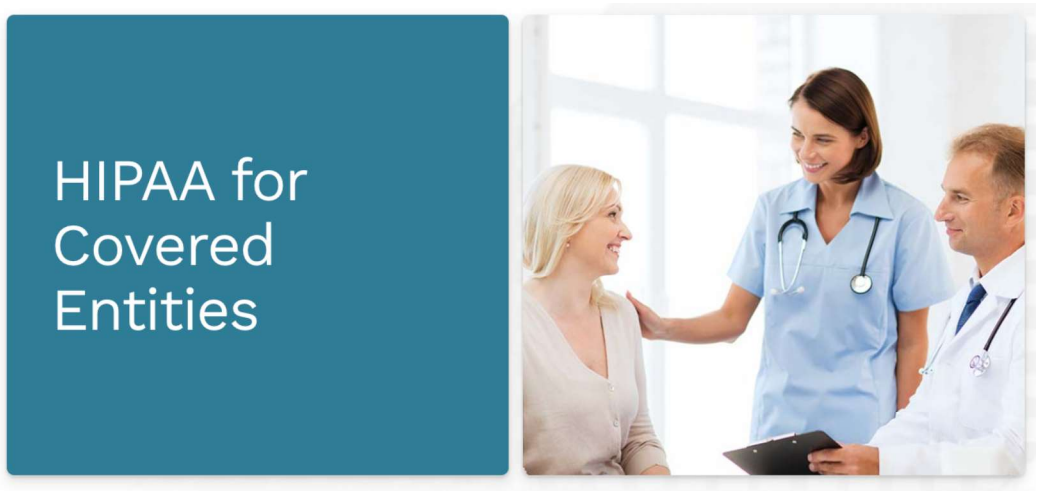
HIPAA for Covered Entities



PDF Terms of Use

This PDF version of this module is intended to be provided as an alternate format of transmission to licensed users of the KnowBe4 content only and may not be distributed beyond the licensed users, published anywhere that provides access beyond this group (including the Internet), or otherwise used outside of the terms of the subscription licensing agreement, including after the subscription ends. This PDF may also not be manipulated or modified. All images, text, and other assets are copyrighted by KnowBe4 and cannot be used in derivative works. Please refer to your master service agreement and/or subscription agreement for more information.

2.0 Who Must Comply With HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) applies to covered entities, business associates, and hybrid entities.

Click each tab to learn more.

Definitions

Covered Entity
Health care provider, health plan, or health care clearinghouse

Business Associate
Entity that performs functions, activities, or services on behalf of a covered entity that may involve the use or disclosure of protected health information (PHI). Example: A third-party administrator that assists a health plan with claims processing.

Hybrid Entity
Entity that performs some health care functions that a covered entity performs and also performs some non-health care functions. Example: A university that includes a medical center.

Covered Entities

Our organization is considered a covered entity: health care provider, health plan, or health care clearinghouse.

Health care providers include:

- Doctors
- Clinics
- Hospitals
- Psychologists
- Dentists
- Chiropractors
- Nursing Homes
- Pharmacies

Health plans include:

- Health insurance companies
- HMOs
- Employer-sponsored health plans
- Government programs that pay for health care, such as Medicare, Medicaid, and the military and veterans' health care programs

Health care clearinghouses process nonstandard health information they receive from another entity into a standard format. For example, a health care clearinghouse may check medical claims from a health care provider for errors.

3.0 Introduction

[NARRATOR] The Health Insurance Portability and Accountability Act (HIPAA) grants individuals a variety of rights pertaining to their protected health information (PHI). HIPAA also requires us to take action so that patients' PHI is protected and secure. We follow HIPAA regulations because they're the law but also because doing so protects our patients and customers. In this course, you'll learn how you can help us live up to our HIPAA requirements.

4.0 Part 1: Introduction – Objectives

- Recall the negative impacts for organizations and individuals when personal health information isn't protected.
- Identify items that contain protected health information (PHI).
- Recognize your responsibilities for complying with HIPAA regulations.

5.0 Real People, Real Stories

When you visit a health care professional, you trust that your information will remain private.

You expect that your medical records will be accessed only by those with a legitimate need to know, even though that information will pass through the hands of dozens of employees, from registration staff to clinical employees to third-party services.

This expectation passes to each of us as we assist our customers or patients. Whether we handle information in a doctors' office, hospital, insurance company, or other organization in the health industry, individuals are trusting us to treat their information responsibly. But sometimes carelessness or misguided intentions keep this from happening.

Click each button to learn what could happen if private health information isn't protected.

Criminal Snoop

"A co-worker told me that a celebrity is a patient at our clinic. Curiosity got the best of me, so I peeked into their records to get some more information. I got excited and spread the gossip around.

"It turns out that snooping is a criminal offense. I was fired for violating our agreement with our customer, our internal policies, and the HIPAA privacy and security rules. In addition, my workplace was fined for violating federal medical privacy laws."

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."

Email Mishap

"It was a hectic day, and we needed to send some medical billing information to a customer. In a rush, I entered the wrong email address and sent the information to an unauthorized recipient.

"Apparently the email contained identifying health information, so my simple mistake was the cause of a privacy breach and violated federal medical privacy laws."

6.0 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. We are required to protect patient privacy when collecting, using, storing, disclosing, transmitting, and disposing of PHI in verbal, written, or electronic form (including photos and videos).

PHI may be found in health care records, demographic information, payment information, insurance claims—the list is endless.

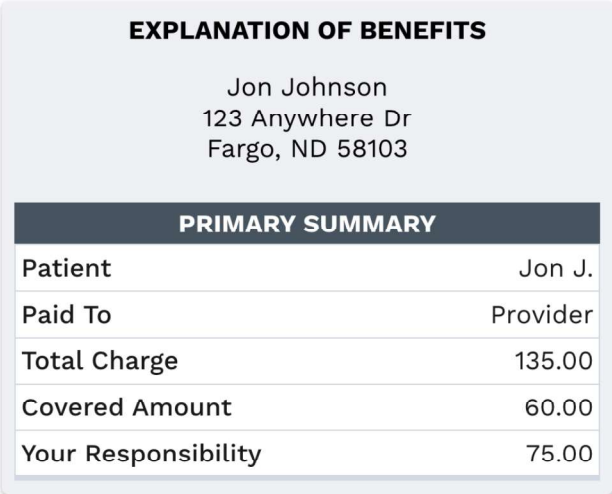
Examples

Common Examples of PHI:

- Names of individuals and relatives
- Postal addresses
- Dates
- Telephone and fax numbers
- Email 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

7.0 PHI- Question 1

Does It Contain PHI?



EXPLANATION OF BENEFITS

Jon Johnson
123 Anywhere Dr
Fargo, ND 58103

PRIMARY SUMMARY	
Patient	Jon J.
Paid To	Provider
Total Charge	135.00
Covered Amount	60.00
Your Responsibility	75.00

Does this example contain PHI?

A. Yes
B. No

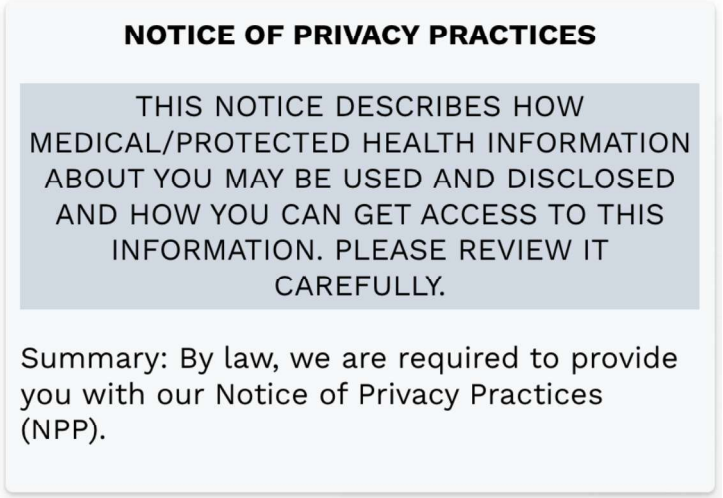
Correct Answer:

A. Yes

This example contains PHI.

8.0 PHI- Question 2

Does It Contain PHI?



NOTICE OF PRIVACY PRACTICES

THIS NOTICE DESCRIBES HOW MEDICAL/PROTECTED HEALTH INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

Summary: By law, we are required to provide you with our Notice of Privacy Practices (NPP).

Does this example contain PHI?

A. Yes
B. No

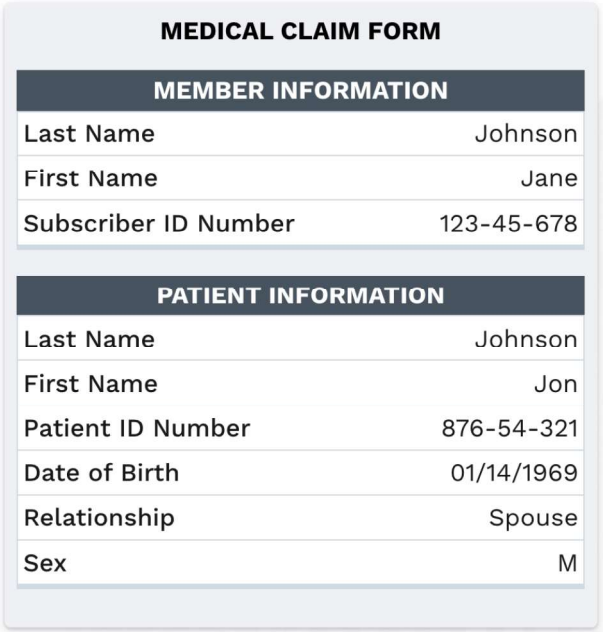
Correct Answer:

B. No

This example does not contain PHI. Note that if the Notice of Privacy Practices includes a patient's acknowledgment, it is considered PHI.

9.0 PHI- Question 3

Does It Contain PHI?



MEDICAL CLAIM FORM

MEMBER INFORMATION	
Last Name	Johnson
First Name	Jane
Subscriber ID Number	123-45-678

PATIENT INFORMATION	
Last Name	Johnson
First Name	Jon
Patient ID Number	876-54-321
Date of Birth	01/14/1969
Relationship	Spouse
Sex	M

Does this example contain PHI?

A. Yes
B. No

Correct Answer:

A. Yes

This example contains PHI.

10.0 Your Responsibilities

As a covered entity, we are committed to HIPAA compliance. We need employees in every role to support that commitment.

By providing high-quality services that safeguard PHI, you protect our reputation and help us avoid costly penalties, legal sanctions, and litigation fees for violating the law.

Click each button to learn more about your responsibilities.

Privacy

Privacy is the foundation of HIPAA. It's the underlying principle that determines how and when we can use or disclose an individual's PHI. It also grants patients the rights to keep their information confidential.

You have the responsibility to keep all PHI private; therefore, you cannot reveal that information to any other person without the patient's consent.

Security

Patients expect that their medical records and data will be kept safe and secure, regardless of how many hands touch it.

You have a responsibility to secure any confidential information related to a patient (such as names, dates, diagnoses, and medications). You are also expected to safeguard information from misuse.

Patient Rights

HIPAA gives individuals very important rights that must be respected.
These include the right to:

- Access electronic copies of their PHI.
- Amend or update their information.
- Account for all disclosures of information.
- Trust that PHI will be transmitted with the appropriate restrictions and safeguards.

11.0 Scenario 1

Apply What You've Learned

Employee: "Hmm, I wonder if I need to keep this patient's contact information secure?"

Does this employee need to protect this information?

A. Yes, this record contains PHI.
B. Yes, but only if the patient has a federally recognized insurance policy.
C. No, this information is not confidential.

Correct Answer:

A. Yes, this record contains PHI

Patient contact information, as well as medical claim forms, health care billing statements, and Explanation of Benefits forms contain PHI and need to be safeguarded.

12.0 Scenario 2

Apply What You've Learned

Employee: "Check out this patient's records! You won't believe who just got plastic surgery!"

Can this employee share this information?

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

Correct Answer:
B. No. this is PHI and it is against the law to share.

Any information pertaining to the health care of an individual is PHI and cannot be shared or accessed unless there is an authorized need to know.

13.0 Scenario 3

Apply What You've Learned

First Employee: "I'm worried about being personally liable if we are out of HIPAA compliance."
Second Employee: "Don't worry! HIPAA compliance isn't our responsibility. Our managers handle most of the compliance stuff."

Is the second employee's response accurate?

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

Correct Answer:
B. No, everyone – regardless of role – needs to know and comply with HIPAA regulations.

We are contractually and legally obligated to comply with HIPAA and our policies and procedures.

14.0 Part 1: Introduction – Summary

Complying with HIPAA isn't about checking the box—it's about taking action to protect real people.
Doing your part to keep us in compliance helps safeguard PHI and ensure our organization isn't penalized with fines.

Take a moment to review the key points covered.

- Failure to protect health information can result in fines or penalties associated with violating federal medical privacy laws, medical identity theft, and loss of customer or patient trust.
- PHI is any health-related information that can be used alone, or in combination with other information, to identify an individual.
- You are responsible for complying with HIPAA regulations by keeping all PHI private, securing any confidential information related to our patients and customers, and providing them access to their PHI.

15.0 Applying HIPAA

[NARRATOR] Compliance with HIPAA applies at every level of our organization. When each employee does their part, we can successfully limit unauthorized or inappropriate access to PHI, and limit unauthorized disclosures. No matter your role, you maintain the standing of our organization and protect the privacy of our customers each time you apply HIPAA to our business practices.

16.0 Part 2: Using and Disclosing PHI – Objectives

- Recognize that the HIPAA Privacy Rule regulates how we use PHI, share it with others, and handle requests to disclose PHI to outside entities.
- Recall the administrative requirements that we implement to ensure our compliance with the HIPAA Privacy Rule.
- Recall the permissible purposes for sharing PHI under the HIPAA Privacy Rule.
- Determine when it is permissible to disclose PHI and when it is not.

17.0 HIPAA Privacy Rule

The HIPAA Privacy Rule defines the permitted uses and disclosures of PHI. At its most fundamental level, the rule states that we must use only the minimum necessary PHI for treatment, payment, and health care operations.

No matter how our organization uses PHI, the first step to help us stay in compliance is to be aware of when HIPAA applies.

Click each button to learn about situations where HIPAA applies.

Treatment

Treatment Activities Include:

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

Exception: Psychotherapy notes are subject to restrictions.

Payment

Payment Activities Include:

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

Operations

Health Care 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.

18.0 Administrative Requirements

Your daily interactions with PHI are the most important way that we maintain HIPAA compliance. However, we also implement a variety of administrative policies and procedures at all levels of our organization to ensure that we live up to our obligations.

Click each tab to learn about the administrative requirements we follow to comply with the HIPAA Privacy Rule.

Tab 1

Privacy Officer
We designate a privacy officer to implement the Privacy Rule and to be the primary point of contact for all privacy-related concerns.

Employee Training
We train as applicable team members on the importance of complying with HIPAA.

Tab 2

Safeguards
We place appropriate administrative, technical, and physical safeguards to protect PHI in all its forms.

Complaints
We give individuals a clear process for making complaints, and we document and investigate each complaint we receive.

Tab 3

Sanctions
We are required to take actions against team members that do not comply with HIPAA regulations or with our policies and procedures.

Mitigation
We take practical steps to mitigate the harmful effects caused by impermissible disclosure of PHI.

Tab 4

Refrain From Intimidation or Retaliation
We never punish individuals for exercising the rights granted to them by HIPAA.

No Waiver of Rights
We don't require that individuals waive their HIPAA rights as a provision of treatment, payment, plan enrollment, or eligibility of benefits.

Tab 5

Documentation
We maintain written documentation of all HIPAA-related policies, procedures, communications, and any other action, activity, or designation.

Document Storage and Disposal
PHI and other HIPAA-related documents must be kept out of public view and stored in secure areas. HIPAA-related documents, such as notices of privacy practices, disclosure authorizations, or risk assessments, must be retained for a period of 6 years from the date of creation (or the date when last in effect). Once that period is met, HIPAA-related documents must be disposed of in a secure shredder or electronically deleted.

19.0 Use and Disclosure

The HIPAA Privacy Rule also regulates the use, disclosure, and handling of requests for PHI. Click each button to learn how these terms apply to your job functions.

Use

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

Disclosure

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

Request

Refers to any situation where we—or an individual within our workplace—request and/or are requested to disclose PHI to an outside entity. Requests for PHI may be necessary for operational purposes, but they are subject to certain limitations.

20.0 Types of Disclosures

It is critical to understand the limitations around disclosing PHI. Most disclosures fall into one of the following four categories.

Click each button to learn more.

Permitted Disclosures

"I need to share a patient's PHI with her insurance company for billing purposes. Is it okay to disclose this information?"

Yes. PHI can be disclosed in this circumstance.

In order to obtain payment, you can share information with other providers, pharmacies, labs, or other entities involved in the patient's care or with the patient's health plan. Other permitted disclosures include the following circumstances or purposes:

- To the individual to whom the PHI relates
- To a business associate under a valid Business Associate Agreement
- Cases involving victims of abuse, neglect, or domestic violence
- The operation of coroners, medical examiners, and funeral directors
- Public health activities
- Health oversight activities
- Law enforcement purposes
- Organ donation purposes

- Research (under certain conditions)

Disclosures Required by Law

"I received a subpoena for PHI provided by our customer, so I can disclose this information ... right?"

Yes. PHI can be disclosed in this circumstance.

We are legally required to disclose information in certain situations; receiving a subpoena, which is a court order, is one of them. Always follow our policies for handling this type of disclosure.

Disclosures Following an Opportunity To Object

"A patient's family member is requesting information; however, the patient has not consented to the disclosure. Can I release this information?"

It depends on the patient's status.

Patients available and capable of making decisions must be given the opportunity to consent or object to disclosures. Use your professional judgment if the patient is unavailable or incapable of providing consent themselves. Before sharing, verify the identity of the person requesting the information and the authority of that person to receive the information. Only share relevant details, and only share when it's in the best interests of the patient. You can refer to our policies and procedures for more information related to this type of disclosure.

Disclosures Requiring Authorization

"An employer called and requested the status of an employee who was admitted to our facility this morning. Is it okay to disclose this patient’s information?"

No. PHI cannot be disclosed in this circumstance.

Disclosing PHI to a patient's employer without proper authorization is illegal. Disclosures must be related to the patient's treatment, payment for the treatment, and/or health care operations, and provided to only those with an administrative need to know.

21.0 Scenario 4

Apply What You’ve Learned

Patient: "Do I need to call the insurance company to provide my information so they will pay for the treatment? It would be great if you would call them for me."

Nurse: "No, our staff will take care of that for you."

Does providing medical information about this patient to an insurance company violate HIPAA regulations?

A. Yes, the patient must contact the insurance company directly or authorize the nurse to do so.
B. No, covered entities can share information with other parties involved in order to obtain payment for treatment.

Correct Answer:

B. No, covered entities can share information with other parties involved in order to obtain payment for treatment.

A covered entity can share information with other providers, pharmacies, labs, or other entities involved in the patient's care or with the patient's health plan to obtain payment.

22.0 Scenario 5

Apply What You've Learned

Receptionist (looking at X-ray): "Gross! What a gnarly fracture!"

Is this receptionist violating HIPAA law by viewing this X-ray?

A. Yes, as a receptionist they don't have a business need to view a patient's X-ray.
B. No, viewing an X-ray alone does not violate privacy regulations.

Correct Answer:

A. Yes, as a receptionist they don't have a business need to view a patient's X-ray.

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.

23.0 Scenario 6

Apply What You've Learned

Employee: "I have a patient on the phone making a complaint about the disclosure of their health care information. Rather than raise a fuss, I gave them a 15% refund on their last treatment."

Did this employee handle the complaint in a way consistent with HIPAA requirements?

A. Yes, the most important thing is that the patient walks away happy and drops the complaint.
B. No, any complaints should be escalated to the Privacy Officer.

Correct Answer:

B. No, any complaints should be escalated to the Privacy Officer.

The HIPAA Privacy Rule requires that all privacy-related concerns be handled by a single point of contact: our Privacy Officer.

24.0 Part 2: Using and Disclosing PHI – Summary

Keep the HIPAA Privacy Rule in mind when performing your duties, and remember the most common disclosures, including permitted disclosures for treatment, payment, and health care operations.

Take a moment to review the key points covered.

- The HIPAA Privacy Rule states that only the minimum amount of PHI necessary can be used and disclosed for treatment, payment, and health care operations purposes.
- We employ a variety of administrative policies and procedures that help ensure our compliance with the HIPAA Privacy Rule.
- We must only use, disclose, or request PHI when doing so for the purposes of treatment, payment, or other health care operations.
- We must only disclose PHI when the disclosure is permitted under HIPAA, authorized by the patient, or required by law.

25.0 Our Principles

NARRATOR] We comply with HIPAA not simply to adhere to legal requirements but because we care about the individuals whose PHI we handle each day. They trust us with this information because we treat their PHI with the same care we'd expect for our own. It's this principle that guides how we respect the rights of individuals granted by HIPAA.

26.0 Part 3: Rights of Individuals – Objectives

- Identify the rights that HIPAA grants to individuals in regard to their PHI.
- Identify the information that HIPAA requires us to include in our Notice of Privacy Practices.
- Identify how you should handle requests for PHI.

27.0 Rights of Individuals

HIPAA isn't just about protecting information; it also gives individuals a variety of rights that must be upheld.

It's your duty to ensure that these rights are respected.

Individuals have a right to:

1. Inspect and request a copy of their medical record.
2. Amend their PHI.
3. Request an accounting of all PHI disclosures. Note that some exceptions apply, such as for routine disclosures, disclosures to the individual, authorized disclosures, and disclosures related to permitted uses.
4. Request confidential communications of their PHI by alternative means.
5. Obtain a paper copy of the Notice of Privacy Practices.
6. File a complaint regarding the privacy or security of their PHI.
7. Request restrictions on uses and disclosures of their PHI—including restricting disclosures to a health plan if the individual pays for a service or item in full themselves.

28.0 Notice of Privacy Practices

Click each tab to learn about our responsibility to provide Notice of Privacy Practices.

Providing Notice

To ensure that individuals are well informed of their rights—and our responsibilities—HIPAA regulations require that we develop and issue a Notice of Privacy Practices.

We must provide individuals our Notice of Privacy Practices as soon as it is reasonable to do so. It must also be available upon request.

Notification Requirements

1. A description of how we may and may not use and disclose PHI.
2. A description of our legal duties and responsibilities to maintain the privacy of PHI.
3. A description of individuals' rights concerning their PHI and how to exercise those rights.
4. An explanation of how individuals can file a complaint with us and/or the federal government.
5. The name of a person or office that individuals may contact for further information.
6. A statement regarding our responsibility to notify individuals in the case of a breach of unsecured PHI.

29.0 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.

Click each button to learn how to handle different requests.

Right To File a Complaint

Request:
"I just lost a job prospect because the manager felt that my medical history would be a liability. Can you explain to me how they found out about this?"

Response:

- Inform the individual of their right to file a complaint if they suspect their privacy rights have been violated.
- Refer the complaint to the employee designated to handle complaints, typically the Privacy Officer.

Right To Limit Access

Request:
"My daughter is feeling better, but I worry that this procedure may affect her chances of getting a student loan or inclusion in some activities. Can I limit who has access to her medical information?"

Response:

- Inform the individual that they have a right to request a restriction or limitation on the PHI we use or disclose for certain specified reasons.
- Refer the request to the employee designated to handle these requests, typically the Privacy Officer. Note that we are not required to agree to the restriction request.

Request To Amend Record

Request:
"I've been seeing a variety of specialists lately, and they all seem to be looking at the same record—which is inaccurate. How can I fix the problem?"

Response:

- Explain that the patient has a right to request an amendment, and it's the provider's decision whether or not to accommodate the request.
- Refer the request to the employee designated to handle these requests, typically the Privacy Officer.

Written Authorization

Request:
"Hey buddy, I need a spreadsheet of our patients' contact information for marketing purposes."

Response:

- Explain that using or disclosing PHI for marketing purposes is against our policy and not allowed under HIPAA.
- Explain that we need to obtain written authorization from all patients to use or disclose their information before fulfilling this request.

30.0 Scenario 7

Apply What You've Learned

First Employee: "Okay, let's get this Privacy Notice up on our website."

Second Employee: "Wait a minute! We forgot to detail our process for how employees can make formal complaints about the use or disclosure of their PHI."

Is the second employee correct about the need to include this information in our Privacy Notice?

A. Yes, information about how to file complaints, as well as the contact information of our Privacy Officer, should be included.
B. No, all customer service and billing staff are trained to handle complaints, so this information does not need to be included.

Correct Answer:

A. Yes, information about how to file complaints, as well as the contact information of our Privacy Officer, should be included.

A Privacy Notice must include an explanation of how individuals can file a complaint with us and/or the federal government, in addition to the name of a person or office that individuals may contact for further information.

31.0 Scenario 8

Apply What You've Learned
Employee: "I need medical information on the following patients in order to process insurance claims."

Does this request for information comply with HIPAA regulations?

A. Yes, requesting information associated with the payment for health care is allowed.
B. No, only medical and legal requests for PHI are complaint with HIPAA regulations.

Correct Answer:

A. Yes, requesting information associated with the payment for health care is allowed.

Requests made for PHI that deal with health care treatment, payment, or operations comply with HIPAA regulations.

32.0 Scenario 9

Apply What You've Learned
Patient: "I know that I did not authorize you to share my information!"

How should an employee process this patient complaint?

A. Do their best to explain the situation and make amends.
B. Refer the person to the employee designated to handle complaints.

Correct Answer:

B. Refer the person to the employee designated to handle complaints.

All complaints of this nature should be referred to the employee designated to handle complaints. In most situations, this will be our Privacy Officer.

33.0 Part 3: Rights of Individuals – Summary

Each day you might take actions that affect the rights granted to individuals under HIPAA regulations. Remember to be open about how we honor these rights in our Notice of Privacy Practices, and think about how you can help patients exercise them when handling requests.

Take a moment to review the key points covered.

- We respect the rights that HIPAA grants to individuals in regard to their PHI.
- HIPAA regulations require that we develop and issue a Notice of Privacy Practices that includes specific information.
- You play an important role in protecting individuals' rights by handling requests appropriately.

34.0 Securing PHI

[NARRATOR] We're surrounded by PHI every day, so much so that it's easy to forget just how important it is to keep it safe from unauthorized disclosure. It's important to remember that all PHI must be kept secure, whether it's printed on paper, stored in an electronic directory, or simply spoken over the phone or to a co-worker.

35.0 Part 4: Securing PHI – Objectives

- Recognize that the HIPAA Security Rule defines the standards required for securing electronic PHI (e-PHI).
- Recall the administrative requirements that we implement to ensure our compliance with the HIPAA Security Rule.
- Identify the physical security practices you should follow to minimize the risk of unauthorized access to PHI.
- Identify the technical safeguards you should follow to help protect PHI.

36.0 HIPAA Security Rule

The HIPAA Security Rule defines the standards required for securing electronic PHI (e-PHI).

Anyone who comes into contact with e-PHI must follow our administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of health care information.

In general, these safeguards accomplish four requirements.

Click each card to learn about the requirements.

1. Ensure the confidentiality, integrity, and availability of all e-PHI in our care.
2. Protect against reasonably anticipated threats or hazards to e-PHI in our care.
3. Protect against reasonably anticipated uses or disclosures of e-PHI not permitted or required under the HIPAA Privacy Rule.
4. Ensure our workforce complies with the HIPAA Security Rule.

37.0 Administrative Safeguards

Implementing the Security Rule requires a variety of important administrative safeguards. These safeguards detail the reasonable policies and procedures we use to limit access to and protect e-PHI.

Click each button to learn about the administrative techniques we use to comply with the HIPAA Security Rule.

Security Management Process

We implement policies and procedures to prevent, detect, contain, and correct security violations. These address the topics of Risk analysis, Risk management, Sanction policy, and Information System activity review. These processes must also monitor log-in occurrences and track suspicious activity.

Security Officer

We designate a Security Officer who develops and implements our required policies and procedures.

Awareness and Training

We train all team members on the importance that security plays in helping us remain HIPAA compliant, document training completion, and implement ongoing reminders to ensure security stays on the forefront of day-to-day operations.

Incident Procedures

We report suspected security incidents without delay.

Contingency Plan
We take precautions to back up PHI in our care, so that we can respond to an emergency or other occurrence (e.g., fire, vandalism, system failure, natural disaster) that damages systems that contain e-PHI.

Mitigation
We take practical steps to mitigate the harmful effects caused by inappropriate disclosure of PHI.

38.0 Physical Safeguards

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

Click each button to review some of our organization's policies for physical security.

Access
- Always keep office doors and cabinets locked.
- Do not allow anyone to follow you into a secure location.
- Report suspicious tampering with equipment or the presence of unauthorized individuals to security.

Around the Office
- Keep PHI out of clear view of the public (e.g., desks, whiteboards, or copiers/fax machines).
- Do not discuss PHI when it might be overheard by others who do not have a legitimate business need to know.
- Dispose of documents and electronic media containing PHI in secured containers or by shredding.

Workstations
- Always follow our policies for accessing e-PHI.
- Do not use your computer for activities unrelated to your job duties.
- Do not alter or modify physical components of your workstation.
- Physically secure your laptop and other mobile equipment with security cables or in locked drawers.
- Report suspicious use of your computer or unauthorized access of sensitive information to security.

Devices and Media
- Never leave your laptop or smartphone unattended in the office, in your car, or when traveling.
- Follow our approved processes for disposal of digital media that has accessed e-PHI, such as CD-ROMs or USB drives.

- Contact IT for assistance in backing up data before moving any equipment that accesses e-PHI; ensure that movement is documented.
- Do not transmit or make copies of PHI using your personal devices (such as taking pictures of information using your smartphone).
- Appropriately store and dispose of any recordings, such as security camera footage or voice calls taped for quality purposes.

39.0 Technical Safeguards

We require a variety of technical safeguards when it comes to accessing, storing, or transmitting PHI on computers, smartphones, and other electronic devices.

Click each item to learn the dos and don'ts for safeguarding PHI.

Do

- Create strong passwords for work accounts.
- Lock your laptop or mobile device with a screensaver that requires a password or other security feature.
- Encrypt files containing PHI whenever they are stored or transmitted.
- Be on the lookout for suspicious links in emails or websites, which could be used to install malware.
- Report suspicious computer behavior or the presence of malware to IT.

Don't

- Share your password with anyone, including co-workers, family, and managers.
- Install third-party software on your device or mobile phone.
- Transmit PHI when connected to public Wi-Fi networks.

40.0 Scenario 10

Apply What You've Learned
Employee: "Hold the door! I forgot my badge."

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

A. Yes, if the person is in the building, they must be a valid employee.
B. Yes, but only if the employee has valid ID.
C. No, all employees need to scan their badges to enter secure areas.

Correct Answer:

C. No, all employees need to scan their badges to enter secure areas.

It is a security violation to allow anyone to follow you into a secure location. Ensure that everyone who enters a secure area scans their badge.

41.0 Scenario 11

Apply What You've Learned
First Employee: "I can't access this system with my password. I was just in the system yesterday!"

Second Employee: "They must be in the middle of a system update. Here, go ahead and use my password."

Does sharing your password violate our security policy?

A. Yes, you should never share your password with anyone.
B. No, as long as you change your password immediately afterwards.

Correct Answer:
A. Yes, you should never share your password with anyone.

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

42.0 Part 4: Securing PHI – Summary

The HIPAA Security Rule details how we can build the administrative, technical, and physical safeguards to secure e-PHI. By following these guidelines and our policies, you help maintain the trust of our patients and customers and reduce the risk of privacy incidents.

Take a moment to review the key points covered.

- HIPAA regulations require that we maintain reasonable administrative, technical, and physical safeguards to protect electronic PHI.
- We employ a variety of administrative policies and practices that help ensure our compliance with the HIPAA Security Rule.
- You can minimize the risk of unauthorized access to PHI by following physical security practices in your workplace.
- When accessing, storing, and/or transmitting PHI, you are required to follow our technical safeguards related to our networks, encryption, passwords, and software.

43.0 Consequences for Noncompliance

[NARRATOR] Unfortunately, balancing the day-to-day realities of business with our HIPAA obligations can be challenging. Whether through ignorance or negligence, there are significant consequences for falling out of compliance with HIPAA regulations. These can have serious ramifications for our organization and employees.

44.0 Part 5: Enforcement and Breach Notification – Objectives

- Recognize the penalties associated with violating HIPAA regulations.
- Identify the most common HIPAA privacy and security violations.
- Recall the factors considered during a Breach Risk Assessment for the purpose of determining the probability of information compromise.
- Recognize the importance of enforcing HIPAA and properly reporting breaches.

45.0 HIPAA Enforcement and Penalties

Click each tab to learn how HIPAA is enforced.

Enforcement

Any impermissible release, acquisition, use, or disclosure of PHI can bring significant risks to our organization, ranging from fines to criminal penalties. These monetary penalties and legal sanctions exist to discourage incidents from occurring and provide consequences for those who violate HIPAA rules and regulations.

We're legally accountable to comply with HIPAA regulations, but we also follow privacy and security best practices to protect customers and patients. It's the right thing to do.

Violation Penalties

- The Office for Civil Rights, the government agency charged with enforcing the privacy and security regulations, is very active in investigating complaints and reported breaches. The largest fine related to an Office for Civil Rights settlement was $16 million.
- To remain HIPAA compliant, our organization must apply appropriate sanctions against employees who fail to comply with security policies and procedures.
- This means the organization can discipline you, up to and including terminating your employment, for failing to follow HIPAA policies and procedures. Additionally, you could be individually fined and face criminal charges for violating HIPAA regulations.

46.0 Types of Violations

The biggest risks to maintaining the privacy and security of PHI usually occur from within our workplace.
We must protect against violations, whether caused by someone failing to follow the appropriate privacy and security procedures, or by a malicious attempt to steal information. HIPAA legislation increases the penalty amounts based on the level and intent of a breach of privacy. All breaches are classified and penalized according to their type, but some are more common than others.

Click each type of violation for examples.

Lacking Administrative Safeguards for e-PHI

- Using e-PHI without the proper security controls.
- Sending e-PHI to technology vendors that are not business associates.
- Failing to document actions taken to address complaints or incidents.

Using or Disclosing More Information Than Necessary

- Leaving a phone message for a patient with a family member that details a medical condition.
- Placing informal medical alerts on the exterior of patient files which can be seen by those without the need to know.

Denying Patients Access to Their PHI

- Refusing a parent a copy of their child's medical record.
- Refusing to provide an individual a copy of their pharmacy prescription records.
- Providing access to mental health records but not copies.

Failing To Protect PHI

- Leaving passwords in plain view of others.
- Giving discharge instructions to the wrong patient.
- Sending lab results to the wrong patient.

Impermissible Use or Willful Neglect

- Providing PHI to a research entity without the patient's authorization.
- Disclosing PHI without following verification procedures.
- Examining an individual's PHI without the need to know.

47.0 Identifying a Breach

We 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 impermissible types of access and disclosures—inside and outside of our workplace. However, separating an actual breach from a suspected one can be tricky.

Breach Risk Assessments are performed by the Security Officer and others trained specifically for that purpose. But you may be required to help gather information that will allow the Security Officer and their team to determine the nature, extent, and circumstances of a suspected incident.

Click each card to learn about the factors considered during a Breach Risk Assessment.

1. What is the nature and extent of the PHI involved?
2. Who was the unauthorized person who used the PHI or to whom the disclosure was made?
3. Was the PHI actually acquired or viewed?
4. To what extent has the risk to PHI been mitigated?

48.0 Enforcement and Breach Notification

When you suspect a breach—no matter how minor it may appear—it must be reported immediately through our incident reporting process.

Reporting incidents immediately can help prevent simple mistakes from turning into catastrophic breaches.

If the incident is determined to be a breach, we must make certain notifications.

Click each button to learn about required notifications.

Individuals

Affected individuals must be alerted by first-class mail, or by email if they have agreed to electronic notices, within 60 days of discovery. Notification should include:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach.
- A brief description that includes what information was involved.
- Steps the individual can take to protect themselves.
- What our organization is doing to manage the incident.
- Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an email address, a website, or a postal address.

Media

- Prominent media outlets must be notified of breaches affecting more than 500 individuals.
- This notification may be in the form of a press release that includes the same information sent to individuals.
- Notice must be given without unreasonable delay and in no case later than 60 days after discovery.

Health and Human Services Secretary

- An electronically submitted breach report must be sent to the Health and Human Services Secretary.
- If the breach affects 500 or more individuals, this form must be sent within 60 days.
- Incidents that affect fewer than 500 individuals may be reported annually (but no later than 60 days after the end of the calendar year).

49.0 Scenario 12

Apply What You've Learned
Employee: "Who threw away this patient's contact information? I wonder who saw this."

What should this employee do?

A. Take no action. No one outside of our organization will see the information.
B. Remove the record from the trash and report the incident.
C. Notify the patient.

Correct Answer:

A. Remove the record from the trash and report the incident.

Unsecured PHI is a violation. The PHI needs to be secured, and the incident needs to be reported immediately.

50.0 Scenario 13

Apply What You've Learned
Employee: "Uh-oh. I just emailed a patient's contact information to the wrong address!"

What should this employee do?

A. Wait to see if the email bounces back before doing anything.
B. Take no action. Small mistakes like this do not qualify as a violation.
C. Consider this mistake an incident and report it.

Correct Answer:

C. Consider this mistake an incident and report it.

Although mistakes do happen, sending PHI to an unauthorized party is an incident and, by law, must be reported.

51.0 Part 5: Enforcement and Breach Notification – Summary

You now understand the importance of protecting PHI to prevent serious impacts on both our organization and our patients. To comply with HIPAA, we must investigate all privacy and security incidents in which PHI has been improperly accessed, acquired, used, or disclosed. Therefore, we rely on you to report suspicious actions immediately in an effort to prevent them from turning into catastrophic breaches.

Take a moment to review the key points covered.

- Improperly releasing, acquiring, using, or disclosing PHI is a violation of HIPAA regulations and subject to penalties.
- The biggest risks to maintaining the privacy and security of PHI usually occur from within our workplace.
- HIPAA requires that we investigate all privacy and security incidents in which PHI is suspected to have been improperly accessed, acquired, used, or disclosed.
- We must adhere to HIPAA requirements for notification in the event of a breach of PHI.