GUIDES 29 MIN READ

HIPAA for Dummies: The Ultimate HIPAA Security and Compliance FAQ

by Michael Osakwe

Published Jul 23, 2022

TABLE OF CONTENTS

Building a HIPAA-compliant security program is a very time intensive and demanding undertaking. It can also be confusing, as satisfying requirements like the HIPAA Security Rule require extensive interpretation and documentation on the part of security professionals. However, by arming yourself with knowledge before beginning the process, you can cut down on unnecessary difficulties.

That's why we've created this guide to help security professionals and teams understand the basics of HIPAA compliance. This includes everything, from the structure of the law, to thorough overviews of the different sections of the regulation you'll need to interpret in order to satisfy HIPAA's stringent data security requirements.

How is this HIPAA compliance guide structured?

This guide includes answers to the most frequently asked questions about HIPAA, first starting by talking about the law at a high level, then going into the specifics of HIPAA compliance by looking at the privacy rule, security rule, and breach notification rules in more detail.

- → **What is HIPAA?**
- → **What is HIPAA compliance?**
  - → **Who does HIPAA compliance apply to?**
  - → **How do organizations prove compliance?**
- → **HIPAA Privacy Rule**
  - → **Definition of PHI**
  - → **Uses and Disclosures**
    - → **Permitted uses and disclosures**
    - → **Minimum Necessary Standard**
- → **Business Associate Agreement**
- → **Administrative requirements**

What is the purpose of this HIPAA guide and who is it for?

The purpose of this guide is to serve as a quick reference document for some very important FAQs often asked by security practitioners or individuals who are otherwise new to HIPAA compliance. Contained in this post are links to other reference materials we've created, like our **Remote-First Security Playbook**, which might aid in better understanding aspects of HIPAA, like **the Security Rule**.

Should you download this guide, it'll also come with a matrix of every implementation specification for the HIPAA Security Rule and guidance for each one (which you can also view below). Additionally, we've included our checklist for important questions for HIPAA-bound entities to ask any cloud providers they intend to work with.

Please note that this post is not intended to be a substitute for legal advice, and is just a starting point for any covered entities and business associates wanting to learn more about the basics of HIPAA compliance.

What is HIPAA?

The Health Insurance Portability and Accountability Act of 1996, commonly referred to as HIPAA, is a sprawling piece of legislation. In 2002, HIPAA **was estimated to exceed 100,000 words** and span over 500 pages. **New additions to the law** since then have ensured steady, continuous growth in HIPAA's size.

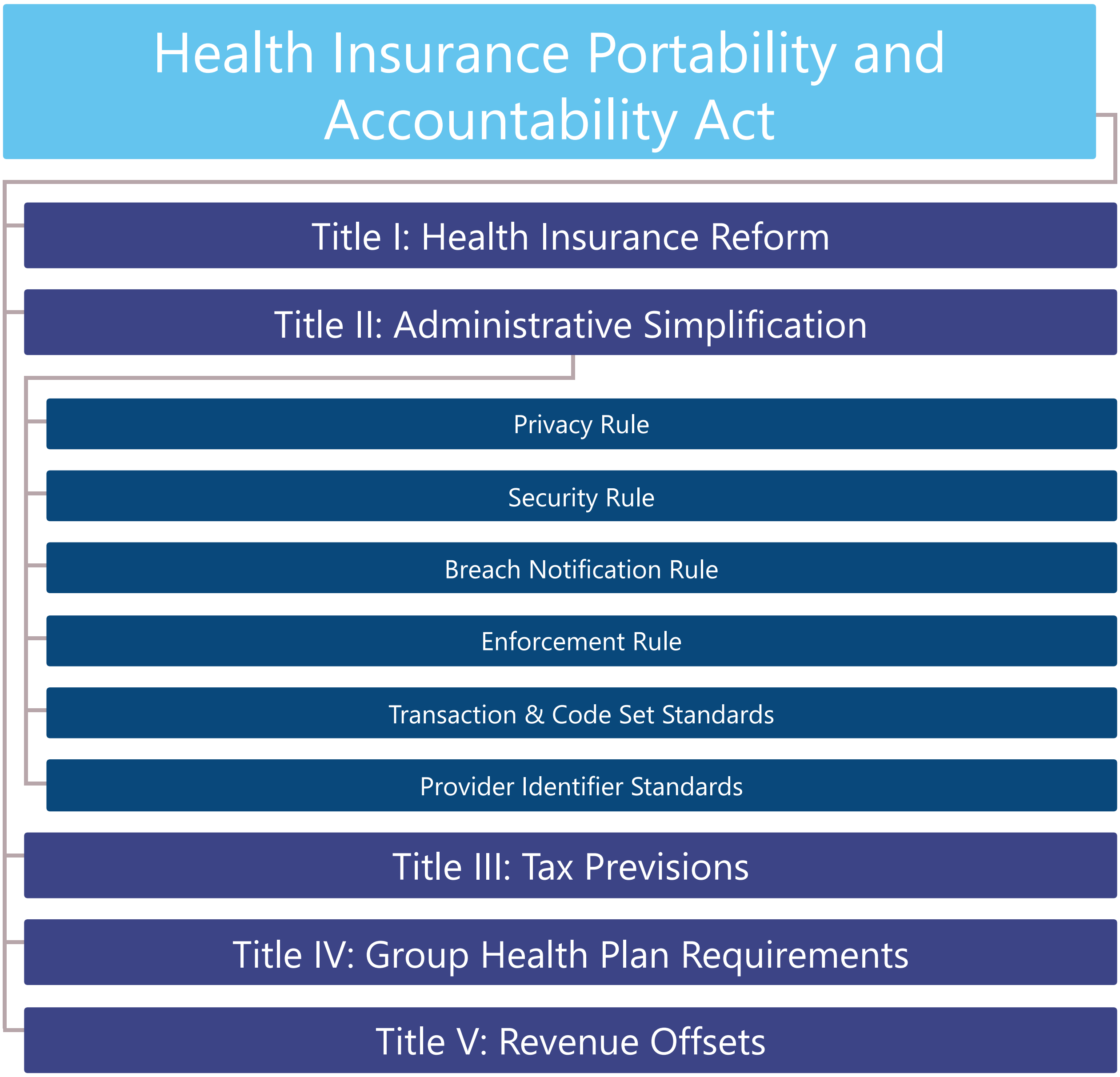
The four main objectives of HIPAA include:

- Ensuring the portability of healthcare coverage for employees (hence the name "healthcare Insurance Portability Act"). While this is not really a problem of today, this is in great part due to HIPAA (and laws like COBRA) addressing some of the coverage limitations facing employees switching between jobs.
- Helping healthcare organizations **reduce administrative complexity** through things like standardizing electronic communications and the implementation of electronic systems for things like billing, communicating diagnoses, etc.
- **Reducing fraud and abuse** against programs like Medicare, Medicaid, as well as private programs.
- Guaranteeing standards for the security and privacy of patient health information.

By design, HIPAA covers a lot of ground, as it was meant to tackle problems emerging in the nascent days of digitization in the healthcare space. Newer additions to HIPAA like **2009's HITECH Act** continued this trend by updating HIPAA in order to ensure its relevance in the face of emerging technologies. HIPAA as a whole also addresses the processes of a variety of entities such as insurance providers, healthcare providers, healthcare clearinghouses.

A key reason for HIPAA's size and complexity is that **HIPAA is divided** into five **titles**, or sections, with each one dealing with a different range of issues. The five titles of HIPAA are:

1. Title I: HIPAA Health Insurance Reform
2. Title II: HIPAA Administrative Simplification
3. Title II: HIPAA Administrative Simplification
4. Title IV: Application and Enforcement of Group Health Plan Requirements
5. Title V: Revenue Offsets


Health Insurance Portability and Accountability Act
Title I: Health Insurance Reform
Title II: Administrative Simplification
Privacy Rule
Security Rule
Breach Notification Rule
Enforcement Rule
Transaction & Code Set Standards
Provider Identifier Standards
Title III: Tax Previsions
Title IV: Group Health Plan Requirements
Title V: Revenue Offsets

What is HIPAA compliance?

Typically, when people discuss HIPAA compliance or the idea of "becoming HIPAA-compliant" they're referring to reviewing and implementing the rules included in HIPAA Title II: Administrative Simplification. Title II of HIPAA can be subdivided into six key areas:

→ **HIPAA Privacy Rule**. The Standards for Privacy of Individually Identifiable Health Information (known as the *HIPAA Privacy Rule* or just "the Privacy Rule") set national standards for the protection of individuals' health information and medical records (PHI), including the appropriate boundaries on use, release, and disclosure of health information.

→ **HIPAA Security Rule**. The Security Standards for the Protection of Electronic Protected Health Information (known as the *HIPAA Security Rule* or just “the Security Rule”) can be considered a subset of the HIPAA privacy rule. It sets standards for securing electronically stored and transmitted protected health information (ePHI) via required and addressable security implementations that HIPAA-bound entities must adopt.

- → **HIPAA Breach Notification Rule**. The HIPAA **Breach Notification Rule** provides HIPAA-bound entities with the determinations required to assess when impermissible uses and disclosures of PHI occur within your org, and when such incidents need to be reported.
- → **HIPAA Enforcement Rule**. The Enforcement Rule details how the Health and Human Services’ Office for Civil Rights, the entity responsible for HIPAA enforcement, will carry out investigations and penalties for HIPAA violations.
- → **HIPAA National Provider Identifier Standards & Code Set Standards.** HIPAA Administrative Simplification also includes standards for activities involving the transfer of health information and identifier standards for employers and health care providers. **45 CFR § 160.103** contains definitions of what constitutes healthcare transactions.

Perhaps unsurprisingly, for security teams, the HIPAA Security Rule is perhaps the most important aspect of HIPAA to understand for addressing compliance. However, the Security Rule works in conjunction with the HIPAA Privacy Rule. Furthermore, the Breach Notification Rule informs HIPAA-Bound entities of the “fail state” they’re aiming to prevent through the development of their compliance program.

Therefore, validating that you’ve correctly implemented the HIPAA Security Rule involves being able to verify that you can identify impermissible uses and disclosures of PHI within your organization, as well as, connect the dots between how your security implementations protect ePHI and, more broadly, PHI when applicable.

While the National Provider Identifier (NPI) standards and Transaction Code Standards are part of administrative simplification (HIPAA Title II), for the purposes of this guide to HIPAA for security teams we won’t be covering them directly.

Who does HIPAA apply to?

In the language of HIPAA, the term **covered entity** (CE) refers to the most common type of organization that must comply with HIPAA. Organizations that count as covered entities often include:

- → Healthcare providers that transmit electronic information using a HHS standard like NPI (such as doctors, clinics, and nursing homes)
- → Health plans (such as insurance companies HMOs and company plans)
- → Healthcare clearinghouses

The other type of organization that HIPAA applies to is referred to as business associates (BAs). The definition of a business associate is any business or organization that disclose PHI in order to perform a service or function on behalf of a covered entity.

The HITECH and HIPAA Omnibus Final Rule (or just the Final Rule), which were mentioned above, adds modifications to the definition of a business associate, including Health Information Organizations (HIOs), E-Prescribing Gateways, as well as vendors of personal health records and other persons that facilitate data transmission.

But, most importantly, the Final Rule expands the definition of business associates to subcontractors of business associates. Effectively, any business or service provider that must disclose PHI in the course of providing services and functionality of any entity bound by HIPAA, be they a business associate or covered entity, must be treated as a business associate.

How do organizations prove HIPAA compliance?

The Health and Human Services Office of Civil Rights is responsible for enforcing HIPAA regulations. As per the Privacy Rule (**45 CFR § 160.308 “Compliance reviews”**), the OCR may perform a review of your compliance program. In such an instance, covered entities and business associates must do the following (as outlined in **45 CFR § 160.310** “Responsibilities of CEs and BAs”):

- → **Provide compliance reports**. HIPAA requires extensive documentation. This includes detailed risk assessments evaluating the security of PHI, to documentation of your policies and practices and controls.

- → **Cooperate with requests to review your policies, procedures, and practices**.

Is there a HIPAA Certification process?

There is no official agency that provides HIPAA compliance certification, nor is there a process to become "HIPAA-certified." While there are many organizations who will claim they can help you obtain HIPAA certification, the OCR does not officially recognize this status, nor will going through such a process provide any guarantee that your organization will successfully pass an audit from the OCR.

It's possible that working with external organizations to improve your HIPAA posture might be useful as a soul-searching exercise of sorts, especially if you have no idea where to begin the HIPAA compliance process. However, this is by no means legally obligatory, nor is it something that will ensure that your organization is fully compliant.

This is actually the case with many federal regulations, like **FERPA** (Family Educational Rights and Privacy Act) and **GLBA** (Gramm-Leach-Bliley Act), federal standards like these don't involve formal certification processes. This confusion likely stems from the fact that many industry-established compliance standards, like **SOC 2** do have certification requirements. Federal regulations like HIPAA are less about demonstrating point-in-time compliance, and more about permanently adopting a specific posture towards sensitive information.

Technically, the only time you'll have to "demonstrate" compliance is when the OCR knocks on your door. However, because many organizations and people take compliance seriously, it'll be important to create a well documented program not just to satisfy official audits, but to reassure your customers and to assure your business associates that your organization is a trustworthy partner.

What triggers a HIPAA compliance audit?

HIPAA audits can occur in a variety of ways, including:

- → When an impermissible disclosure or breach of PHI occurs and is reported to the OCR.
- → When an individual **files a complaint** against your organization regarding privacy violations.
- → In the rare circumstance that your organization is **randomly selected** to be in the OCR's audit program.

While HIPAA audits might appear to be semi-random, you're better off not trying to time when they'll occur. Much like with car insurance, make sure your documentation is in order, so that on the off chance you're asked to demonstrate compliance, you won't be in violation of the law.

Understanding of HIPAA compliance requirements

As highlighted in the previous section, HIPAA compliance requirements are spread across the HIPAA Privacy Rule, HIPAA Security Rule, and the HIPAA Breach Notification Rule with the HIPAA Enforcement Rule, highlighting the penalties for non-compliance. We'll briefly outline some of the most important parts of each rule before covering them in depth, in their own section.

In the next section, we'll discuss each of these core aspects of HIPAA compliance, starting with the HIPAA Privacy rule and then working our way down.

What is the HIPAA Privacy Rule?

The HIPAA Privacy Rule can be thought of as the core component of HIPAA, with the other rules being subsets of the Privacy Rule. The key purpose of the Privacy Rule is to ensure the privacy of individuals protected health information. This is done through the establishment of standards like **minimum necessary**, which establish permissible uses of protected health information.

Defining PHI

With **protected health information** (PHI) being an essential part of the HIPAA Privacy rule, it's one of the key terms defined within **45 CFR Subpart A,** the general Provisions section of HIPAA. However, in order to understand what PHI is, it's important to understand what health information and individually identifiable health information are. This is because

PHI is a subset of **individually identifiable health information**, which itself is a subset of health information.

What is individually identifiable health information?

Given that individually identifiable health information constitutes PHI, it's also important to understand this term as well as the term "health information" more broadly, both of which are defined in **45 CFR § 160.103**.

Health information is any information, including **genetic information** that is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse.

This information must relate to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Individually identifiable health information includes the above definition of health information, but additionally it:

- Directly identifies the specific individual the health information pertains to, or…
- There is reasonable basis to believe the information can be used to identify the individual

In **45 CFR § 164.514(b)(2)**, in ***Requirements for the de-identification of protected health information***, the Privacy Rule calls out specific health information that must be removed to ensure that health information is not individually identifiable health information:

- Names
- All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes
- All elements of dates directly related to an individual, including birthdate, admission date, discharge date, date of death; and all ages over 89
- Phone numbers
- Fax numbers
- Email addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Full face photographic images and any comparable images
- Vehicle identification numbers; including license plates
- Device identifiers and serial numbers
- Web URLs
- IP addresses
- Biometrics, including fingerprints and voice prints
- Any other unique identifying number, characteristic, or code

What is protected health information (PHI)?

As defined in **45 CFR § 160.103**, PHI consists of individually identifiable health information that is:

- Transmitted by **electronic media**
- Maintained in **electronic media**

- Transmitted or maintained in any other form or medium

This however doesn't include individually identifiable health information:

- Contained in educational records (which are covered by FERPA)
- Contained in employment records for records held by a covered entity in its role as an employer
- For persons who've been deceased for more than 50 years

Putting this together with the definitions of **health information** and **individually identifiable health information**:

PHI is health information that includes some combination of the 18 HIPAA **PII** identifiers defined in **45 CFR § 164.514(2)(i)** that is transmitted or maintained in electronic media (or in any other form) **by a covered entity** like a healthcare provider, health plan, or healthcare clearinghouse for the purposes of the provision of care or payment for the provision of care.

Common examples of protected health information

Some common examples of protected health information include:

- A bill from a medical provider
- Results from a patient's medical test or diagnostic, like a blood test or X-ray in a patient's chart.
- A patient's after visit summary

Important exclusions to keep in mind about PHI protections are that they don't apply to:

- Information in educational records (these are instead covered by FERPA)
- Employment records that are managed by a covered entity in its capacity as an employer. However, should the employee become a patient of the covered entity, HIPAA will apply.
- Information that has been sufficiently de-identified. Mainly through the removal of the 18 identifiers specified in **45 CFR § 164.514(2)(i)**.
- Health information created or maintained by an entity that is not a covered entity or a business associate.

Below, we'll go over some common examples of what doesn't count as exposure of PHI.

Examples of what doesn't count as PHI

1. Example 1: Wearable device data not shared with or used by a covered entity

In many cases, **wearable device data doesn't meet the standard of PHI**. Information like data from a pedometer generally doesn't constitute health information by itself. More detailed biometric data, like heart rate, might rise to the level of PHI; however, if this data isn't created or maintained by a covered entity then it's not covered under HIPAA.

2. Example 2: An image of an MRI with no other accompanying PII or identifiers

In this example, because the MRI has no other identifiers attached, like a patient name or the date of admission providing context as to when the image was taken, it doesn't count as PHI.

Use and disclosure of PHI

In **45 CFR § 164.502**, HIPAA describes permitted, required, and prohibited uses and disclosures of PHI for covered entities and business associates. We're going to break these down in the sections below.

Permitted uses and disclosures of PHI for covered entities

Covered entities are **permitted** (but not required) to use or disclose PHI as follows:

- To the individual who is the subject of the information
- For a covered entity's own treatment, payment, or health care operations activities.

- For the treatment activities of any healthcare provider
- For the payment activities of another covered entity and of any healthcare provider
- The health care operations of another covered entity involving either quality or competency assurance activities or fraud and abuse detection and compliance activities
- As part of an incidental use and disclosure, which occur as a result of an otherwise permitted use or disclosure.
- As part of a limited data set from which specified identifiers of individuals and their relatives, household members, and employers have been removed. Such data sets can be used or disclosed for research, healthcare operations, and public health purposes, provided the recipient of the data enters into a data use agreement providing specified safeguards for the PHI in the data set.

Permitted uses and disclosures of PHI requiring an opportunity for individuals to consent

45 CFR § 164.510 lists other additional uses and disclosures that covered entities are **permitted to make, provided that they provide an opportunity for the individual to agree or object**:

1. **Facility directories**

A covered health care provider may rely on an individual’s informal permission to list in its facility directory the individual’s name, general condition, religious affiliation, and location in the provider’s facility. The provider can also disclose the individuals’ condition and location in the facility to anyone asking for the individual by name.

2. **Disclosure to family & other identified contacts**

A covered entity also may rely on an individual’s informal permission to disclose to the individual’s family, relatives, or friends or to anyone else the individual identifies, any PHI relevant to that person’s involvement in the provision of care or payment for care.

Additionally, a covered entity may rely on an individual’s informal permission to use or disclose PHI to notify contacts identified by the individual about the individual’s location, general condition or death.

3. **Disaster relief**

PHI may be disclosed for notification purposes to public or private entities authorized by law or charter to assist in disaster relief efforts.

Permitted uses and disclosures of PHI which don’t require authorization or consent

45 CFR § 164.512 lists uses and disclosures that covered entities are **permitted to make without seeking authorization or an opportunity to agree or object**:

- If required by law
- For victims of abuse, neglect or domestic violence
- Health oversight activities, such as for audits, and investigations for oversight of the healthcare system and government benefit programs
- For judicial and administrative proceedings if requested through a court order or administrative tribunal
- To funeral directors, coroners, or medical examiners either to identify a deceased person, determine a cause of death, or other functions allowed by law.
- To facilitate the donation and transplantation of organs and tissue.
- To lessen a serious and imminent threat to a person or the public or to identify or detain an escapee or violent criminal
- For essential government functions like the proper execution of a military mission or national security activities
- To comply with worker’s compensation and similar laws
- For research, provided that the covered entity obtains either:

1. Documentation that an alteration or waiver of individuals' authorization for the use or disclosure of protected health information about them for research purposes has been approved by an Institutional Review Board or Privacy Board

2. Representations from the researcher that the use or disclosure of the protected health information is solely to prepare a research protocol or for similar purpose preparatory to research, that the researcher will not remove any protected health information from the covered entity, and that protected health information for which access is sought is necessary for the research

3. representations from the researcher that the use or disclosure sought is solely for research on the protected health information of decedents, that the protected health information sought is necessary for the research, and, at the request of the covered entity, documentation of the death of the individuals about whom information is sought

→ To law enforcement officials for law enforcement purposes:

1. As required by law

2. To identify and locate a suspect, fugitive, material witness, or missing person

3. In response to a law enforcement official's request about a victim or suspected victim of a crime

4. To alert law enforcement about a person's death if the cause is believed to be in association with criminal activity

5. When a covered entity believes that PHI is evidence of a crime that occurred on its premises

6. During a medical emergency experienced by a covered healthcare provider to inform law enforcement about the commission and nature of a crime, the location of a crime, or victims and perpetrators of a crime.

Permitted uses and disclosures of PHI that require authorization

A covered entity can use or disclose PHI for the following for the following purposes provided they first get written authorization beforehand:

→ Sharing psychotherapy notes, unless being used by the covered entity who originated the notes for the purposes of treatment, or for training purposes and in defense within legal proceedings brought by the individual.

→ For the purposes of marketing. Marketing is defined as activities involving "financial remuneration" where a covered entity is compensated for providing the communication on behalf of a third-party.

Covered entities are prohibited from using or disclosing PHI in the following circumstances:

→ Using or disclosing genetic information for the purposes of underwriting

→ Selling of PHI

Use and disclosure of PHI for Business Associates

In **45 CFR § 164.502** HIPAA also describes permitted uses and disclosures for business associates.

→ Business associates are primarily allowed to use and disclose PHI as permitted or required by its business associate agreement (BAA).

→ Business associates can also use or disclose PHI to satisfy a covered entity's obligations with respect to an individual's request for information

→ Additionally, if the business associate is working with a subcontractor, it may disclose PHI and allow the subcontractor to create, receive, maintain, or transmit PHI on its behalf assuming it obtains satisfactory assurances (via a BAA) that the subcontractor will appropriately safeguard the PHI.

→ Business associates are required to share PHI when mandated by law or by a request from the OCR to determine compliance.

Explaining the HIPAA minimum necessary rule

Minimum necessary or the minimum necessary rule (MNR) is a standard defined briefly in **45 CFR § 164.502(b)** and elaborated on in **45 CFR § 164.514**. It requires that covered entities and business associates make reasonable efforts to limit the amount of PHI required to complete a task or fulfill a request to the minimum required to successfully carry out duties. Minimum necessary applies to uses of PHI, disclosures of PHI, and managing requests for PHI.

Achieving the minimum necessary for using PHI

In 45 CFR § 164.514(d), HIPAA specifies that covered entities can achieve **minimum necessary use of PHI** by:

- Identifying persons or classes of persons within the workforce who need access to PHI to carry out their duties
- Then, for each of these, the covered entity must identify the category or categories of PHI which are required to be accessed by these employees, as well as the conditions under which this PHI will be accessed
- Finally, a covered entity must make reasonable efforts to limit access as appropriate for each of the employees or groups who will be accessing PHI to ensure that the correct categories of PHI are accessed by the appropriate groups only when necessary

Achieving the minimum necessary for disclosures and requests of PHI

In 45 CFR § 164.514(3), HIPAA specifies that covered entities can achieve **minimum necessary disclosures and requests of PHI** by:

- Ensuring that for any routine and recurring request or disclosures, the covered entity implements policies and procedures (or standard protocols) that limit the PHI disclosed to what is reasonably necessary.
- Then for all other requests and disclosures, criteria must be designed to limit PHI disclosed to what is reasonably necessary for the purpose and requests for disclosure are reviewed on an individual basis.

45 CFR § 164.514(3)(iii) notes that covered entities, if reasonable under the circumstances, can trust that requests made by other covered entities, public officials, or by workforce professionals or business associates affiliated with the covered entity comply with the minimum necessary rule and fulfill them. This effectively provides reasonable reliance for any covered entity responding to these requests. However, the covered entity is not required to comply with such requests if it determines that they do not meet its own minimum necessary standard for requests of that nature.

Exceptions to the minimum necessary rule

Minimum necessary also does not apply to:

- Disclosures or requests by a healthcare provider for the purposes of treatment
- Uses or disclosures made to the individual or subject of the PHI
- Uses or disclosures made under an authorization
- Disclosures made to the OCR for the purpose of an investigation
- Or any of the other permitted uses and disclosures allowed by HIPAA

The importance of minimum necessary

Minimum necessary is a very significant part of the HIPAA Privacy rule, as minimum necessary is an essential determination that must be made when evaluating if HIPAA has been breached. Efforts to verify compliance with HIPAA will often revolve around demonstrating appropriate safeguards are in palace and that all uses and disclosures followed the minimum necessary standards.

To see an example of this in action, consider the story of a nurse **who was found in violation of HIPAA's minimum necessary rule**. Before preparing a patient for a procedure, she performed a "Time-Out" to inform the patient of what the procedure would entail, but as part of this explanation, she disclosed the patient's condition in a semi-private setting loud enough for other patients and non-relevant medical staff to hear.

The nurse claimed this was an incidental disclosure, which is allowed by HIPAA, however the original assessment was upheld as it was argued that disclosure of the patient's condition was not done for the benefit of the patient, nor was it required to inform the patient of what the procedure would entail. In effect, more information than what was needed to educate the patient about the procedure was disclosed.

While the example here focuses on oral disclosure of PHI, minimum necessary (and the Privacy Rule more broadly) applies to PHI in all of its forms. For security teams, the minimum necessary standard will be the bedrock for building the administrative and technical controls required by the Privacy and Security Rules.

What is a Business Associate Agreement?

A business associate agreement (BAA), sometimes referred to as a business associate contract, is a legal document put into place to establish how business associates can use PHI, as well as their obligations for protecting PHI and reporting breaches. BAAs are required for a covered entity to begin working with any entity that will be using and disclosing PHI in the course of their work. Business associates will also be required to execute a BAA with any subcontractors doing the same.

According to HIPAA a BAA must:

→ Determine what PHI the Business Associate will access and how they're permitted and/or required to use it.

→ Provide that the BA will not disclose protected health information save when permitted by the agreement or by HIPAA or by law.

→ Require that the Business Associate will use appropriate safeguards to secure PHI.

→ Require the BA to report any use or disclosure of information not allowed by contract.

→ Require the BA to make available to HHS its internal practices, books, and records relating to the use and disclosure of PHI in its capacity as a BA.

→ Outline procedures in the event of a data breach or unauthorized disclosure.

→ Enforce subcontractor compliance for any working involving a CE's PHI.

→ Detailed provisions for the termination of the agreement.

The official regulations can be found in **45 CFR § 164.504(e)** and a BAA template (along with a summary of the regulations) can be found **on this page**.

When is a BAA agreement required?

A BAA is required whenever a business associate will be handling protected health information. However, not every relationship between a covered entity and a service provider will entail a business associate relationship.

For example, disclosures by a covered entity to a healthcare provider for the purposes of treatment don't require a BAA. These are things like a hospital managing the care of a patient referred by a specialist, or a physician sending and receiving PHI for a patient's blood test from a lab. Relationships like these don't require business associate agreements.

Additional exclusions include:

→ Relationships with entities whose functions or services do not involve use and disclosure of PHI (or where access to PHI would be incidental at best). Examples include services like plumbing, electricians, landscaping, etc.

→ Relationships with entities that merely act as a conduit for protected health information, such as the US Postal Service, private couriers, or their electronic equivalents.

For more examples of exclusions, see **the following page**.

Is a BAA agreement required for SaaS and cloud providers?

Cloud adoption has accelerated for healthcare organizations, especially in the wake of COVID-19. As such, one question we're often asked is whether cloud service providers, especially SaaS providers, require a BAA.

In most cases, yes, cloud providers do require BAA contracts or agreements to be signed in order to provide services and typically, these providers will have a BAA agreement template that will be made available to you before you work with them.

While HIPAA Privacy and Security rule give some leeway in how you implement access and security controls, it's important to note that a number of cloud provider BAAs will specify specific platform settings that must be implemented before the BAA can take effect and the platform can be considered HIPAA-compliant.

For example, **Zendesk** specifies several configurations **that must be in place** on your Zendesk instance, like single sign on (SSO). The same is **true for Slack**. One of the **indicated requirements** for **making Slack HIPAA-compliant** is a cloud data loss prevention solution, like **Nightfall**.

Examples of other popular SaaS platforms that require BAAs include:

DocuSign

Microsoft Teams

Dropbox

Google Drive (which Nightfall natively integrates with)

Atlassian Cloud (which Nightfall natively integrates with)

We've prepared a checklist that includes questions you should ask any cloud provider you intend to work with. You can download it with the PDF version of this guide, or **as a standalone document**.

HIPAA Privacy Rule administrative requirements

Both the HIPAA Privacy rule and Security rule have requirements that determine how your compliance program should be structured, which has significant implications for security teams building out their compliance programs. These requirements have overlap, but are listed in different portions of HIPAA's text. We'll briefly cover the privacy rule's administrative requirements here, and detail how they interact with those in the security rule in a later section.

The privacy rule administrative requirements include the following standards:

- **Personnel designations –** Covered entities must assign:
    - A privacy officer/official who is responsible for development and implementation of privacy policies and procedures protecting PHI.
    - A contact person or office responsible for receiving complaints about violations and providing further information about the covered entity's **Notice of Privacy Practices**.
- **Training –** Covered entities must provide training to each member of the entity's workforce within a reasonable period of time after the employee joins.
- **Safeguards –** Covered entities must reasonably safeguard PHI from intentional or unintentional uses and disclosures that violate HIPAA as well as to limit incidental uses and disclosures made as part of an otherwise permitted use or disclosure. This can include practices like shredding sensitive documents once they're no longer needed, or locking paper records. The Security Rule has its own detailed safeguards for the protection of electronic protected health information.
- **Accepting and processing complaints –** Covered entities must provide a process for individuals to may complaints regarding their privacy policies and procedures, including regarding privacy violations of HIPAA.
- **Workforce sanctions –** Covered entities must create and apply sanctions against workforce members who fail to comply with privacy policies and procedures. This excludes whistleblowers and workforce member crime victims (as defined in **45 CFR § 164.502(j)**).
- **Mitigation of harmful effects** – covered entities must mitigate, to the extent practicable, any harmful effect that is known by the entity and stems from a HIPAA PHI violation or violation of internal policies.
- **Refraining from intimidating or retaliatory acts –** Covered entities may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual who exercises rights granted by HIPAA, including filing complaints.

- **Waiver of rights –** Covered entities must not require individuals to waive rights to file complaints to OCR as a condition of treatment, payment, or enrollment in a health plan, or be eligible for benefits.

The Privacy Rule includes additional standards that specify that covered entities must implement policies and procedures to comply with the standards above. Additionally, all policies and procedures must be maintained in written or electronic form, and the covered entity must maintain documentation demonstrating how each of these standards are being followed. The documentation must be maintained for at least six years from its creation date or the date when it was last in effect (whichever is later).

What is the HIPAA Security Rule?

The HIPAA Security Rule can be thought of as a critical sub-component of the HIPAA Privacy Rule. While the Privacy Rule applies to protected health information or PHI in all its forms, the Security Rule more narrowly impacts electronic protected health information or ePHI. Because the OCR recognizes the extensive impact of technology on healthcare delivery and communications, the security rule contains 16 specific safeguards, with detailed implementation specifications highlighting the objectives that must be met by the safeguard being implemented.

Because t**he HIPAA Security Rule protects ePHI**, it's important to understand what that is.

What is ePHI?

ePHI is any PHI that is created, stored, transmitted, and received in electronic formats or media. Because HIPAA was originally written in the earliest days of healthcare technology, the 2013 Final Rule amended the definition of electronic media to include more examples. These include:

- Hard drives
- Optical disks
- Memory cards

Additionally, electronic media includes transition media used to exchange information already in electronic storage media. These are things like:

- The internet, extranets, or intranets
- Private networks
- The physical movement of removable/portable digital storage

However, excluded from this definition are things like paper, voice, and telephone assuming that the information being exchanged did not exist in electronic form immediately before the transmission.

For an illustration, consider someone reading off a patient chart from their computer over the phone. This disclosure would involve ePHI as the information being exchanged did exist in electronic form immediately before the transmission. However, someone reading off handwritten notes containing PHI over the phone does not involve the disclosure of ePHI, as the information being exchanged did not exist in electronic form before the transmission occurred.

To understand how to identify ePHI, scroll up to the section "Defining PHI" to learn about the 18 PHI identifiers that should be removed when de-identifying individually identifiable health information.

Overview of the HIPAA Security Rule

The objective of the HIPAA Security Rule, as outlined in **45 CFR § 164.306** has four components which are highlighted in "general requirements":

1. Ensure the confidentiality, integrity, and availability of all ePHI created, received, maintained or transmitted.

2. Protect against any reasonably anticipated threats or hazards to the security and integrity of PHI.

3. Protect against any reasonably anticipated uses or disclosures that are not permitted or not required by the Privacy Rule.

4. Ensure compliance with the Security Rule by all workforce members.

We'll go over each of these below.

1. The CIA Triad & ePHI

The Security Rule's mention of "confidentiality, integrity, and availability" hearkens back to information security fundamentals, specifically a concept known as the **CIA Triad**. Each letter stands for a core principle that constitutes a part of the triad.

Confidentiality

Confidentiality refers to the privacy of the information in question. In order for information like PHI to be confidential, it needs to only be disclosed or accessed on a need to use or need to know basis by parties who are authorized to use, view, or share the information. This can be complex when different individuals have different privileges with regard to using vs sharing information, but the principle of limiting access to appropriate persons for use or transmission at the appropriate time remains the same.

In order to maintain confidentiality, physical and electronic access controls as well as identity verification should be put into place ensuring that requests, use, and disclosure of ePHI is monitored, logged, and when inappropriate, prohibited. Additionally, employees should be educated on when it's appropriate to use or disclose ePHI based on their roles and responsibilities.

Integrity

Integrity of information refers to whether it's been inappropriately edited, modified, destroyed, or otherwise tampered with. Integrity of data like ePHI is often maintained with access controls as well as encryption, especially when in transit.

Availability

Availability refers to data that is reliably accessible, not only when needed, but also when stored away. Ensuring availability means assessing the health of storage devices, maintaining ePHI, setting and monitoring uptime metrics for data stored on remote systems, backing up data in case of corruption or **ransomware attacks**.

The CIA triad forms the bedrock of a wide variety of industry security frameworks, such as the **NIST cybersecurity framework**. NIST or the National Institute of Standards and Technology is a part of the U.S. Department of Commerce and has helped create science and technology standards that are used across multiple industries. Although there are many great cybersecurity frameworks, the OCR has created a **HIPAA policy crosswalk** that maps HIPAA security rule implementation specifications to functions within the NIST framework.

This shouldn't be seen as an endorsement of NIST, per se, but rather it's a sign of the importance of leveraging security frameworks to structure how you build your security program and decide how to implement and layer your security controls. NIST is simply one example of a framework that you can use for this purpose.

If you want to learn more about NIST, you can **read our primer on it**.

2. Protecting against reasonably anticipated threats, hazards, uses, and disclosures

The notion of "reasonably anticipated" is a determination that requires **risk analysis** to assess, as understanding the scope of risks relevant to your specific organization will be crucial to understanding what constitutes "reasonably anticipated" threats to ePHI.

The third object of the Security Rule involves applying this standard to not only misuse of PHI, but also to reducing against disclosures and uses that are "not required" by the Privacy Rule. This is, in effect, enforcement of the minimum necessary rule applied to ePHI.

The HIPAA security rule formally contains risk analysis as a required implementation specification, which we'll cover below.

3. Workforce compliance

Workforce compliance essentially means educating your workforce on appropriate use and disclosure of ePHI, as well as the controls that are required to be maintained in order to monitor and ensure the protection of ePHI. Additionally, sanctions and penalties should be in place for workforce members who violate the policies and controls in place to ensure the security and privacy of ePHI.

Workforce education and management are both specified safeguards within the HIPAA Security Rule, which we'll cover below.

How to implement the Security Rule

45 CFR § 164.306 not only specifies the general requirements or objectives of the Security Rule, but it also details how organizations can go about building out the safeguards necessitated by the rule.

In 164.306 (b), within a section titled "Flexibility of Approach" HIPAA highlights that organizations can choose any security measure they deem appropriate to satisfy the security rule as long as they take into account:

1. The size and capabilities of the organization adopting the measures
2. The technical infrastructure of the organization
3. The costs of the security measures
4. The probability and criticality of potential risks to ePHI

Safeguards for the HIPAA Security Rule are outlined in standards contained within the rule, and each standard has a number of "**implementation specifications**" highlighting the objectives that must be met by the safeguard being implemented.

The Security Rule distinguishes between implementation specifications that are "required" and those that are "addressable."

Required implementation specifications are those that must be adopted completely. Addressable implementation specifications are those which the HIPAA-bound entity must make an assessment about the reasonableness and appropriateness of the safeguard. If implementing the specification is not deemed reasonable, the entity can choose not to adopt it. However, when doing, so documentation is required to justify what assessment was made and, if possible, find an alternative measure to implement.

Are "addressable" HIPAA Security Rule implementation specifications optional?

While the contrasting of the word addressable with "required" may lead you to believe that HIPAA is framing these terms as opposites, addressable implementation specifications are absolutely not "optional." HIPAA is merely giving you leeway in how you apply the particular objective to your program.

Typically, when an organization documents its reason for not implementing one of the addressable implementation specifications, it's because one or more alternative security measures it's already implemented fulfill that purpose.

Organizations should think carefully about not implementing an addressable implementation specification, and ensure they have good justification for not doing so if they don't have an alternative.

Typically, when an organization documents its reason for not implementing one of the addressable implementation specifications, it's because one or more alternative security measures it's already implemented fulfill that purpose.

Organizations should think carefully about not implementing an addressable implementation specification, and ensure they have good justification for not doing so if they don't have an alternative.

HIPAA Security Rule Safeguards

The Security Rule safeguards, which are the core of the Security Rule, are broken up into the following 3 categories:

- → **Administrative safeguards**. Administrative safeguards are the administrative actions, policies, and procedures that go into managing how to choose, implement, and maintain the security measures which will protect ePHI.
- → **Physical safeguards.** Physical safeguards are the measures, policies, and procedures in place to protect against hazards or intrusion of hardware, facilities, and equipment used to house or manage access to ePHI.
- → **Technical safeguards**. Technical safeguards are the technical implementations and policies that are used to protect the electronic systems storing ePHI as well as the ePHI itself, either while in use, transit, or storage.

Below is a table aligning each implementation specification under the safeguard and standard it belongs to.

How the HIPAA Privacy & Security Rules work together

Within HIPAA, the concepts of privacy and security are inextricably linked. It's not possible to have privacy without security, however the terms of the Privacy Rule should determine how you implement security policies and controls. While both Rules are intended to be implemented separately—safeguards implemented to satisfy the Privacy rule, don't necessarily satisfy those of the Security Rule—there is overlap for the two rules.

In a deck for a conference on the Security Rule, the OCR **provided two example violations** to illustrate this relationship, which we'll cover below.

HIPAA Privacy & Security Rule example violations

1. Example 1: No access controls in place

An existing information system with ePHI has no capability to provide access controls and workforce members are able to view more information than needed for their job function. The covered entity did not make a decision whether to implement procedural access controls. No additional safeguards or additional training were implemented.

– Privacy violation(s): Lack of minimum necessary §164.502(b); No administrative and technical safeguards §164.530(c); No specific privacy training § 164.530(b)

– Security violation(s): Lack of access controls §164.312(a)(1); No specific security training §164.308(a)(5)

2. Example 2: Failure to dispose of media no longer in use

As part of community outreach and charity efforts a covered entity donates surplus

workstations and servers to a special needs school. No procedures for device and media

controls including disposal and media re-use were developed by the covered entity. The

workstations and servers included PHI that was accessed by staff and volunteers at the school.

– Privacy violation(s): Lack of administrative and technical safeguards §164.530(c)

– Security violation(s): Lack of device and media controls policies and procedures 164.310(d)(1)

What is the HIPAA Breach Notification Rule?

The Breach Notification Rule is critical for specifying what constitutes a breach event regarding PHI or ePHI. In 45 CFR § 164.402 a breach is defined as any acquisition, access, use, or disclosure of protected health information in a manner not permitted under the Privacy Rule which compromises the security or privacy of PHI.

Exceptions to the HIPAA Breach Notification Rule

All incidents that result in acquisition, access, use, or disclosure of PHI prohibited by HIPAA are presumed to be breaches, unless the impacted organization is able to demonstrate that there's a low probability the PHI had been compromised, using a four part assessment that evaluates:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification

2. The person(s) who used the PHI and/or to whom any disclosures were made

3. Whether the PHI was actually acquired or viewed by anyone.

4. The extent to which the risk to the PHI was mitigated.

It's important to note, though, that this definition has exclusions listed in 45 CFR § 164.402(1), including:

- → Unintentional acquisitions, access, or use of PHI by an authorized workforce member operating in good faith within the scope of their authority, assuming it doesn't result in further use or disclosure
- → An inadvertent disclosure to an authorized person to someone else who is also authorized to have access to the PHI
- → An inadvertent disclosure to an unauthorized individual, where there's a good faith belief that the individual would not reasonably be able to retain the PHI.

Breach Notification Rule obligations for covered entities & business associates

The Breach Notification rule obligates HIPAA-bound organizations to notify:

- → Each individual whose unsecured PHI has been impacted, no later than 60 days after the discovery of the incident.
  - → Additionally, 45 CFR § 164.404(c) contains an implementation specification defining the contents of this correspondence, such as details of the breach event and what the individual can do to protect themselves.
- → For breaches involving more than 500 residents of a state or jurisdiction, prominent media outlets serving that jurisdiction must be notified.
- → The OCR must be notified of any breaches
  - → **If the breach impacts less than 500 individuals**, the impacted organization must maintain a log or documentation of the breach and no later than 60 days after the end of the calendar year, provide the notification to the OCR.
  - → **If the breach impacts more than 500 individuals,** the impacted organization will notify individuals, the media, and OCR contemporaneously unless requested by law enforcement to delay a notice (see **45 CFR § 164.412** – Law enforcement delay.)

The OCR has a **HIPAA breach decision tool** that can help you determine when an incident arises to the level of a breach that must be disclosed.

What are HIPAA violation penalties?

HIPAA has **steep violation penalties**. According to the HHS:

> From the compliance date to the present, the compliance issues most often alleged in complaints are, compiled cumulatively, in order of frequency:

- → Impermissible uses and disclosures of protected health information;
- → Lack of safeguards of protected health information;
- → Lack of patient access to their protected health information;
- → Lack of administrative safeguards of electronic protected health information; and
- → Use or disclosure of more than the minimum necessary protected health information.

We've covered some of these in depth **elsewhere**.

Within Section 1176(a)(1) of the HIETECH Act there is a table titled **Categories of Violations and Respective Penalty Amounts** that contains categories of HIPAA offenses along with their penalties.

Scenario	Description	Fine per Violation	Maximum Fine
Did Not Know	For a violation in which it is established that the covered entity or business associate did not know and, by exercising reasonable diligence, would not have known that the covered entity or business associate violated such provision.	$100 – $50,000	$1,500,000
Reasonable Cause	Reasonable cause means an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect. Reasonable diligence means the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.	$1,000 – $50,000	$1,500,000
Willful Neglect – Corrected	*Willful neglect means conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated.* For a violation in which it is established that the violation was due to willful neglect and was corrected during the 30-day period beginning on the first date the covered entity or business associate liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred,	$10,000 – $50,000	$1,500,000
Willful Neglect – Not Corrected	For a violation in which it is established that the violation was due to willful neglect and was not corrected during the 30- day period beginning on the first date the covered entity or business associate liable for the penalty knew, or, by exercising reasonable diligence, would	$50,000	$1,500,000

Next steps for HIPAA Compliance

Before concluding the guide, we wanted to highlight some important next steps for HIPAA compliance. While this guide is packed with information, we hope you'll continue to use it as a reference.

Useful tools for the next leg of your HIPAA compliance journey might include:

→ The implementation specification matrix we embedded above. This guide provides important guiding questions to keep in mind as you evaluate how to build out your HIPAA security program.

→ If you're planning on speaking to a cloud service provider about their HIPAA compliant processes, we've written **a checklist of questions you should ask.**

→ Our security playbook for remote-first organizations covers a variety of technologies that will be useful for anyone **fulfilling requirements** for the HIPAA Security Rule.

→ If you are specifically looking to be HIPAA Compliant on Slack, **read our guide**.

→ In addition to these resources, feel free to **schedule a call with us** to learn more about how we enable HIPAA Compliance across cloud environments.

Besides these resources, keep in mind that the HHS has **resources and materials** on its primary HIPAA for Professionals hub.

About Nightfall

Nightfall is the industry's first cloud-native DLP platform that discovers, classifies, and protects data via machine learning. Nightfall is designed to work with popular SaaS applications like **Slack**, **Google Drive**, **GitHub, Confluence**, **Jira,** and many more via our **Developer Platform**. You can schedule a demo with us via email at **sales@nightfall.ai**.

Nightfall™

Guide to HIPAA Compliance for SaaS Applications

Section A - Evaluating a provider's status as a Business Associate

1. Evaluating the Service Provider's Status as a HIPAA Compliant Entity

□ **The service provider is capable of executing a Business Associate Agreement (BAA)**

Vendors or service providers whose work requires them to handle PHI for a HIPAA covered entity must be able to sign and execute a BAA. Even if the provider's platform does support the requirements necessary for satisfying HIPAA, the BAA must be in effect before your organization can be in compliance with HIPAA. Often a provider's terms of service may clarify if and how the entity can execute a BAA.

□ **The service provider can satisfy your specific HIPAA use case**

Before executing a BAA, confirm with the provider that your specific HIPAA use case can be satisfied using their service. For example, a service like Slack is not sanctioned for communication between patients and healthcare providers but is suited for communication between providers. An organization seeking to use Slack to communicate with patients would not have an appropriate use case, even though the application serves other HIPAA compliant use cases.

Section B - Evaluating proper implementation of security controls

2. Implementing HIPAA Security Rule Technical Safeguards

□ **Adopt the appropriate product or tier of service**

SaaS applications can offer a variety of service tiers, however, not all of them may allow for the configurations or controls needed to maintain HIPAA compliance while using the application. Ensure that your organization purchases the tier or product(s) required for HIPAA compliance.

□ **Successfully implement the appropriate audit controls**

HIPAA covered entities leveraging digital technologies for sharing and storing ePHI must have mechanisms to record and examine access and other activities within systems that contain or use ePHI. Such mechanisms may be offered by the service provider or through marketplaces managed by the service provider. These can include (but are not limited to):

- Audit Logs
- Security Information and Event Management (SIEM)
- Data Loss Prevention (DLP)

□ **Ensure administrative and physical safeguards are in place**

The above items ensure your organization is compliant with the HIPAA Security Rule technical safeguards for ePHI. Beyond the HIPAA Security Rule technical safeguards, implementing facility and device level policies are essential. Make sure these are in place regardless of whether you adopt SaaS applications. Learn more here.

□ **Successfully implement the appropriate access controls**

HIPAA covered entities leveraging digital technologies for sharing and storing ePHI must have policies and solutions in place that limit access exclusively to authorized persons. Such solutions may be offered by the service provider or through marketplaces managed by the service provider. These can include (but are not limited to):

- Single Sign-on (SSO)
- Multi-factor Authentication (MFA)
- Data Loss Prevention (DLP)

□ **Successfully implement the appropriate integrity controls and ensure transmission security**

HIPAA covered entities leveraging digital technologies for sharing and storing ePHI must have policies and solutions in place that ensure ePHI isn't improperly altered or destroyed. Such solutions may be offered by the service provider or through marketplaces managed by the service provider. These can include (but are not limited to):

- Encryption at rest
- Encryption in transit
- Backup/Archival

Nightfall™

HIPAA Security Rule Implementation Specification Matrix

Implementation Specifications	Status	Safeguard	Description	Guidelines to Consider
Section I: Administrative Safeguards				
Risk Analysis	Required	Security Management Process 45 CFR § 164.308(a)(1)	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.	Risks assessments require you to survey and inventory risks specific to your org. Some questions to consider include: **-How does ePHI move throughout your systems? You should identify the lifecycle (creation, use, storage, deletion, etc.) of ePHI within your org.** **-Who are your high risk users? This can either be as a result of their position (they have the most access/privileges and are likely to be targeted by threat actors) or as a result of their behavior (they consistently engage in risky behavior)** **-What does your third party risk look like? What ePHI will third-parties have access to and what policies do you have in place to moderate their behavior?** **-What are potential sources of external access to ePHI from outside your org?** **-What are some environmental threats to your ePHI? What kinds of disruptions would such threats result in?**
Risk Management	Required		Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the Security Rule.	Based on your Risk Assessment, you'll most likely want to identify and adopt an appropriate security framework to address risks (i.e.NIST CSF, HITRUST, etc.) Regardless of how you go about this you should: **-Make sure your risk assessment has effectively categorized the different types of risks specific to your org as well as how severe or urgent they are.** **-Invest in the tools/controls necessary to maintain visibility into risks.** **-Set objectives for your security program based on the urgency and nature of the risks unique to your org.** **-Create metrics that measure and demonstrate how your security program is minimizing risks and mitigating the ones that emerge.**
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.	Being able to apply sanctions to workforce members who violate policy entails: **-That you have detailed security policies in place.** **-That these policies as well as any sanctions for violations of policies are clearly communicated to employees.** **-For good measure employees should be required to demonstrate competency around policies regularly through training and testing (See the section of our Remote-First Security Playbook on** building a high-quality security training program **for more on this).**
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.	To monitor and regularly audit logs, you'll want to make sure you: **-Have a way to monitor and digest logs for systems across your organization.** Many security teams invest in tools like a **Security Information and Event Manager (SIEM)** which allows their security tool alerts and system logs to feed into one place.
	Required	Assigned Security Responsibility 45 CFR § 164.308(a)(2)	Identify the security official who is responsible for the development and implementation of the policies and procedures required by the Security Rule.	As part of guidance for this rule the HHS notes that: **-This standard is comparable to the Privacy Rule standard that requires a privacy officer or official to be designated [45 CFR §164.530(a)(1)].** **-The security official and privacy official can be the same person, but are not required to be.**

Implementation Specifications	Status	Safeguard	Description	Guidelines to Consider
Authorization/Supervision	Addressable	Workforce Security 45 CFR § 164.308(a)(3)	Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed.	Implementing authorization and/or supervision could entail: **-Enforcing role-based access or using the identity lifecycle to manage the permissions and authorizations of users based on their function.** **-Additionally remediating violations that expose data to unauthorized users.** **-To accomplish this invest in controls that monitor for policy violations and/or restrict access based on attributes of the user.** For example, Nightfall's healthcare customers integrate our platform within SaaS environments like Slack and Gmail to monitor employee communications for potential PHI violations. When Nightfall detects a violation it can prohibit ePHI from appearing within channels, files, and other content accessible by unauthorized users. You'll need to think carefully about where ePHI is within your org and the persons who have access to it in order to determine what types of controls and policies make sense to satisfy this requirement.
Workforce Clearance Procedure	Addressable		Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	Procedures to manage an employee's access to ePHI to ensure it's appropriate: **-Can involve onboarding processes that ensure each individual employee is only given access to the systems and data they use in their regular work, based on role or function.** **-Can involve regularly reviewing employees' permissions to ensure that permissions are revoked for systems and data employees no longer used in the course of their work.** **-Finally, when an employee is terminated, make sure there is an immediate process to deprovision access to all systems.** For an overview of what this might entail, see the section titled "What is Identity and Access Management" in our Remote-First Security Playbook.
Termination Procedures	Addressable		Implement procedures for terminating access to ePHI when the employment of a workforce member ends or as required by determinations made as specified in the Workforce Clearance Procedure.	See above
Isolating Helathcare Clearinghouse Function	Required	Information Access Management 45 CFR § 164.308(a)(4)	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.	This implementation specification only applies in the situation where a health care clearinghouse is part of a larger organization. In these situations, the health care clearinghouse is responsible for protecting the ePHI that it is processing. Evaluating how to approach this requires understanding how ePHI flows between the clearinghouse and other entities within the org.
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.	Policies and procedures to authorize access to ePHI should: **-Determine who needs access to ePHI, when, and for what purpose.** **-Ensure there's a reliable way to verify employee identities to ensure the correct person is being granted access to systems and data.**
Access Establishment and Modification	Addressable		Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	Policies and procedures to manage access to ePHI should: **-Involve regular review of access logs and permissions to ensure that users are accessing only the resources they need.** **-Can involve tracking user permissions via the identity lifecycle, depending on the relationship of the user to the org.** **-Involve editing access to resources as the nature of a user's role changes or as the purpose of the ePHI evolves.**

Nightfall™

HIPAA Security Rule Implementation Specification Matrix

Implementation Specifications	Status	Safeguard	Description	Guidelines to Consider
Security Reminders	Addressable	Security Awareness Training 45 CFR § 164.308(a)(5)	Implement periodic security updates.	As part of guidance for this rule the HHS notes that: **-There are many types of security reminders that covered entities may choose to implement.** **-Examples might include notices in printed or electronic form, agenda items and specific discussion topics at monthly meetings, focused reminders posted in affected areas, as well as formal retraining on security policies and procedures.** **-Covered entities should look at how they currently remind the workforce of current policies and procedures, and then decide whether these practices are reasonable and appropriate or if other forms of security reminders are needed.** To provide a concrete example, we want to note that Nightfall's healthcare customers integrate our platform within their SaaS environments to monitor employee communications for potential PHI violations. When Nightfall detects a violation it can send a custom message to the employee who violated policy to remind them of how to appropriately share or disclose ePHI, before remediating the incident.
Protection from Malicious Software	Addressable		Procedures for guarding against, detecting, and reporting malicious software.	Under the Security Awareness and Training standard, the workforce must also be trained regarding its role in protecting against malicious software, and system protection capabilities. See Section A of our Remote-First Security Playbook to learn how to build a culture of security within your workforce.
login Monitoring	Addressable		Procedures for monitoring login attempts and reporting discrepancies	As part of risk management and audit logging you should monitor access to resources, including systems requiring authentication. Doing so can tell you if a malicious actor is trying to use credentials as opposed to a genuine user. As part of your work in satisfying this requirement you can also evaluate tools like **User and Entity Behavior Analytics (UEBA)** to apply heuristics that may proactively blog illegitimate and unauthorized users from misusing credentials.
Password Management	Addressable		Procedures for creating, changing, and safeguarding passwords.	You should create policies that: **-Determine password complexity for user accounts.** **-Determine how frequently passwords should be changed.** **-Encourage practices that employees must observe in managing their credentials (i.e. not storing passwords on sticky notes)**. Tools like Single Sign On or password managers can simplify this process and allow you to use a security solution to make it easier for you to monitor user behavior and enforce proper policies. For an overview of what this might entail, see the section titled "What is Identity and Access Management" in our Remote-First Security Playbook.
Response and Reporting	Required	Security Incident Procedures 45 CFR § 164.308(a)(6)	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; and document security incidents and their outcomes.	Incident response can involve: **-Determining how employees should respond to security incidents and disruptions based on their role and responsibilities.** **-Determining how the incident will be documented and remediated.** **-Determining how to evaluate the extent of the disruption caused by the incident and when the organization's function has returned to normal.** We discuss some of this in Section C of our Remote-First Security Playbook.
Data Backup Plan	Required		Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.	You should adopt policies and tools that help you: **-Identify critical ePHI that requires redundancies.** **-Store backups securely.** **-Develop a process for retrieving backups under the appropriate circumstances.**
Disaster Recovery Plan	Required		Establish (and implement as needed) procedures to restore any loss of data.	Guidance for this section notes that while you might have a general disaster recovery plan for your broader business, you need policies and practices in place to securely recover ePHI. For a broad overview of Disaster recovery see Section C of our Remote-First Security Playbook.

Implementation Specifications	Status	Safeguard	Description	Guidelines to Consider
Emergency Mode Operation Plan	Required	Contingency Plan 45 CFR § 164.308(a)(7)	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.	When a covered entity is operating in emergency mode due to a technical failure or power outage, security processes to protect ePHI must be maintained. This might include: **-Evaluating alternative security measures that should be already in place in the instance of a failure.** **-Identifying if there need to be manual procedures in place to secure ePHI during the emergency or enable normal operations once the emergency has passed.**
Testing and Revision Procedure	Addressable		Implement procedures for periodic testing and revision of contingency plans.	As part of guidance for this rule the HHS notes that: **-This implementation specification applies to all implementation specifications under the Contingency Plan standard, including the Data Backup Plan, Disaster Recovery Plan, and Emergency Mode Operations Plan.**
Applications and Data Criticality Analysis	Addressable		Assess the relative criticality of specific applications and data in support of other contingency plan components	As part of guidance for this rule the HHS notes that: **-This implementation specification requires covered entities to identify their software applications (data applications that store, maintain or transmit ePHI) and determine how important each is to patient care or business needs, in order to prioritize for data backup, disaster recovery and/or emergency operations plans. A prioritized list of specific applications and data will help determine which applications or information systems get restored first and/or which must be available at all times.**
	Required	Evaluation 45 CFR § 164.308(a)(7)	Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operations changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of the Security Rule.	As part of guidance for this rule the HHS notes that: **-Initially the evaluation must be based on the security standards implemented to comply with the Security Rule. Subsequent periodic evaluations must be performed in response to environmental or operational changes that affect the security of ePHI. The on-going evaluation should also be performed on a scheduled basis, such as annually or every two years. The evaluation must include reviews of the technical and non-technical aspects of the security program.**
Written Contract or Other Arrangement	Required	Business Associate Contracts and Other Arrangement 45 CFR § 164.308(b)(4)	Document the satisfactory assurances required by this standard through a written contract or other arrangement with the business associate that meets the applicable requirements of the organizational requirements [§164.314(a)] in the Security Rule.	As part of guidance for this rule the HHS notes that: **-To minimize additional work efforts, can existing business associate contracts, which involve ePHI, could potentially be modified to include Security Rule requirements**
Section II: Physical Safeguards				
Contingency Operations	Addressable	Facility access Controls 45 CFR § 164.310 (a)(1)	Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	As part of guidance for this rule the HHS notes that: **-Facility access controls during contingency operations will vary significantly from entity to entity.** **-For example, a large covered entity may need to post guards at entrances to the facility or have escorts for individuals authorized to access the facility for data restoration purposes. For smaller operations it may be sufficient to have all staff involved in the recovery process.** **-In the instance that some of the content of this procedure is also addressed within the organization's contingency plan, it could be valuable to combine it.**
Facility Security Plan	Addressable		Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	As part of guidance for this rule the HHS notes that: **-Facility security plans must document the use physical access controls. These controls must ensure that only authorized individuals have access to facilities and equipment that contain ePHI.** **-Plans must be reviewed periodically, especially when there are any significant changes in the environment or information systems.**

Implementation Specifications	Status	Safeguard	Description	Guidelines to Consider
Access Control and Validation Procedures	Addressable		Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.	As part of guidance for this rule the HHS notes that: **-The purpose of this implementation specification is to specifically align a person's access to information with his or her role or function in the organization. These functional or role-based access control and validation procedures should be closely aligned with the facility security plan.** **-The controls implemented will depend on the covered entity's environmental characteristics.**
Maintenance Records	Addressable		Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).	As part of guidance for this rule the HHS notes that: **-In a small office, documentation may simply be a logbook that notes the date, reason for repair or modification and who authorized it. In a large organization, various repairs and modifications of physical security components may need to be documented in more detail and maintained in a database.**
	Required	Workstation Use 45 CFR § 164.310(b)	Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.	As part of guidance for this rule the HHS notes that: **-The Workstation Use standard requires covered entities to specify the proper functions to be performed by computing devices as well as the proper environment for workstations (where to use, how to store).** **-Organizations might want to specifically identify devices that contain/have access to ePHI versus those that don't.** Organizations can address this with acceptable use policies that account for the locations where employees work, as well as the obligations employees have for ensuring the safety of devices
	Required	Workstation Security 45 CFR § 164.310(b)	Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.	As part of guidance for this rule the HHS notes that: **-While the Workstation Use standard addresses the policies and procedures for how workstations should be used and protected, the Workstation Security standard addresses how workstations are to be physically protected from unauthorized users.** **-As with all standards and implementation specifications, what is reasonable and appropriate for one covered entity may not apply. Your risk analysis should be used to help with the decision-making process.**
Disposal	Required	Device and Media Controls 45 CFR § 164.310(d)(1)	Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.	As part of guidance for this rule the HHS notes that: **-When covered entities dispose of any electronic media that contains ePHI they should make sure it is unusable and/or inaccessible.**
Media Re-use	Required		Implement procedures for removal of electronic protected health information from electronic media before the media are made available for reuse.	As part of guidance for this rule the HHS notes that: **-In addition to appropriate disposal, covered entities must appropriately reuse electronic media, whether for internal or external use. Internal re-use may include re-deployment of PCs External re-use may include donation of electronic media to charity organizations or local schools.**
Accountability	Addressable		Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	As part of guidance for this rule the HHS notes that: **-Many applications have configuration settings for automatic logoff. After a predetermined period of inactivity the application will automatically logoff the user.**
Data Backup and Storage	Addressable		Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.	As part of guidance for this rule the HHS notes that: **-This specification protects the availability of ePHI and is similar to the Data Backup Plan implementation specification for the contingency plan standard of the Administrative Safeguards, which requires covered entities to implement procedures to create and maintain retrievable exact copies of ePHI. Therefore both implementation specifications may be included in the same policies and procedures.**
Section III: Technical Safeguards				
Unique User Identification	Required		Assign a unique name and/or number for identifying and tracking user identity.	As part of guidance for this rule the HHS notes that: **-The Rule does not describe or provide a single format for user identification. Covered entities must determine the best user identification strategy based on their workforce and operations.**

Nightfall™

HIPAA Security Rule Implementation Specification Matrix

Implementation Specifications	Status	Safeguard	Description	Guidelines to Consider
Emergency Access Procedure	Required	Access Control 45 CFR §164. 312(a)(1)	Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	As part of guidance for this rule the HHS notes that: **-Access controls are necessary under emergency conditions, although they may be very different from those used in normal operational circumstances. Covered entities must determine the types of situations that would require emergency access to an information system or application that contains ePHI.**
Automatic Logoff	Addressable		Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	As part of guidance for this rule the HHS notes that: **-Many applications have configuration settings for automatic logoff. After a predetermined period of inactivity the application will automatically logoff the user.**
Encryption and Decryption	Addressable		Implement a mechanism to encrypt and decrypt electronic protected health information.	As part of guidance for this rule the HHS notes that: **-There are many different encryption methods and technologies to protect data from being accessed and viewed by unauthorized users. Evaluate your organizational structure to determine where encryption is appropriate (i.e. at rest, in-transit) and by what means to employ it.**
	Required	Audit Controls 45 CFR § 164.312(b)	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	As part of guidance for this rule the HHS notes that: **-It is important to point out that the Security Rule does not identify data that must be gathered by the audit controls or how often the audit reports should be reviewed. A covered entity must consider its risk analysis and organizational factors, such as current technical infrastructure, hardware and software security capabilities, to determine reasonable and appropriate audit controls for information systems that contain or use ePHI.**
Mechanism to Authenticate ePHI	Addressable	Integrity 45 CFR § 164.312(c)(1)	Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	As part of guidance for this rule the HHS notes that: **-In order to determine which electronic mechanisms to implement to ensure that ePHI is not altered or destroyed in an unauthorized manner, a covered entity must consider the various risks to the integrity of ePHI identified during the risk analysis. Once covered entities have identified risks to the integrity of their data, they must identify security measures that will reduce the risks.**
	Required	Person or Entity Authentication 45 CFR § 164.312(d)	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	As part of guidance for this rule the HHS notes that: **-Although the password is the most common way to obtain authentication to an information system and the easiest to establish, covered entities may want to explore other authentication methods**.
Integrity Controls	Addressable	Transmission Security 45 CFR § 164.312(e)(1)	Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	As part of guidance for this rule the HHS notes that: **-Protecting the integrity of ePHI maintained in information systems was discussed previously in the Integrity standard. Integrity in this context is focused on making sure the ePHI is not improperly modified during transmission. A primary method for protecting the integrity of ePHI being transmitted is through the use of network communications protocols. In general, these protocols, among other things, ensure that the data sent is the same as the data received. There are other security measures that can provide integrity controls for ePHI being transmitted over an electronic communications network, such as data or message authentication codes, that a covered entity may want to consider.**
Encryption	Addressable		Implement a mechanism to encrypt electronic protected health information.	As part of guidance for this rule the HHS notes that: **-As previously described in the Access Control standard, encryption is a method of converting an original message of regular text into encoded or unreadable text that is eventually decrypted into plain comprehensible text. The Encryption implementation specification is addressable, similar to the addressable implementation specification at §164. 312(a)(2)(iv), which addresses Encryption and Decryption.** It's important to note that this implementation specification explicitly refers to data in-transit, like for an employee sharing PHI over a network or the internet. As an illustration, Nightfall works with Virtru to enable encryption of PHI over Gmail, so that email communications containing specific PHI identified by your security program will automatically be sent encrypted.