HIPAA Handbook & Reference Manual

Insert Company Logo Here

Insert Company Logo

[Company Name]

HIPAA Handbook & Reference Manual
Table of Contents

- HIPAA | Introduction 3
- HITECH | Introduction 3
  - Subpart D
- HIPAA Security Awareness Training Requirements 5
- HIPAA Security Rule 5
- HIPAA Security | 164.308 Administrative Safeguards 5
  - Complete text for 45 CFR 164.308
- HIPAA Security | 164.310 Physical Safeguards 8
  - Complete text for 45 CFR 164.310
- HIPAA Security | 164.312 Technical Safeguards 10
  - Complete text for 45 CFR 164.312
- HIPAA Security | 164.314 Organizational Requirements 11
  - Complete text for 45 CFR 164.314
- HIPAA Security | 164.316 Policies and Procedures 12
  - Complete text for 45 CFR 164.316
- HIPAA Notification of Breaches | As Amended by the Final Omnibus Ruling | January, 2013 13
- HIPAA Privacy Rules 14
- HIPAA Privacy | 164.500 - 164.534 15
- HIPAA Privacy | General Principles for Uses and Disclosures 16
- HIPAA Privacy | Permitted Uses and Disclosures 17
- HIPAA Privacy | Authorized Uses and Disclosures 18
- HIPAA Privacy | Individual Rights 18
- HIPAA Privacy | Administrative Requirements 19
- HIPAA Privacy | General Safeguards and Best Practices 20
- Covered Entities 21
- Business Associates 21
- Final Omnibus Ruling (January, 2013) 22
- Helpful HIPAA Resources 23
- Reporting a Security Breach 23

Insert Company Logo

HIPAA Handbook & Reference Manual

Overview

The HIPAA Handbook & Reference Manual is a helpful, easy-to-use guide for keeping all employees and other workforce members abreast of core components within the Health Insurance Portability and Accountability Act (HIPAA). HIPAA is without question the most in-depth and comprehensive healthcare legislative mandate in North America, essentially affecting millions of business from coast to coast. One of the most important aspects of HIPAA is providing concise material to all interested parties for ensuring a strong understanding of all major mandates within this enormous piece of legislation. The healthcare industry has undergone many changes in recent years, with HIPAA being in the forefront, thus it's vital that employees have a helpful document for answering questions regarding HIPAA, while also learning valuable facts and information regarding the Health Insurance Portability and Accountability Act. The more knowledgeable and educated employees are about HIPAA, the better prepared an organization will be when it comes to ensuring the safety and security of Protected Health Information (PHI).

Goals & Use
The HIPAA Handbook & Reference Manual covers all the essential topics and subject matter relating to the broader aspect of the Health Insurance Portability and Accountability Act. In it you'll find dozens of helpful sections for obtaining a very strong understanding of HIPAA, such as the Security Rule and Privacy Rule provisions, HITECH, the Final Omnibus Rulings, and much more.

- HIPAA | Introduction
- HITECH | Introduction
- HIPAA Security Awareness Training Requirements
- HIPAA Security Rule
- HIPAA Security | 164.308 Administrative Safeguards
- Complete text for 45 CFR 164.308
- HIPAA Security | 164.310 Physical Safeguards
- Complete text for 45 CFR 164.310
- HIPAA Security | 164.312 Technical Safeguards
- Complete text for 45 CFR 164.312
- HIPAA Security | 164.314 Organizational Requirements
- Complete text for 45 CFR 164.314
- HIPAA Security | 164.316 Policies and Procedures
- Complete text for 45 CFR 164.316
- HIPAA Notification of Breaches | As Amended by the Final Omnibus Ruling | January, 2013
- HIPAA Privacy Rule
- HIPAA Privacy | 164.500 - 164.534
- HIPAA Privacy | General Principles for Uses and Disclosures
- HIPAA Privacy | Permitted Uses and Disclosures
- HIPAA Privacy | Authorized Uses and Disclosures
- HIPAA Privacy | Individual Rights
- HIPAA Privacy | Administrative Requirements
- HIPAA Privacy | General Safeguards and Best Practices

- Covered Entities
- Business Associates
- Final Omnibus Ruling (January, 2013)
- Helpful HIPAA Resources

HIPAA | Introduction

The Health Insurance Portability and Accountability (HIPAA) is a comprehensive set of healthcare provisions enacted by the United States Congress and subsequently signed into law by President Bill Clinton in 1996. The bill effectively mandated broad-based legislation regarding healthcare access, portability, renewability, along with security and privacy rules for electronic health records and related information ("protected health information" | PHI, and subset thereof known as "electronic protected health information | ePHI).

Within Title II of HIPAA, the main emphasis has been that of the "Privacy Rule" and the "Security Rule", two (2) critically important legislative mandates that established, for the first time, a set of national standards for the protection of certain health information (the "Privacy Rule") along with establishing a national set of security standards (the “Security Rule”) for protecting certain health information that is held or transferred in electronic form.

Being "compliant" with HIPAA is a broad statement indeed, due in large part to the depth of the HIPAA legislation itself. While Title I and Title II of HIPAA contain numerous, far-reaching provisions for many organizations in the health and benefits arena, great emphasis has been in placed on the Privacy Rule and the Security Rule regarding regulatory compliance due to their applicability to many entities. Additionally, supporting legislation from subtitle D of The Health Information Technology for Economic and Clinical Health ACT of 2009 (HITECH) strengthens the civil and criminal enforcements of the HIPAA Privacy and Security Rules. Additionally, it must be noted that for both the Privacy Rule and Security Rule, along with the mandates within subtitle D of HITECH, organizations are identified as either "Covered Entities" or "Business Associates".

A "Covered Entity" (CE) is defined as that of:

- A health plan.
- A health care clearinghouse.
- A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter [e.g., HIPAA Administrative Simplification transaction standards].

A "Business Associate" (BA) is defined as that of a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. Simply stated, business associate functions and activities vary widely and can include claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management and data warehousing, just to name a select few. The technical definition of a "business associate" – expanded by the final Omnibus ruling in 2013 – can now include emerging technologies and businesses, such as data centers, Software as a Service (SaaS) entities, and managed services providers, just to name a select few. Visit the Department of Health and Human Services (www.hhs.gov) to learn more about HIPAA and helpful guidelines on protecting healthcare information.

HITECH | Introduction

The Health Information Technology for Economic and Clinical Health Act, simply known as the HITECH Act to many, was officially enacted under Title XIII of the American Recovery and Reinvestment Act of 2009, and is considered a major piece of health care legislation in many ways. Specifically, HITECH advocates the adoption of electronic health records (EHR) for creating efficiency, transparency, and overall improvements in care. And there are many provisions within the Act that require much attention by various parties, particularly *Subpart D—Notification in the Case of Breach of Unsecured Protected Health Information*. Nevertheless, it's a huge goal and a large task indeed, with untold numbers of organizations being affected by the HITECH Act. Essentially, HITECH emphasizes the concept of "meaningful use", whereby the main components are the following:

- The use of a certified electronic health records (EHR) in a meaningful manner, such as e-prescribing.
- The use of certified EHR technology for electronic exchange of health information to improve quality of health care.
- The use of certified EHR technology to submit clinical quality and other measures.

Essentially, providers need to show they're using certified EHR technology in ways that are deemed beneficial, ultimately resulting in the following:

- Improvement of care coordination
- Reduction of healthcare disparities
- Engaging of patients and their families
- Improving the population and public health
- Ensuring adequate privacy and security

It's without question a transformational piece of legislation that advocates, dictates - and ultimately requires - a significant expansion in the exchange of electronic protected health information (ePHI).

Subpart D

For purposes of regulatory compliance - specifically for that of HIPAA Privacy and Security, the HITECH ACT component of critical importance is *Subpart D—Notification in the Case of Breach of Unsecured Protected Health Information*, which consists of the following areas:

§ 164.400 Applicability.
§ 164.402 Definitions.
§ 164.404 Notification to individuals.
§ 164.406 Notification to the media.
§ 164.408 Notification to the Secretary.
§ 164.410 Notification by a business associate.
§ 164.412 Law enforcement delay.
§ 164.414 Administrative requirements and burden of proof.

Subpart D essentially strengthens the civil and criminal enforcements of the HIPAA Privacy and Security Rules by placing strong requirements and mandates on breaches. For purposes of HITECH Subpart D, breach means the following:

"The acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information".

Additionally, major changes came into play for HIPAA because of the HITTECH ACT - more specifically – the Privacy and Security Rules for HIPAA have been broadened and strengthened by the final Omnibus ruling put forth on January, 2013. Learn more about the HITECH ACT and Subpart D by visiting the Department of Health and Human Services (www.hhs.gov)

HIPAA Security Awareness Training Requirements

It's important to note that under the HIPAA Administrative Safeguards - specifically - 164.308(a)5 states the following, *"Standard: Security awareness and training. Implement a security awareness and training program for all members of its workforce (including management)."* This statement, though brief, requires covered entities, business associates and any other relevant party to do just that - undertake comprehensive security awareness training, for "all" members within an organization. The HIPAA security awareness training provided to [company name] within this handbook and other applicable training material, offers an in-depth overview on important HIPAA and HITECCH subject matter, while also covering dozens of critical information security awareness topics and issues.

HIPAA Security Rule

The HIPAA Security Rule, considered rather brief in terms of length and documentation for regulatory compliance legislation - nonetheless places a large focus on the protection of electronically Protected Health Information (ePHI). Ultimately, this requires covered entities, business associates, and any other relevant parties to have best-of-breed operational, business specific, and information security policies, procedures, processes and practices in place. While the HIPAA Security Rule technically includes parts 164.302 to 164.318, it's the Administrative, Physical, and Technical Safeguards that draw most attention - and rightfully so - as they provide explicit guidance on various mandates that must be in place for ensuring compliance.

HIPAA Security | 164.308 Administrative Safeguards

HIPAA 164.308 requires the following:

- Implement policies and procedures to prevent, detect, contain, and correct security violations.
- Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.
- Implement policies and procedures to ensure that only appropriate members of the workforce have access to ePHI.
- Implement policies and procedures for authorized access to ePHI that are consistent with the applicable requirements of the PR.
- Implement a security awareness and training program for all members of its workforce (including management).
- Security incident procedures.
- Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that could damage systems that contain ePHI.

- Perform a periodic technical and non-technical evaluation to ensure that standards continue to be met in response to operational and environmental changes.
- Business associate contracts and other arrangements.

In summary, covered entities, business associates and other relevant parties are to have comprehensive policies and procedures in place addressing the aforementioned areas. As an employee of [company name], you have the right to request such documentation from authorized personnel for gaining a greater understanding of HIPAA 164.308 and general best practices relating to the protection of electronically Protected Health Information (ePHI).

The Full, complete text for 45 CFR 164.308 is as follows:

(a) A covered entity or business associate must, in accordance with §164.306:

(1) (i) Standard: Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations.

(ii) Implementation specifications:

(A) Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.

(B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a).

(C) Sanction policy (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.

(D) Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

(2) Standard: Assigned security responsibility. Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.

(3) (i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.

(ii) Implementation specifications:

(A) Authorization and/or supervision (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.

(B) Workforce clearance procedure (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

(C) Termination procedures (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.

(4) (i) Standard: Information access management. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.

(ii) Implementation specifications:

(A) Isolating health care clearinghouse functions (Required). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.

(B) Access authorization (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.

(C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

(5) (i) Standard: Security awareness and training. Implement a security awareness and training program for all members of its workforce (including management).

(ii) Implementation specifications. Implement:

(A) Security reminders (Addressable). Periodic security updates.

(B) Protection from malicious software (Addressable). Procedures for guarding against, detecting, and reporting malicious software.

(C) Log-in monitoring (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.

(D) Password management (Addressable). Procedures for creating, changing, and safeguarding passwords.

(6) (i) Standard: Security incident procedures. Implement policies and procedures to address security incidents.

(ii) Implementation specification: Response and reporting (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.

(7) (i) Standard: Contingency plan. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

(ii) Implementation specifications:

(A) Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

(B) Disaster recovery plan (Required). Establish (and implement as needed) procedures to restore any loss of data.

(C) Emergency mode operation plan (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

(D) Testing and revision procedures (Addressable). Implement procedures for periodic testing and revision of contingency plans.

(E) Applications and data criticality analysis (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components.

(8) Standard: Evaluation. Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.

(b)(1) Business associate contracts and other arrangements. A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with §164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.

(2) A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with §164.314(a), that the subcontractor will appropriately safeguard the information.

(3) Implementation specifications: Written contract or other arrangement (Required). Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of §164.314(a).