## About This Course

HIPAA, the Health Insurance Portability and Accountability Act, was passed to allow people to carry insurance from one employer to another and to protect the privacy of a patient's personal health information.

The stimulus bill, officially titled the American Recovery and Reinvestment Act (ARRA), includes a section called the Health Information Technology for Economic and Clinical Health (HITECH) Act, which changed some of the provisions of HIPAA, especially in terms of enforcement.

In this course, you will learn how to comply with HIPAA, as amended by the HITECH Act.

---

## HIPAA/HITECH Overview

Before HIPAA, your personal medical information could have been used in ways you never anticipated, without your permission or even your knowledge.

HIPAA changed that by requiring the privacy of your Protected Health Information (PHI) through what are known as the Privacy and Security Rules.
This course focuses primarily on how HIPAA protects PHI through the Privacy Rule.

---

## The HITECH Act

The HITECH Act was mainly created to incentivize the health care industry to adopt Electronic Health Record systems. However, because electronic records have a greater risk of being compromised, increased safeguards were needed to ensure their protection.

The HITECH Act:

- Strengthened elements of the Privacy Rule.
- Directed HHS to conduct regular audits to ensure compliance.
- Authorized states' Attorneys General to bring actions under HIPAA.
- Dramatically raised the penalties for noncompliance.

## Penalties for Non-Compliance

Failing to comply with HIPAA regulations, as amended by HITECH, could lead to:

- **Disciplinary action**
- **Personal criminal penalties** under the law of up to ten years in prison and personal fines of up to **$250,000 USD**.

For each incident of non-compliance, organizations could be fined:

- **$60,000 USD per occurrence**
- Up to **$1.8 million USD per year** for each standard violated.

---

## Who Must Comply?

There are two types of organizations that must comply with HIPAA:

1. **Covered Entities**
   These include:
   - Healthcare providers
   - Health plans
   - Healthcare clearinghouses

## What Must Covered Entities Do?

Under HIPAA, Covered Entities must:

- Safeguard individuals' Protected Health Information (PHI) when they store or transmit it.
- Request, use, or disclose Protected Health Information (PHI) only as permitted by HIPAA.
- Provide individuals certain rights with respect to their Protected Health Information (PHI), as required by HIPAA.

Additionally, Covered Entities must:

- Provide a Privacy Notice that explains individuals' rights under HIPAA.
- Ensure group health plan documents comply with HIPAA, if applicable.
- Create HIPAA Privacy and Security policies and procedures.
- Appoint a Privacy Officer and Security Officer.

## Business Associates

The second type of organization that must comply is a **Business Associate**. Business Associates are companies or individuals who perform services for Covered Entities and who have access to Protected Health Information (PHI) from Covered Entities.

## Examples of functions performed by Business Associates include:

- Claims processing
- Pharmacy benefits management
- Management consulting
- Accounting services
- Administrative services
- Actuarial services
- Legal services
- Billing

---

## Rules for Business Associates

Before sharing Protected Health Information (PHI) with a Business Associate, the Business Associate must first sign a **Business Associate Agreement** in which they promise to comply with the HIPAA Privacy and Security Rule requirements.

No Protected Health Information (PHI) may be released to any Business Associate who has not signed this contract.

Additionally, the **HITECH Act** changed HIPAA so that many provisions of HIPAA are directly applicable to Business Associates. This means Business Associates:

- Must comply with both the terms of the Business Associate Agreement and directly with HIPAA rules.
- Are subject to periodic compliance audits.
- Are subject to direct regulatory actions and penalties.

**Note:** Business Associates are not required to provide Privacy Notices, as that is the responsibility of the Covered Entity.

## Scope of HIPAA

Please also note that the provisions of HIPAA generally apply equally in the private and public sectors. For example, both private and government-run hospitals are Covered Entities, and we act as a Business Associate when we provide services to either one.

Additionally, HIPAA applies nationwide. However, all state laws that provide stronger protections or give individuals more access to, or control over, their information apply alongside HIPAA. Be sure to verify with the Privacy Officer that you are in compliance with any additional state laws.

## What Information Is Protected?

The **Privacy Rule** applies to a class of information known as **Protected Health Information (PHI)**.

PHI is all information held or transmitted by a Covered Entity or its Business Associate, in any form or media, whether electronic (ePHI), paper, or spoken that relates to:

- An individual's past, present, or future physical or mental health,
- The provision of healthcare to the individual, and
- The past, present, or future payment for the provision of healthcare to the individual, where the information identifies the individual or gives a reasonable basis for identifying the individual.

---

## Reasonable Basis for Identification

Below are different examples of information that could identify the individual or provide a reasonable basis for identification.

If you are unsure whether information should be treated as PHI, seek clarification from your Privacy Officer.

- Name
- Social Security Number
- Email address
- A personal description
- Telephone number
- Birthdate
- License plate number
- Health plan number
- Photographs
- Zip code

## Privacy Administration

The rest of this course teaches you how to handle PHI and ePHI properly. However, it is not always obvious how you should handle PHI in a particular situation.

When in doubt, seek help from the **Privacy Officer**.

---

## Reporting and Mitigating HIPAA Breaches

The **Privacy Officer** is responsible for collecting information about possible HIPAA breaches and notifying the proper parties when a breach occurs. Because of the **HITECH Act**, in many instances, breach notifications are mandatory.

If you suspect a HIPAA violation has occurred within our organization or in an organization with which we share PHI, report this immediately to the **Privacy Officer**.

---

### Privacy Breach Notification Requirements

When a breach occurs, the Privacy Officer will alert the Covered Entity, and a breach notice will be sent to the affected individual(s), the media (if applicable), and HHS, as required by the HITECH Act.

## Definition of a Breach

A breach has occurred when **Unsecured PHI** has been acquired, accessed, used, or disclosed in violation of the Privacy Rule, and the disclosure compromises the security or the privacy of the PHI, unless one of the three exceptions applies, which are discussed later in this course.

---

## Unsecured PHI

**Unsecured PHI** is PHI that has not been rendered unusable, unreadable, or indecipherable through either of the following two methods:

- **Encryption**
- **Destruction**

It may be written, electronic, or oral.

So, if a laptop is lost with properly encrypted PHI, that is not considered a breach so long as the encryption key has not been breached. But if any hard copy PHI is lost or stolen, that is a breach, unless it has been shredded or otherwise destroyed so that it cannot be reconstructed or falls under one of the three exceptions.

## Internal and External Access

The notification requirement applies not only to unauthorized disclosures to outside parties, but also to intentional unauthorized access of PHI by people within our organization.
In other words, an employee intentionally snooping through files could trigger the notification requirement.

---

## Notification Requirement

A **Covered Entity** must notify affected individuals of any breach of privacy. A **Business Associate** must notify the Covered Entity it serves of a breach so that the Covered Entity may ensure notice to the affected individuals.
In addition, **Personal Health Record (PHR) vendors** must notify affected individuals.

**Note:** PHR vendors and their third-party service providers are regulated by the FTC and not HHS.

## Reporting Incidents

If you discover PHI has been impermissibly accessed, used, or disclosed, you must report it immediately to the **Privacy Officer**.

In such instances, our organization is required to conduct and document an analysis of the use or disclosure to determine if it is a breach.

---

## Breaches Affecting More than 500 Individuals

A **Covered Entity** that has a breach affecting more than 500 people in a single state or jurisdiction must notify **HHS** immediately and will be listed on the HHS website.
Furthermore, if a breach affects more than 500 individuals in a single state or jurisdiction, notice must also be provided to prominent media outlets following the discovery of a breach.

---

## Exceptions to the Breach Notification Requirement

Please keep in mind that it is the **Privacy Officer** that will determine if an incident is an actual privacy breach and whether individuals, HHS, or the media must be contacted.
Only the **Privacy Officer** or **public relations** should have any communications with the media regarding a breach.

## Determining if an Incident Is a Breach

We must presume that any impermissible use, acquisition, or disclosure of PHI is a breach, unless a low probability that the PHI has been compromised can be demonstrated. This is done through a risk assessment of the following factors:

- The nature of the unauthorized recipient of the PHI (e.g., an entity subject to privacy laws vs. one that is not)
- The nature and extent of the PHI involved (e.g., whether it contains information about what type of treatment an individual received vs. the bare fact that they were once treated at a hospital)
- Whether the PHI was actually acquired or viewed
- The extent to which the risk to the PHI has been mitigated (e.g., a reliable unintended recipient may be asked to execute a confidentiality agreement regarding the PHI to lower the risk of harm)

Finally, we consider whether one of the three exceptions applies

---

## Authorization

Generally speaking, an individual may authorize a **Covered Entity** or its **Business Associates** to access, use, or disclose PHI for any purpose. That authorization must be written, not oral, and may be submitted via paper form, fax, or electronic media. A valid authorization will describe:

- The PHI to be disclosed
- Who may receive or use the PHI
- Who may release the PHI
- An expiration date or event
- A statement of the individual's right to revoke the authorization and a description of how to do so
- A statement of the individual's right to refuse to sign the authorization
- The purpose of the use or disclosure

---

## Authorization Examples

Examples of when we require a signed authorization before we release PHI include:

- When releasing information to an employer from a pre-employment screening
- When releasing information to a pharmaceutical firm for marketing purposes

## An example of when we must get a signed authorization before PHI may be released to us include:

- When we are trying to help a plan participant get their claim paid.
  Because authorizations have very strict requirements, you should have your supervisor review all authorizations prior to disclosure of the PHI.

---

## When Is Authorization Not Required?

Keep in mind that authorization is not always required. For example, it is **NOT REQUIRED** when:

- Disclosing the individual's own health information to them
- Disclosing records for purposes of HIPAA enforcement
- Conducting public health and safety disclosures required by law
- Accessing, using, and disclosing PHI as necessary for treatment, payment, and healthcare operations (TPO)

In all other circumstances, authorization is required.

## Treatment

**Authorization is not required for treatment.** Treatment is providing, coordinating, or managing healthcare and related services for an individual.

Examples of treatment activities include:

- Examination and diagnosis
- Consultation among providers regarding an individual

- Laboratory analysis
- Pharmaceutical services

---

## Payment

**Authorization is not required for payment.** Payment includes:

- Activities by providers to obtain payment for healthcare
- Activities by health plans to provide payment for healthcare

Examples of payment activities include:

- Determining eligibility or coverage under a health plan and adjudicating claims
- Risk adjustments
- Billing and collections activities

## Healthcare Operations

**Authorization is not required for healthcare operations.** Healthcare operations include things such as:

- Quality assessment and improvement activities, including case management and care coordination
- Competency assurance activities, including provider or health plan
- Conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs
- Specified insurance functions, such as underwriting, risk rating, and reinsuring risk
- Business planning, development, management, and administration
- Business management and general administrative activities of the entity including, but not limited to, de-identifying protected health information, creating a limited data set, and certain fundraising for the benefit of the Covered Entity

## Please note that healthcare operations does not include marketing

---

## Marketing Limits

**PHI cannot be used for marketing products and services without authorization from the individual.** The rules defining what constitutes marketing are complex. Please consult the **Privacy Officer** before using any PHI for a purpose that might be construed as marketing.

---

## The Minimum Necessary Rule

The **HIPAA Privacy Rule** requires that we limit the use and/or disclosure of PHI to the minimum necessary to accomplish the intended purpose. In other words, employees should not request or have access to more PHI than is necessary to fulfill their job duties.

This rule applies both when communicating with other organizations and within our own organization.

## Limited Data Sets

As a **Business Associate**, our first goal is to utilize a limited dataset to accomplish our task, if practical. A **limited data set** is PHI that has been stripped of most identifiers such as name, phone number, social security number, email address, and employer. It may, however, include dates and certain address information such as city, state, and zip code.

---

## Limited Data Set Examples +

**Examples of Identifiers That Must Be Removed:**

- Name
- Postal address information, other than town or city, state, and zip codes
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Social security numbers
- Device identifiers and serial numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images

## Exceptions to the Minimum Necessary Rule

Note that the **minimum necessary rule** does not apply to:

- Healthcare providers treating individuals
- Disclosures to the individual about his or her own health information
- Uses or disclosures authorized by the individual
- Disclosures to HHS for HIPAA enforcement purposes
- Uses or disclosures required by law

---

## Limiting Disclosures

We have the right and, in some cases, the responsibility to limit the PHI we disclose to the minimum necessary, even if a person, business, or agency requests more.

If you suspect someone outside our organization is requesting more than the minimum necessary PHI, consult the **Privacy Officer** before releasing the PHI.

## Safeguarding PHI

**HIPAA** requires us to take reasonable steps to safeguard PHI and ePHI. We must do whatever we reasonably can, without compromising the quality of healthcare, to avoid accidentally disclosing PHI. This lesson will cover the key things you can do to protect PHI.

---

## Use Encryption When Transmitting PHI Electronically

Ensure all electronically transmitted **ePHI** is sent in an encrypted format, if possible.

Ask for assistance with encryption if necessary and remember that information transmitted over the Internet is **not encrypted by default**.

---

## Avoid Sending PHI via FAX

In general, PHI should not be transmitted via fax.

If transmission via fax is your only option, ask your supervisor for guidance.

---

## Use Encryption When Storing PHI Electronically

Ensure any **ePHI** stored on computers, or any other digital medium, is encrypted, if possible.

## Lock Up Hardcopy Files

Never leave sensitive documents containing **PHI** lying on your desk unattended where others can see them.

---

## Properly Dispose of PHI

Once **PHI** is no longer needed, it should be rendered unreadable before disposal. Hard copy files should be shredded, and electronic files should be digitally “wiped."

---

## Talk Behind Closed Doors

Hold conversations about **PHI** in non-public areas.

---

## Secure Your Desktop

Just as individuals and others might look at paper files left unattended on your desk; the same is true of computer monitors.

Never leave a computer unattended without logging off or locking the computer and place monitors such that unauthorized individuals cannot "shoulder surf," i.e., view the data on your monitor while you work.

## Foil Thieves

Remember that briefcases and laptops can be lost or stolen. Don't take **PHI** with you when you travel unless it is absolutely necessary.

And if you must take **PHI** with you, make sure that any electronic **PHI** is encrypted, including files stored on laptops, tablets, smartphones, or removable media, such as DVDs or USB drives.

---

## Leave only Name and Number on Voicemail

**HIPAA** permits us to leave messages via voicemail; it is best to leave only your name and number so the individual can call you back.

Do not leave medical information via voicemail.

## Right to Receive a Privacy Notice

Under the Privacy Rule, individuals have a right to receive a **Privacy Notice** from the Covered Entity, which explains:

- How **PHI** may be used,
- The individual's rights under **HIPAA**, and
- The individual's right to complain about perceived **HIPAA** violations.

Remember that a **Privacy Notice** acknowledgement does not give us the authority to release or use **PHI** in a way not allowed by **HIPAA**. For that, we must have a signed authorization from the individual, which is a separate form.

---

## Different Rules for Different Entities

Different kinds of organizations have different **Privacy Notice** rules.

**Privacy Notice Acknowledgements**

- **Direct Care Providers** have the most extensive **Privacy Notice** requirements, including obtaining **Privacy Notice Acknowledgements**.
- **Business Associates** need not provide a **Privacy Notice**.
- **Health Plans** must provide a **Privacy Notice** but need not obtain acknowledgment that the notice was received.
- **Healthcare Clearinghouses** need not provide a **Privacy Notice** as long as they act only in the capacity of a **Business Associate** with respect to the creation and transmission of **PHI**.

---

## Right to Inspect, Copy, and Amend PHI

With a few rare exceptions, individuals have the right to inspect, copy, and amend their medical records and other **PHI**.

It is the responsibility of the **Covered Entity** to inform individuals how to make a request to inspect, copy, or amend their **PHI**, to field those requests, and to provide the individuals access to their records within 30 days. State law may provide for a shorter deadline.

**Business Associates** must assist **Covered Entities** in this by providing access to and amendment of the **PHI** held by the **Business Associate**. **HHS** can directly penalize **Business Associates** for failing to do so. The

**Business Associate Agreement** contains the details of how the **Business Associate** must help.

---

## Exceptions to Right to Inspect, Copy, and Amend

Depending on state law, information held by:

- Prisons regarding inmates,
- Research information where the individual has agreed to limit his or her access (but only during the clinical trial),
- Certain psychotherapy notes that are not part of the medical record,
- Documents prepared in anticipation of litigation (but not the underlying **PHI**),
- A situation where access would harm the individual (subject to the review of an outside professional), and
- A situation where a personal representative of the individual wants to see the **PHI** and granting them access could cause substantial harm to the individual.

## Right to Request Electronic Copies

Individuals have the right to request an **electronic copy** of their medical records if a **Covered Entity** maintains their records in electronic format, i.e., **Electronic Health Records**.

If an individual requests a copy of their medical records, we may charge individuals for the cost of copying and sending the records, including electronic records, unless state law provides otherwise. The charge to the individual may not exceed the reasonable cost of labor involved, and the individual may direct that it be sent directly to another person or entity.

---

## Right to Amend

Individuals have the right to request a **Covered Entity** make corrections to their records.
The **Covered Entity** must make the requested corrections within 60 days or deny the request and comply with **HIPAA** denial formalities.
Insofar as the incorrect information exists in our possession, we must make the corrections too when notified by the **Covered Entity**.

---

## Our Responsibility for Informing Others of Corrections

It is also the responsibility of the **Covered Entity** to ask the individual whom it should inform of the correction and inform them.

Additionally, it must alert others to whom it has given incorrect **PHI**, and who may have relied on it to the detriment of the individual.
Our responsibilities in this case will depend on our **Business Associate Agreement** with the **Covered Entity**.

## Right to Request Restrictions on Disclosures

An individual may request that a **Covered Entity** restricts how it uses or discloses his or her health information for **TPO** (Treatment, Payment, and Operations).

Under **HIPAA**, it does not have to agree, but it and its **Business Associates** are bound by any restriction to which it does agree.

---

## Right to Request Restrictions on Disclosures

The **HITECH Act** adds that a **Covered Entity** must agree to the requested restriction if:

- The individual requests **PHI** not be disclosed to a health plan, and
- The **PHI** pertains only to services that have been paid for in full out of pocket.

As a **Business Associate**, we are bound by both types of restrictions as well.

---

## Right to Request Accounting of Disclosures and Access Report

**HIPAA** gives individuals the right to an accounting of certain disclosures that we have made of their **PHI** for up to six years preceding the request. Therefore, we must track all reportable **PHI** disclosures that have been made by us or one of our **Business Associates**.

---

## Accounting of Disclosures

We must account for all disclosures pertaining to:

- Public health activities (except potentially disclosures about abuse or neglect),
- Judicial and administrative proceedings,
- Law enforcement activities,
- Activities to avert a serious threat to health or safety,
- Military and veterans' activities,
- The Department of State’s medical suitability determination, and
- Government programs involving public benefits.

## Exceptions

We do not have to account for disclosures:

- That are part of a limited data set,
- Pertaining to treatment, payment, or healthcare operations, unless the **PHI** was part of an **electronic health record**,
- To the individual or their personal representative,
- To the individual's friends or family members when the individual is present or due to an emergency,
- To prisons regarding inmates, or
- For national security or intelligence purposes.

---

## Access Rights of Parents

A **parent** is generally a **personal representative** of their minor child under the Privacy Rule and has the same rights of access to **PHI** for their child.

The rule is the same in the case of a **guardian** or other person acting in place of a parent of a minor.

---

## State Law

The first exception to the parental right of access is when **state law** (or other applicable law) permits a minor to obtain a health service without parental consent and the child does so.

**Example:**

When a state law provides an adolescent the right to consent to mental health treatment without the consent of his or her parent, and the adolescent obtains such treatment without the consent of the parent, the parent is not the personal representative under the Privacy Rule for that treatment and has no right to access the **PHI** related to that treatment unless the child authorizes it.

---

## Court or Legal Requirements

The second exception to the parental right of access is when a **court** determines, or other law authorizes someone other than the parent to make treatment decisions for the child.

In order to not undermine these court decisions, the parent is not the personal representative under the Privacy Rule in these circumstances and has no right to related **PHI**.

## Parental Agreement

The third exception to the parental right of access is when a parent agrees to a confidential relationship between the minor and the physician.

---

## Emancipation of the Minor

If a minor is **emancipated**, they are treated as an adult and the parents or former guardians have no right to the minor's **PHI**.

---

## Abuse or Neglect

When a physician (or other Covered Entity) reasonably believes in their professional judgment that the child has been or may be subjected to abuse or neglect, or treating the parent as the child's personal representative could endanger the child, the physician may choose not to treat the parent as the personal representative of the child.

In that case, the parent has no right to **PHI** regarding the care.

## Right to Confidential Communications

Under the Privacy Rule, individuals can request that a direct care provider or health plan communicate with them by alternative means or at alternative locations.

- **Direct care providers** must accommodate such requests so long as they are reasonable.

- **Health plans** must do so if they are reasonable and the individual states that the disclosure could endanger them.

As a **Business Associate**, we are bound by the rules governing the Covered Entity we are serving.

---

## Right to Complain About Violations

Despite our best efforts, it is inevitable that individuals will occasionally object to our privacy practices or identify an instance of noncompliance. Not only do they have the right to lodge a complaint, we appreciate it when they do. Complaints enable us to perfect our privacy policy and monitor our **HIPAA** compliance.

### Filing Complaints

An individual's complaints may be filed either with our **Privacy Officer** or the U.S. Department of Health and Human Services' Office for Civil Rights, the organization responsible for investigating complaints and enforcing the privacy regulation.

- If an individual complains to you, take the complaint seriously, express your concern, and refer the person to the **Privacy Officer**.
- Health plans' and **Direct Care Providers**' Privacy Notices detail the procedure for lodging a complaint and the phone numbers to call for assistance with complaints.

---

## Intimidating and Retaliatory Acts

Our policy requires us to refrain from intimidating or retaliatory acts in all circumstances.

- **Individuals cannot be threatened** for filing a complaint with us or the Department of Health and Human Services, participating in an investigation, or any other reason.

### Examples of Inappropriate Behaviors

- Threatening monetary, physical, or other retaliation to prevent an individual from exercising their rights under HIPAA.
- Offering bribes to prevent an individual from exercising their rights under HIPAA.
- Retaliating verbally, physically, or otherwise against a person or entity who has exercised their rights under HIPAA.

---

## Waiver of Rights

Our policy also prevents us from forcing individuals to waive their rights under HIPAA as a condition of service.

This, together with our policy against intimidating and retaliatory acts, protects individuals' rights.

---

## Course Summary

Our obligation to safeguard **PHI** includes guarding electronic and hardcopy data as well as avoiding unintended verbal disclosures.

If you have any questions about your obligations under **HIPAA**, please do not hesitate to revisit any of these lessons or contact the **Privacy Officer**.