenance Records (addressable): Implement policies and procedures to create maintenance logs and records of modifications and repairs to physical security components (hardware, locks, doors, barriers, etc.)

Workstation Use (required)

Implement policies and procedures that specify proper use, functions, physical attributes of the workspace around the workstation and of the workstation itself that is used to access PHI.

Workstation Security (required)

Implement physical safeguards for all workstations that access PHI, restricting access to authorized users.

Device and Media Controls

Disposal (required): Implement policies and procedures for the disposal of hardware and electronic media on which PHI is stored.

Media Re-Use (required): Implement procedures for removal of PHI from electronic media prior to media being made available for reuse.

Accountability (addressable): Maintain a log of hardware and electronic media movement and transport including any person responsible for that movement.

Data Backup and Storage (addressable): Create backup and restorable copies of PHI prior to movement and transport of hardware and electronic media containing PHI.

Administrative Safeguards

Administrative Safeguards are policies and procedures governing the conduct of employees, and associated security measures put in place to protect PHI.

Businesses that implement a HIPAA compliance program are required to assign a privacy officer, complete a risk assessment annually, implement employee training, review policies and procedures, and execute business associate agreements with all partners and 3rd party entities who handle protected health information.

There are nine standards under Administrative Safeguards, including:

1. Security Management Processes
2. Assigned Security Responsibilities
3. Workforce Security
4. Information Access Management
5. Security Awareness and Training
6. Security Incident Procedures
7. Contingency Plans
8. Evaluations
9. Business Associate Contracts and Other Arrangements

When considering these nine standards, businesses need to address eighteen specific areas:

Security Management Process

Risk Analysis (required): Perform a risk assessment to determine where PHI is being used, how it is stored, and vulnerabilities which could result in violations of HIPAA.

Risk Management (required): Design and implementation of necessary measures to mitigate/reduce risks to appropriate levels.

Sanction Policy (required): Implement sanction policies for employees who fail to comply with security policies and procedures.

Information Systems Activity Reviews (required): Regularly review of system logs, activities, audit trails, etc.

Assigned Security Responsibility - Officers (required)

Designate HIPAA Security and Privacy Officers.

Workforce Security - Employee Oversight (addressable)

Implement procedures for authorization and supervision of employees working with PHI. Implement procedures for granting and removing employee access to PHI, including termination of access to PHI when employment is terminated.

Information Access Management

Multiple Organizations (required): Manage access to prevent access by parent company, partner companies, and subcontractors that are not authorized for access to PHI.

PHI Access (addressable): Implement procedures for granting access to PHI, and documentation of that access to PHI including services and systems that grant access to PHI.

Security Awareness and Training

Security Reminders (addressable): Implement procedures to provide updates and reminders about security and privacy policies to employees.

Protection Against Malware (addressable): Implement procedures for preventing, detecting and reporting of malicious software.

Login Monitoring (addressable): Implement monitoring of system logins and reporting of login discrepancies.

Password Management (addressable): Design and implement password policies and procedures for creating, changing, and protecting passwords.

Security Incident Procedures - Response and Reporting (required)

Establish procedures for identifying, documenting and responding to security incidents.

Contingency Plan

Contingency Plans (required): Ensure that there are backup copies of PHI, that they are accessible and restorable.

Contingency Plans Updates and Analysis (addressable): Implement policies and procedures for periodic testing and revision of contingency plans. Assess the relative criticality of specific applications and data, and the interrelation with other contingency plan components.

Emergency Mode (required): Design and implement procedures to provide continuity of critical business process and the protection of PHI while operating in emergency mode.

Evaluations (required)

Perform periodic evaluations to see if any changes in the business or in the law require changes or modifications to the business' current HIPAA compliance procedures.

Business Associate Agreements (required)

Create, distribute and execute special contracts with business partners who will be accessing PHI.

HIPAA Enforcement Rule

The HIPAA Enforcement Rule contains provisions relating to compliance and investigations, the imposition of civil money penalties for violations of the HIPAA Administrative Simplification Rules, and procedures for hearings.

HITECH Act Enforcement Interim Final Rule

The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, was signed into law on February 17, 2009, to promote the adoption and meaningful use of health information technology. The HITECH Act addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules.

Section 13410(d) of the HITECH Act, which became effective on February 18, 2009, revised section 1176(a) of the Social Security Act (the Act) by establishing:

Four categories of violations that reflect increasing levels of culpability;

Four corresponding tiers of penalty amounts that significantly increase the minimum penalty amount for each violation; and

A maximum penalty amount of $1.5 million for all violations of an identical provision.

It also amended section 1176(b) of the Act by:

Striking the previous bar on the imposition of penalties if the covered entity did not know and with the exercise of reasonable diligence would not have known of the violation (such violations are now punishable under the lowest tier of penalties); and

Providing a prohibition on the imposition of penalties for any violation that is corrected within a 30-day time period, as long as the violation was not due to willful neglect.

This interim final rule conforms HIPAA's enforcement regulations to these statutory revisions that are currently effective under section 13410(d) of the HITECH Act. This interim final rule does not make amendments with respect to those enforcement provisions of the HITECH Act that are not yet effective under the applicable statutory provisions.

HIPAA Breach Notification Rule

The Breach Notification Rule requires HIPAA covered entities and their business associates to prove notification to HHS following a breach of unsecured PHI. In the event the breach affects more than 500 patients, notification must also be provided to the media and public.

Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC), apply to vendors of personal health records and their third party service providers, pursuant to section 13407 of the HITECH Act.

Covered entities and business associates, as applicable, have the burden of demonstrating that all required notifications have been provided or that a use or disclosure of unsecured protected health information did not constitute a breach. Thus, with respect to an impermissible use or disclosure, a covered entity (or business associate) should maintain documentation that all required notifications were made, or, alternatively, documentation to demonstrate that notification was not required:

- its risk assessment demonstrating a low probability that the protected health information has been compromised by the impermissible use or disclosure; or
- the application of any other exceptions to the definition of “breach.”

Covered entities are also required to comply with certain administrative requirements with respect to breach notification. For example, covered entities must have in place written policies and procedures regarding breach notification, must train employees on these policies and procedures, and must develop and apply appropriate sanctions against workforce members who do not comply with these policies and procedures.

Preliminary Questionnaire

Answers of “No” may indicate non-compliance.

1. Do you have a person, position or group designated as the privacy and security officer?
2. Do you have a documented information security and privacy policies and procedures? Have the documented information security and privacy policies and procedures been reviewed and updated as necessary within the past 12 months?
3. Have information security and privacy policies and procedures been communicated to all employees, and are they available for employees to review at any time? Is there ongoing and regular training and awareness communications for information security and privacy provided to all workers?
4. Have you had a formal information security risk assessment performed in the last 12 months?
5. Is there a current backup policy for business information? Are backups performed regularly? Is there a documented disaster recovery and business continuity plan? Are the DR and BC plans regularly updated and tested?
6. Do you require all types of sensitive information, including personal information and health information (PHI), to be encrypted when transmitted through public networks? Is the information encrypted when it is stored on mobile computers and mobile storage devices?
7. Have you implemented controls to limit physical access to devices and locations where PHI is accessed and stored? Is access to PHI limited to those people who need access to fulfill their job responsibilities?
8. Are there technical security controls in-place to protect against unauthorized access to PHI?
9. Are all business associates (BA), including subcontractors of business associates, under a BA agreement? Is the BA agreement signed and does it specifically state what the BA has been engaged to do and require the BA to follow and comply with all HIPAA requirements?
10. Do you require disposal of all information, in all forms, to be securely disposed?
11. Do you have a documented breach response and notification plan? Is there a team identified to support the breach response and notification plan?
12. If you are a covered entity (CE), do you provide a Notice of Privacy Practices (NPP) that meets all HIPAA requirements in compliance with the Omnibus Rule changes?

References

Privacy Rule:

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

Security Standards: Technical Safeguards

http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf

Security Standards: Physical Safeguards

http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/physsafeguards.pd

Security Standards: Administrative Safeguards

http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf

Enforcement Rule:

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

Breach Notification Rule:

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

Conclusion

Maintaining HIPAA compliance can be confusing as the requirements are very general. A common approach is to leverage third-party experts to guide you through the compliance requirements.

About Equilibrium

Founded in 2004, half of Equilibrium is dedicated to providing IT project consulting and the other half dedicated to providing IT services. Equilibrium specializes in IT strategy, security, cloud, datacenter upgrades and ongoing operations.

Visit us at EQinc.com

Request a Free Consultation: http://eqinc.com/request-a-free-consultation

For more information: info@eqinc.com, 773-205-0200