

COMPLYING WITH HIPAA  
for Covered Entities



How to Use This Course

- ✓ Introduction
- ✓ Using and Disclosing PHI
- ✓ Rights of Individuals
- ✓ Securing PHI
- ✓ Enforcement and Breach Notification
- ✓ Next Steps
- Assessment



## Lesson 1: Introduction

### Real People, Real Stories

When you visit the doctor's office, you trust that the information you provide will remain private and secure. You expect that as your medical records pass through the hands of dozens of employees—from registration to clinical staff to billing—only those with a legitimate need to know will access and use your information and that the integrity, availability, and confidentiality is secured at every step.

Our patients and clients trust that we will treat their information with the same care. But sometimes employee carelessness or misguided intentions keep this from happening. Check out what can happen when an individual's health information isn't properly protected:

#### **Medical Identity Theft**

Recently, I received an Explanation of Benefits statement containing charges for services I did not receive.

It turns out that someone had accessed my health information and used my insurance to pay for repeated office visits and treatments. It's going to take months to fix this.

#### **Criminal Snoop**

Rumor had it that a celebrity visited the Emergency Room in critical condition! Curiosity got the best of me and I peeked into the ER files to see who it was and what happened. I got excited and spread the gossip around.

It turns out that snooping can be a criminal offense—shortly after, I was fired, and the hospital was fined \$250,000 for violating federal medical privacy laws. Even worse, I could go to jail!

#### **Fax Number Mishap**

It was a hectic day, and I needed to fax some medical billing information to a client. In a rush, I typed in the wrong fax number and sent the information to the wrong recipient.

Apparently the fax contained health information, and my simple mistake was the cause of a privacy breach and violated federal healthcare laws.

# Lesson 1: Introduction

## HIPAA Overview

The Health Insurance Portability and Accountability Act (HIPAA) grants individuals the ability to access their Protected Health Information (PHI) along with certain other rights. It also requires our organization to establish policies and practices that ensure patients' PHI is protected and secure.

We follow HIPAA regulations because they're the law, but more so because they protect our patients and customers, giving them legal rights on who can access and use their PHI. In this course, you'll learn more about how you can protect our patients—and our organization—by following HIPAA regulations. Take a moment to review the course objectives.

## Course Objectives

Upon completing this course, you will be able to:

- Recognize the importance of HIPAA to individuals and our organization.
- Define the rights of individuals and your responsibility to ensure these rights are granted.
- Identify examples of PHI and how to protect its confidentiality when using and disclosing it.
- Recognize the consequences for non-compliant behaviors.
- Identify your responsibilities for reporting privacy and security incidents.

# Lesson 1: Introduction

## Protected Health Information (PHI)

Protected Health Information (PHI) is any health-related information that can be used alone or in combination with other information to identify an individual. HIPAA regulations apply to all PHI, regardless of how it is communicated—whether it is shared verbally, in writing, or through electronic methods.

PHI may be found in healthcare records, demographic information, payment information, insurance claims—the list is endless, so you must be careful and mindful.

### Help! What Is PHI?

- Names of individuals and relatives
- Postal addresses
- Dates
- Telephone and fax numbers
- E-mail addresses
- Social Security numbers
- Medical Record numbers
- Account numbers
- Health plan beneficiary numbers
- Certification/license numbers
- Automobile VIN and serial numbers
- Device identifiers and serial numbers
- URLs and IP addresses
- Biometric identifiers
- Full face photographic images

## Your Responsibility

Everyone at our organization must comply with HIPAA regulations. That means everyone who provides healthcare directly, health plans and clearinghouses (covered entities), but also anyone who works at an organization that handles any type of PHI (business associates and hybrid entities).

By following HIPAA regulations, you support our organization's commitment to ensuring the security and privacy of PHI. By providing high quality services that safeguard PHI, you also protect our reputation, and help us avoid costly penalties, legal sanctions, and litigation fees for violating the law.

## Did You Know?

Last year medical industry data breaches affected nearly 3 million confirmed individuals throughout the U.S.

## Knowledge Check

Now, you'll have a chance to help employees comply with HIPAA in the workplace. Review each person's scenario and determine the best actions to take for each situation.

### Scenario 1

Employee 1: "I'm worried about being liable for protecting PHI."

Employee 2: "Oh, don't worry! As employees, we don't really have to worry about all the HIPAA compliance. Our managers handle most of the compliance stuff."

Is this accurate information?

- Yes, only those employees who directly handle PHI need to comply with HIPAA regulations.
- No, everyone, regardless of your role, needs to know and comply with HIPAA regulations.

### Scenario 2

Employee "Oh my gosh! You won't believe who just got plastic surgery!"

Can this employee share this information?

- Yes, this is general information and not PHI.
- No, this is PHI and is against the law to share.

### Scenario 3

Employee: "Hmm, I wonder if I need to keep this patient billing information secure..."

Does the employee need to protect this information?

- Yes, these records contain PHI.
- Yes, but only from people outside of his workplace.
- No, the information in these records is not confidential.

### **Answer Key**

Scenario 1: No is Correct. All employees are contractually and legally obligated to comply with HIPAA and our organization's policies and procedures.

Scenario 2: No is Correct. Any information pertaining to the healthcare of an individual is PHI and cannot be shared or accessed unless there is an authorized need to know.

Scenario 3: Yes, these records contain PHI is Correct. Medical claim forms, patient contact information, healthcare billing statements, and explanation of benefits forms all contain PHI and need to be safeguarded.

### **Summary**

You have completed this lesson providing an overview of HIPAA.

Here are the key points covered:

- HIPAA requires us to keep patients' information secure and private.
- PHI is information that can be used alone or in combination with other information to identify an individual.
- HIPAA regulations apply to all PHI, regardless of the method it is stored or communicated.
- Everyone is responsible for complying with HIPAA regulations and our organization's privacy and security policies and procedures—even if your job duties do not directly include working with PHI.

## Lesson 2: Using and Disclosing PHI

### HIPAA Privacy Rule

HIPAA defines the permitted uses and disclosures of PHI. The HIPAA Privacy Rule states that PHI can only be used and disclosed to the minimum necessary for treatment, payment, and healthcare operations purposes. The minimum necessary standard requires us to evaluate our practices and enhance safeguards as necessary to:

- Limit unauthorized or inappropriate access to PHI.
- Limit unauthorized disclosures of PHI.

Take a moment to learn more about the allowable purposes for sharing PHI in Treatment, Payment, and Healthcare Operations purposes.

#### Treatment

Treatment activities include:

- The provision, coordination, or management of healthcare and related services among healthcare providers or by a healthcare provider and a third party.
- Consultation between healthcare providers regarding a patient.
- Referral of a patient from one healthcare provider to another.

#### Payment

Payment activities include:

- Determining eligibility or coverage under a healthcare plan and adjudication claims.
- Risk adjustments.
- Billing and collection activities.
- Reviewing healthcare services for medical necessity, coverage, justification of charges, etc.
- Utilization review activities.
- Disclosures to consumer reporting agencies.

#### Healthcare Operations

Healthcare Operations activities include:

- Quality assessment and improvement activities.
- Underwriting and other activities related to creating, renewing, and replacing health insurance or benefits contracts.
- Medical review, legal, and auditing services.
- Business planning and development.
- Business management and general administrative activities.

## Lesson 2: Using and Disclosing PHI

### Use, Disclosure, and Request

The HIPAA Privacy Rule also regulates the use, disclosure, and request of PHI. Take a moment to learn more about how these terms apply to your job functions.

#### Use – Definition and Guidelines

Refers to activities conducted in routine business activities. Only those involved in the treatment, payment, or operations may share, apply, utilize, examine or analyze PHI.

#### Disclosure – Definition and Guidelines

Refers to how PHI is shared between departments or outside of our organization. It includes the release, transfer, access, or divulgence of PHI. Disclosing PHI may be necessary for operational purposes but is subject to certain limitations.

#### Request – Definition and Guidelines

Refers to any situation where an individual of our organization requests and/or is requested to disclose PHI to an outside entity. Requests for PHI may be necessary for operational purposes, but are subject to certain limitations.

### Types of Disclosures

It is critical to understand the limitations around disclosing PHI. Most disclosures fall into the following three categories:

- Permitted disclosures for treatment, payment, and healthcare operations.
- Disclosures following an “Opportunity to Object.”
- Disclosures required by law.
- Disclosures requiring authorization.

Take a moment to learn more about these types of disclosures by reviewing the examples provided.

#### Permitted Disclosures

“I need to share a patient’s PHI with her insurance company for billing purposes. Is this OK?”

You can share information with other providers, pharmacies, labs, etc., involved in the patient’s care or with the patient’s health plan to obtain payment.

### **Disclosures Following an Opportunity to Object**

“A family member is requesting information on a patient. Since they’re family, I can go ahead and share this.”

Sharing information with a patient’s family and friends—or including a patient in the facility directory—can occur only after the patient has been given an opportunity to object or “opt-out” of these types of disclosures.

### **Disclosures Required by Law**

“I received a subpoena for PHI provided by our customer, so I can disclose this information.”

We are legally required to disclose information in certain situations, being subpoenaed is one of them. Always follow our organization’s policies for handling this type of disclosure.

### **Disclosures Requiring Authorization**

“One of our employees was admitted to your facility this morning. How is he doing?”

Disclosing PHI to a patient’s employer without proper authorization is illegal. All disclosures not related to the patient’s treatment, payment for the treatment, and healthcare operations require authorization—except for requests required by law.

## **Knowledge Check**

Now, you’ll have a chance to help employees properly use and disclose PHI. Review each person’s scenario and determine the best actions to take for each situation.

### **Scenario 1**

Front desk receptionist: “Eww! What a gnarly fracture!”

Is this employee violating HIPAA law by viewing this x-ray?

- Yes, she has no business need to view a patient’s x-ray.
- No, viewing an x-ray does not violate privacy regulations.

### **Scenario 2**

Patient: “Now, do I need to call the insurance company myself to provide my information? It would be great if you would call them for me!”

Employee: “No, Mrs. Jenkins. Our staff will take care of that for you.”

Is this correct?

### Scenario 3

Manager: “I heard a rumor that one of my employees was hospitalized for substance abuse, which may affect his work eligibility. What was he admitted for?”

Nurse: “Hmm...let me check.”

Does releasing patient information to an employer without authorization violate HIPAA regulations?

- Yes, authorization is required before disclosing PHI to a patient's employer.
- No, releasing PHI to a patient's employer is permitted if it could affect his workplace status.

#### Answer Key:

Scenario 1: Yes is correct. The receptionist does not have a business need to view this PHI. Accessing, using, or disclosing PHI without authorization from the patient violates HIPAA regulations.

Scenario 2: No is correct. A covered entity can share information with other providers, pharmacies, labs, etc., involved in the patient's care or to the patient's health plan to obtain payment.

Scenario 3: Yes is correct. Disclosing PHI to a patient's employer—or even looking at the patient's file—is not permitted without proper authorization.

### Summary

You have completed this lesson on using and disclosing PHI.

Here are the key points covered:

- PHI can be used or disclosed to the minimum necessary for treatment, payment, and operations purposes.
- Only those involved in the treatment, payment, or operations may share, apply, utilize, examine, or analyze PHI.
- Most disclosures require authorization.

## Lesson 3: Rights of Individuals

### Notice of Privacy Practices

HIPAA regulations are based on requirements and standards concerning individuals' rights to their PHI. That's why our organization provides every patient with a Notice of Privacy Practices.

The Notice of Privacy Practices describes how a patient's PHI may be used or disclosed, as well as the rights the patient has regarding that information.

This notice must be provided to patients the first time they present for service, whether it is in person, over the phone, or through electronic means. A copy of this notice must also be posted at the location of the service.

#### Did You Know

Covered individuals are those who receive treatment under a healthcare plan.

### Rights of Individuals

You have an ethical and legal responsibility to ensure individuals' rights to their PHI are granted as outlined in the Notice of Privacy Practices. Let's take a closer look at these rights.

#### Did You Know

Denying patient requests for copies of their medical records was reported as one of the top HIPAA complaints.

#### Individuals have a right to:

- Inspect and request a copy of their PHI.
- Amend their PHI.
- Request an accounting of all PHI disclosures—note that some exceptions apply.
- Request confidential communications of their PHI by alternative means.
- Request restrictions on uses and disclosures of their PHI.
- Obtain a paper copy of the Notice of Privacy Practices.
- File a complaint regarding the privacy and security of their PHI.

## Lesson 3: Rights of Individuals

### Handling Requests

You protect individuals' rights by handling requests appropriately, obtaining authorization for use and disclosure when necessary, and processing complaints in accordance with our policies. In general, all requests should be referred to the appropriate person within our organization, such as our Privacy Officer.

Take a moment to explore examples of requests and procedures for handling these requests.

### Right to File a Complaint

"I have been denied service based on information in my health record. I think my PHI has been disclosed illegally."

#### Your Responsibilities

In this situation, you should:

- Inform the individual of his right to file a complaint if he suspects his privacy rights have been violated.
- Refer the complaint to the appropriate person within our organization.

### Request to Amend Record

"I need to correct the way a service is coded in my health record."

#### Your Responsibilities

In this situation, you should:

- Explain that the patient has a right to request an amendment, and it's the provider's decision whether to accommodate the request. If the provider denies the request, the patient can submit a letter of disagreement that will be included in the record.
- Refer the request to the appropriate person within our organization.

### Written Authorization

"I need a spreadsheet of our patients' contact information for marketing purposes."

#### Your Responsibilities

In this situation, you should:

- Explain that using or disclosing PHI for marketing purposes is outside the scope defined by our organization and allowed under HIPAA and State law.
- Explain that we would need to obtain written authorization from all patients to use or disclose their information before fulfilling this request.

## Lesson 3: Rights of Individuals

### Request to Limit Access

“I’d like to limit who has access to my medical information.”

#### Your Responsibilities

In this situation, you should:

- Inform the individual that he has a right to request a restriction or limitation on the PHI we use or disclose for certain specified reasons.
- Refer the request to the appropriate person within our organization. Note that our organization is not required to agree to the restriction request in most instances.

### Knowledge Check

Now, you’ll have a chance to help employees ensure that individuals’ rights are respected. Review each person’s scenario and determine the best actions to take for each situation.

#### Scenario 1

Voice on telephone: “... and I know that I did not authorize you to share my information! I can’t believe this is happening to me ...”

What should this employee do to process this patient complaint?

- Reassure the patient that her situation will be resolved immediately.
- Transfer the call to his manager.
- Refer the complaint to the appropriate person within our organization.

#### Scenario 2

Employee: “I need medical information on the following patients in order to process insurance claims.”

Does this request for information comply with HIPAA regulations?

- Yes, requesting information associated with the payment for healthcare is allowed.
- No, only medical and legal requests for PHI are compliant with HIPAA regulations.

#### Answer Key

Scenario 1: Refer the complaint is correct. All complaints of this nature should be referred to the appropriate person within our organization. In most situations, this will be our privacy officer.

Scenario 2: Yes is correct. Requests made for PHI that deal with healthcare treatment, payment, or operations comply with HIPAA regulations.

## Lesson 3: Rights of Individuals

### Summary

You have completed this lesson on individuals' rights to their PHI.

Here are the key points covered:

- The Notice of Privacy Practices describes how patients' PHI may be used or disclosed, as well as the rights patients have regarding that information.
- It's your responsibility to ensure individuals' rights to their PHI are granted as outlined in the Notice of Privacy Practices.
- Individuals have a right to make requests and file complaints regarding the use of their PHI, and you must ensure requests and complaints are directed to the appropriate person.

## **Lesson 4: Securing PHI**

### **Securing PHI**

HIPAA regulations define the standards required for securing PHI.

Our organization must maintain reasonable administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of PHI. All employees are required to adhere to these safeguards to ensure that all PHI, regardless of its form (e.g., paper, electronic, spoken, etc.), is secure.

Securing PHI not only ensures we keep our customers' trust, but also reduces the risk of incidents—and severe legal consequences.

### **Physical Safeguards**

You can minimize the risk of unauthorized access to PHI by following physical security practices in your workplace.

Review some of our organization's policies for physical security by reviewing the security controls below.

#### **Secure Storage and Disposal**

- Keep PHI out of clear view from the public (desks, copiers/fax machines) and stored in secure areas.
- Dispose of documents and electronic media containing PHI in secured containers or by shredding.

#### **Mobile Device Security**

- Physically secure your laptop and other mobile equipment with security cables or in locked drawers.
- Never leave your laptop or smart phone unattended in the office, in your car, or when travelling.
- Password protect mobile devices such as PDAs, smart phones, and USB drives.

#### **Access Control**

- Always keep office doors and cabinets locked.
- Do not allow anyone to follow you into a secure location. Ensure that anyone who enters swipes his or her badge.
- Always follow our organization's policies for accessing PHI.
- Only discuss PHI in private settings to avoid eavesdropping.

## Lesson 4: Securing PHI

### Technical Safeguards

When accessing, storing, and/or transmitting PHI on computers, smart phones, USB drives, and other electronic devices, be sure that you follow our organization's procedures related to:

- Accessing networks.
- Encrypting e-mail and files containing PHI.
- Using passwords.
- Installing and modifying software.
- Take a moment to learn how our organization implements technical safeguards.

#### Did You Know

There are over 370 passwords that have been identified as the most commonly used and "hackable" passwords. Do your research, and be sure you aren't using one of them!

### Technical Safeguards

- Use passwords that consist of a combination of characters, such as upper and lowercase letters, numbers, and possibly special characters.
- Set your laptop or mobile device's screensaver to require a password and appear automatically when the device is not in use.
- Never share your password with anyone, including family, friends, or coworkers.
- Encrypt CDs and all mobile devices, such as USB drives, containing PHI.
- Only connect to approved and secure networks when accessing PHI.

### Knowledge Check

Now, you'll have a chance to help employees secure PHI in the workplace. Review each person's scenario and determine the best actions to take for each situation.

#### Scenario 1

Employee: "Hold the door! I forgot my badge."

Should this employee hold the door open for another employee when entering a secured area?

- Yes, if the person is in the building, he must be a valid employee.
- Yes, but only if the employee has valid ID.
- No, all employees need to scan their badges to enter the secured area.

## Scenario 2

Employee 1: ““I can’t access this system with my password. I was just in the system yesterday!”

Employee 2: “Hmm...They must be in the middle of a system update. Here, go ahead and login as me.”

Does sharing your login credentials violate our organization’s security policy?

- Yes, you should never share your login or password with anyone.
- No, as long as you change your password immediately afterwards.
- No, you can share passwords with managers or the IT department.

### Answer Key

Scenario 1: No is correct. It is a security violation to allow anyone to follow you into a secure location. Ensure that anyone who enters scans his or her badge.

Scenario 2: Yes is correct. It is against our security policy to share your password with anyone, regardless of their position in our organization. Sharing passwords allows unauthorized people to access information, which violates HIPAA regulations.

## Summary

You have completed this lesson on securing PHI.

Here are the key points covered:

- All employees are responsible for protecting PHI.
- Always follow our organization’s procedures for accessing, transmitting, storing, securing, and disposing of PHI.

## **Lesson 5: Enforcement and Breach Notification**

### **HIPAA Enforcement and Penalties**

In addition to specifying the ways that PHI must be protected, HIPAA regulations also contain specific penalties for failing to protect PHI. Any improper release, acquisition, use, or disclosure of PHI may be a violation of HIPAA regulations.

These types of incidents not only violate individuals' privacy rights—and their trust in our organization—but also may have severe consequences ranging from significant fines to criminal penalties. Monetary penalties and legal sanctions exist to prevent incidents from occurring and also provide consequences for those who violate HIPAA rules and regulations.

Everyone in our organization is legally obligated and accountable for following HIPAA regulations as well as our organization's privacy and security policies and procedures.

### **Types of Violations**

The biggest risks to maintaining the privacy and security of PHI usually occur from within our organization. We must protect against violations, whether caused by a lack of someone following the appropriate privacy and security procedures, or by a malicious attempt to steal information.

Take a moment to learn more about privacy and security violations.

### **Privacy and Security Violations**

HIPAA legislation increases the penalty amounts based on the level and intent of a breach of privacy.

All incidents are classified and penalized according to their type.

Examples include:

- Faxing a document containing PHI to the wrong number.
- Sending lab results to the wrong patient.
- Giving discharge instructions to the wrong patient.
- Leaving a computer logged on and unattended.
- Leaving passwords in plain view of others.
- Using ePHI without the proper security controls.

## Lesson 5: Enforcement and Breach Notification

### Breach Notification

To comply with HIPAA, our organization must investigate all privacy and security incidents in which PHI has been improperly accessed, acquired, used, or disclosed. This requirement applies to all forms of PHI and includes all unauthorized types of access and disclosures—inside and outside of our organization.

We must also notify individuals of the incident if the breach poses significant risk or harm to the privacy or security of their information.

To ensure we fulfill these requirements, you are responsible for promptly reporting suspect actions—no matter how minor they may appear—through our organization’s incident reporting process.

#### Did You Know?

If an incident affects more than 500 people, our organization must notify the media.

### Knowledge Check

Now, you’ll have a chance to help employees report incidents in the workplace. Review each person’s scenario and determine the best actions to take for each situation.

#### Scenario 1

Employee: “Uh oh. I just e-mailed a patient’s contact information to the wrong address...”

What should this employee do?

- Wait to see if the e-mail bounces back before doing anything.
- Nothing. Mistakes like this happen all the time.
- Consider this to be an incident and report it.

#### Scenario 2

Employee: “Who threw this patient’s contact information away in the regular garbage? I wonder who saw this...”

What should this employee do?

- Nothing. No one will ever see it beyond the facility.
- Remove the record from the trash can and report the incident.
- Notify the patient immediately.

### **Answer Key**

Scenario 1: Report this incident is correct. Although mistakes do happen, sending PHI to an unauthorized party is an incident and, by law, must be reported.

Scenario 2: Remove and report is correct. Finding unsecured PHI is a violation. The PHI needs to be secured and the incident needs to be reported immediately.

### **Summary**

You have completed this lesson on HIPAA enforcement and notification.

Here are the key points covered:

- An incident is defined as the suspected or known improper access, acquisition, use, or disclosure of PHI.
- Everyone in our organization is responsible and accountable for following our organization's procedures for safeguarding PHI and promptly reporting incidents.
- To comply with HIPAA, our organization must investigate all suspected or known privacy incidents in which PHI may have been improperly accessed, acquired, used, or disclosed.

## Lesson 6: Next Steps

### Summary

Congratulations! You've completed this training on HIPAA regulations and compliance.

Here's a quick review of the key points covered in the course:

- HIPAA requires us to keep patients' information secure and private.
- You must follow our organization's policies and procedures when using, disclosing, transmitting, storing, or requesting PHI to ensure that individuals' rights are respected.
- PHI may be used and disclosed to the minimum necessary for treatment, payment, and healthcare operations purposes.
- Unauthorized access of PHI has severe consequences to our patients and our organization, and you are obligated to comply with HIPAA standards to ensure PHI remains secure.
- You have a responsibility to identify and promptly report privacy and security incidents using our organization's reporting policies and procedures.

### Next Steps

Remember, HIPAA compliance begins with you!

If you have any questions regarding HIPAA compliance or your role in enforcing HIPAA rules and regulations, contact our organization's privacy or security officers.

### Resources

Privacy complaints, requests, and incidents should be reported to our organization's Privacy Officer. HIPAA privacy & security policies are located in Lucidoc.

### Contact Information

Privacy Officer:	Sheila Green-Shook
Telephone #:	425-899-1939
Hot Line #:	425-899-5599
Email:	<a href="mailto:sgreenshook@evergreenhealthcare.org">sgreenshook@evergreenhealthcare.org</a>