

20

HIPAA



TEACHING PLAN

To use this lesson for self-study, the learner should read the material, do the activity, and take the test. For group study, the leader may give each learner a copy of the learning guide and follow this teaching plan to conduct the lesson.



LEARNING OBJECTIVES

Participants will be able to:

- Uphold the privacy, confidentiality, and security of patients' protected information
- Summarize the critical components of the Health Insurance Portability and Accountability Act (HIPAA)
- Define consent and authorization



ACTIVITY

Do this activity first to get participants thinking about issues of privacy and confidentiality.

Use the situations on the activity page of this packet titled "What Should You Do If...." Cut each situation out, fold it, and put it in a container (without the answers). Ask each participant to draw one of the situations, read it to the group, and explain the best thing to do in that situation. If the participant does not know what to do, he or she can ask others for opinions. You may give the correct answer at this time or tell the participant to keep the situation and try to find the correct answers as the lesson proceeds. The answers are provided to assist you in guiding the discussion.



THE LESSON

Bring copies of your organization's privacy and confidentiality policies and procedures to the training session for the employees to keep and review. Discuss the information in the learning guide and in your policies and procedures with the participants. Be prepared to answer specific questions about your policies.

For more information about HIPAA, go to www.hhs.gov/ocr/hipaa.



CONCLUSION

Have participants take the test. Review the answers together. Award certificates to those who answer at least seven (70%) of the test questions correctly.



TEST ANSWERS

1. d
2. b
3. c
4. c
5. c
6. b
7. b
8. True
9. b
10. a

HIPAA

Activity: What Should You Do If . . .

Directions: Discuss each scenario. Answers follow on the next page.

1. A patient asks to see or copy his patient record.
2. A doctor's office asks you to fax them something from a patient's record.
3. A patient or a friend of a patient asks you about another patient's condition.
4. A patient's family member asks to see the patient's record.
5. A coworker wants to talk to you about a patient.
6. A coworker wants to talk to you about a patient while you are at a restaurant.
7. You notice a patient's record sitting open and out where others can see it.
8. A computer screen that can be seen by others is on, displaying patient information.
9. You answer the phone and someone asks for information about a patient.

Activity Answer Guide

1. Refer the patient to your supervisor. Your organization must allow the person to view and photocopy his record if requested, except in certain special circumstances.
2. If the patient has signed a consent form releasing the information, you may fax the information, using a cover sheet marked "Confidential."
3. Politely explain that you cannot discuss a patient's health condition with others.
4. Patients must sign a special authorization for anyone to see their records other than for purposes of providing healthcare (for which they must sign a consent form).
5. Go to a private area where you cannot be overheard by others.
6. Remind your coworker that you should not discuss patients where others can hear you, and you should discuss patients only when it is important for providing care.

HIPAA

7. Put the record away immediately, out of sight of unauthorized persons.
8. Turn the computer screen so unauthorized persons cannot see it and/or clear the information from the screen if you are able to do so safely.
9. If the individual on the phone is authorized to access the patient's information, you may give the information as long as no one else can overhear you. If the patient has not signed a consent form or a specific authorization, you may not give the information.

HIPAA History and Overview

Congress passed HIPAA to require the security, confidentiality, and privacy of every person's health information.

Privacy is about who should and should not have access to health information. Patients have the right to privacy, meaning that information about them should be available only to people who need it to provide care.

Confidentiality is about preventing someone from hearing or seeing a person's private health records and information unless they have the proper authorization. All health information is confidential. Anyone who possesses personal health information (PHI) is responsible for protecting it.

Security is the means used to provide privacy and confidentiality. The purpose of security is to ensure that only those persons having authorization may access PHI.

Frontline staff should remember the general HIPAA rule of thumb: the right information, to the right person, for the right reasons.

The American Recovery and Reinvestment Act of 2009 and HITECH

On February 17, 2009, the American Recovery and Reinvestment Act of 2009 became a federal law. A subset of that law, called the HITECH Act, enhances and expands the HIPAA Privacy and Security Rules and adds requirements for breach notification. The HITECH Act not only makes privacy regulations more strict, but it gives more power to federal and state authorities to enforce privacy and security protections for patient data, and it raises the fines for noncompliance.

The 2013 Omnibus Privacy, Security, Enforcement, and Breach Notification Rule (Omnibus Rule) implements many of the HITECH Act provisions for PHI protection.

Why Do We Need HIPAA?

More and more health information is in the form of electronic data, either instead of or in addition to paper files. We must protect data in any form. Federal laws make sure every state and every provider follow the same rules for privacy, confidentiality, and security.

Who Has to Follow the HIPAA Rules?

The following public and private organizations must follow the HIPAA rules:

- Health plans and health insurance companies, such as health maintenance organizations (HMO) and preferred provider organizations (PPO)
- A healthcare clearinghouse, such as a billing service
- Healthcare providers, such as doctors, dentists, chiropractors, therapists, hospitals, nursing facilities, clinics, pharmacies, home health agencies, hospices, and long-term care or personal care facilities of any type or size

The HIPAA rules call these organizations covered entities.

What Else Are Covered Entities Required to Do?

Covered entities are required to communicate how HIPAA is implemented to both patients and frontline staff. They must:

- Notify patients about their privacy rights and give clear, written explanation of how the provider may use and disclose the patient's health information. This notifies patients of their right to view their own records, obtain copies, have copies sent to another person or organization, request restrictions on how their PHI is used and disclosed, receive confidential communications, receive a report of certain disclosures of their PHI, and request amendments to their information. The privacy notice must also let patients know how to file a complaint with the entity or with the OCR.
- Adopt written privacy procedures that define who has access to protected information, how the entity will use the information, and when the entity might disclose the information to others.
- Train employees in the privacy procedures.
- Implement safeguards to prevent intentional or accidental misuse of PHI.
- Appoint an individual to make sure that employees follow the privacy procedures.
- Give an accounting of instances where the entity has disclosed PHI for purposes other than treatment, payment, or healthcare operations.

Information Protected Under HIPAA

The privacy protections of HIPAA apply to PHI. PHI is information:

- Created or received by a covered entity or an employer that relates to a person's past, present, or future health condition, health treatment, or payment for healthcare services
- That could identify an individual, such as name, address, telephone number, date of birth, diagnosis, medical record number, Social Security number, employer, position, or other identifying data

PHI can be in any format: paper, electronic, or oral. The most common example of PHI is the patient record.

Protecting Patient Records

If a provider wants to disclose a person's PHI for purposes of providing care, the provider needs that person's consent. These purposes include routine healthcare-related uses of the information, such as when a doctor consults with another doctor in order to provide better care for an individual.

If a covered entity wants to disclose a person's PHI for purposes other than providing care, the covered entity needs that person's specific authorization.

Only authorized personnel should enter confidential medical information into a computer-based patient record. Computer systems should be password protected to help guard against unauthorized access and use.

What is the difference between consent and authorization?

To give consent, a patient must sign a consent form. The patient needs to sign the consent only one time for each provider. The consent will apply whenever that provider discloses the person's PHI for purposes of providing healthcare.

Specific authorization is required when a covered entity wants to use or disclose a person's PHI for purposes not related to providing healthcare. The person must sign an authorization form for each specific instance.

May a person see his or her personal PHI and make changes?

A covered entity must allow a person to view and photocopy his or her PHI if the person submits a request. The organization may charge for copies of these records.

In a few special circumstances, such as when a covered entity has compiled information for use in a civil, criminal, or administrative proceeding, that entity does not have to give a person access to his or her PHI.

HIPAA

A covered entity may deny a person access to his or her PHI if they have reason to believe that access would create a risk of danger to that person's health.

If a person believes that his or her PHI contains information that is incorrect, the person may ask the covered entity to make changes. The covered entity may deny the request if they believe the current information is accurate and complete, or if the entity did not create the information.

Exceptions to the HIPAA Privacy Rule

The HIPAA Privacy Rule permits covered entities to disclose healthcare information without a person's specific authorization in certain situations, depending upon state or local law, such as:

- Emergencies
- Public health needs (such as infectious disease registries)
- Mandatory reporting of child or elder abuse and neglect
- Judicial and administrative proceedings
- When there are substantial communication barriers

If there is no state or local law specifically requiring disclosure of information in the instances listed above, covered entities are required to use "professional judgment" in deciding whether to disclose information and how much to disclose.

Protection of Patient Privacy and Confidentiality

Quality patient care requires communication between care workers. Computers, the internet, emails, and faxes make it easier to share patient records. However, this information is often readily available to anyone who walks by a fax machine or logs on to a computer. Some people fear that the exposure of their PHI could result in job discrimination, personal embarrassment, or the loss or denial of health insurance.

IMPORTANT HIPAA CONSIDERATIONS

- Confidentiality of information, whether in written, electronic, or verbal form, is a priority.
- Confidentiality should extend to all health information.
- Handle all patient records as confidential at all times. Do not leave them open where unauthorized persons can see them.
- Learn the safeguards your organization requires for the use, disclosure, and storage of PHI. Know your organization's privacy policies and procedures.
- Individuals have the right to decide and to know who may have access to their health information and under what circumstances they may have it.
- Discuss patient information in a private place so others cannot overhear the conversation.
- A cover sheet marked "Confidential" should accompany all faxed information.
- When emailing information about a patient, remove any detailed identifying information. For example, refer to the patient by initials or by the internal patient number, instead of by the patient's full name.
- Only authorized personnel should enter confidential medical information into a computer-based patient record. Computer systems should be password protected to help guard against unauthorized access and use.
- Use only objective, precise language when documenting in the patient record. Avoid casual remarks and abbreviations that might be misunderstood.
- Always take the utmost care to protect the privacy and confidentiality of all health information. Be aware of who is around you while you are working and do not allow unauthorized people to hear or see PHI.
- Think about how you would want your PHI treated, and give your patients that much protection and more.
- Always obtain permission from patients before sharing PHI with their family or friends.
- Do not share information you learned while performing your job with patient's family or friends.

Mobile and Online Considerations

Properly managing your electronic passwords, preventing the spread of viruses, logging off your computer, protecting your tablet and smartphone (if used for care), and being aware of and responsible for any patient information taken or accessed off-site are important ways you can contribute to information security.

You should know and understand your agency's policy on which devices can be used for work and in what manner.

Remember that HIPAA applies to all communication. This includes any and all types of social media: Facebook, Twitter, LinkedIn, Instagram, etc., are no places to share any kind of patient information. This includes text and pictures.

Before quickly sharing information you might think is innocent on your smartphone at lunch, realize that if you are in any way identifying a patient's health information, you could find yourself in serious trouble.

Consequences

Covered entities are required to have a sanctions policy covering employees and other workforce members who violate HIPAA privacy and security regulations. Violating HIPAA's Privacy, Security, or Breach Notification Rules can result in civil or criminal penalties for an individual or group of individuals, and your agency will also encounter severe consequences.