The Health Insurance Portability and Accountability Act

Lesson 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 participant a copy of the Learner's Guide and follow this plan to conduct the lesson. Copy certificates for everyone who completes the lesson and passes the test. ***Approximate time: One hour.***

Objectives

At the conclusion of this lesson, participants will be able to:

1. Explain the purpose of the Health Insurance Portability and Accountability Act (HIPAA).
2. Describe the privacy and confidentiality policies and procedures required by law.
3. Implement procedures to protect client information.

Preparation

Obtain copies of your organization's privacy and confidentiality policies and procedures. Make enough copies for everyone and bring them to the training session for the employees to keep and review.

Activity

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 out 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, ask others for opinions. You may give the correct answers at this time or tell the participants to keep the situations and see if they can find the correct answers as the lesson proceeds. The answers are provided to assist you in guiding the discussion.

Lesson

1. Do the activity first to get participants thinking about issues of privacy and confidentiality.
2. Hand out the Learner's Guide and the copies of your organization's policies and procedures regarding privacy and confidentiality.
3. Discuss the information in the Learner's Guide and in your policies and procedures with the participants.
4. Be prepared to answer specific questions about your policies.
5. For more information about HIPAA, go to www.hhs.gov/ocr/hipaa

Evaluation

Ask participants to complete the test and grade their work. Distribute certificates to those who complete the test with at least nine correct answers.

Answers: 1. confidential; 2. protected; 3. health; 4. False; 5. client record; 6. True; 7. True; 8. True; 9. authorization; 10. information, person, reasons; 11. yes.

Activity: What Should You Do If?

1. A client asks to see or copy his client record.

   Answer: Refer the client to your supervisor. Your organization must allow a person to view and photocopy his record if requested, except in certain special circumstances.

2. A doctor's office asks you to fax them something from a client's record.

   Answer: If the client has signed a consent form releasing the information, you may fax the information, using a cover sheet marked "Confidential."

3. A client or a friend of a client asks you about another client's health condition.

   Answer: Politely explain that you cannot discuss a client's health condition with others.

4. A client's family member asks to see the client's record.

   Answer: The client must sign a special authorization for anyone to see his record other than for purposes of providing health care (for which he must sign a consent).

5. A coworker wants to talk to you about a client while you are at work.

   Answer: Go to a private area where you cannot be overheard by others.

6. A coworker wants to talk to you about a client while you are at a restaurant.

   Answer: Remind your coworker that you should not discuss clients where others can hear you, and you should only discuss clients when it is important for providing care.

7. You notice a client's record sitting open and out where others can see it.

   Answer: Put the record away immediately, out of sight of unauthorized persons.

8. A computer screen that can be seen by others is on, displaying client information.

   Answer: 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. You answer the phone and someone asks for information about a client.

   Answer: If the individual on the phone is authorized to access the client's information, you may give the information as long as no one else can overhear you. If the client has not signed a consent form or a specific authorization, you may not give the information.

The Health Insurance Portability and Accountability Act

Learner's Guide

What is HIPAA?

Congress passed the **H**ealth **I**nsurance **P**ortability and **A**ccountability **A**ct (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. Clients have the right to privacy, meaning that information about them should only be available 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 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 personal health information.

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 sent from state to state over telephone wires or the Internet. Federal laws make sure every state and every provider follow the same rules for privacy, confidentiality, and security.

Compliance with the HIPAA Privacy Rule was required by April 14, 2003.

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 Kind of Information Does HIPAA Protect?

The privacy protections of HIPAA apply to "protected health information," or PHI.

Protected health information 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.

- Information 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 *client record*.

How Does the HIPAA Privacy Rule Protect Client 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***.

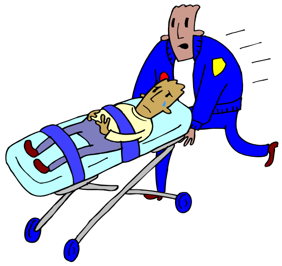
What Is the Difference Between Consent and Authorization?

- To give ***consent***, a client must sign a consent form. The client only needs to sign the consent 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.

Are There Exceptions to the HIPAA Privacy Rule?

The HIPAA Privacy Rule permits Covered Entities to disclose healthcare information without that 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.

May A Person See His Personal Protected Health Information (PHI) and Make Changes?

A Covered Entity ***must allow*** a person to view and photocopy his PHI if that person submits a request. The organization ***may charge*** the person for copies of his 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 PHI.

- A Covered Entity may deny a person access to his 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 PHI contains information that is incorrect, he 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 they did not create the information.

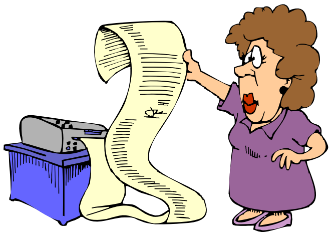
What Else are Covered Entities Required to Do?

- Notify clients about their privacy rights and give clear, written explanation of how the provider may use and disclose the client's health information.
- 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.

Protection of Client Privacy and Confidentiality

Quality client care requires communication between care workers. Computers, the Internet, e-mails, and faxes make it easier to share client 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 personal health information could result in job discrimination, personal embarrassment, or the loss or denial of health insurance.



Considerations for Safeguarding Confidentiality

- Confidentiality of information, whether in written, electronic, or verbal form, is a priority. Confidentiality should extend to all health information.

- **Handle all client records as confidential at all times. Do not leave them open where unauthorized persons can see them.**

> ***Remember this Rule*:**
>
> **The right information, to the right person, for the right reasons.**

- Learn the safeguards your organization requires for the use, disclosure, and storage of personal health information. 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 client information in a private place so others cannot overhear the conversation.**

- A cover sheet marked *Confidential* should accompany all faxed information.

- When e-mailing information about a client, remove any detailed identifying information. For example, refer to the client by initials or by the internal client number, instead of by the full name.

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

- **Use only objective, precise language when documenting in the client 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 personal health information.

- Think about how you would want your personal health information treated, and give your clients that much protection and more.

HIPAA: Test

Name ___________________________ Date ____________ Score _________
(Must score at least 9 points to pass)

Directions: Fill in the blank or circle the best answer.

1. When sending information by fax, the cover sheet should be marked

   ________________________.

2. PHI stands for _____________________ health information.

3. Confidentiality should extend to all ____________________ information.

4. If a person thinks his personal PHI contains incorrect information there is nothing he can do about it. True or False

5. The most common example of PHI is the _____________ ____________.

6. If a provider wants to disclose a client's PHI for purposes of providing care, the provider needs the client's consent. True or False

7. A client must sign a consent form only one time per provider to release information for purposes of providing healthcare. True or False

8. Under the privacy rule, your organization must allow a person to view and photocopy his PHI if that person submits a request. True or False

9. Specific ___________________________ is required if you want to use or disclose a person's PHI for purposes not related to providing healthcare.

10. (worth 3 points) An important rule to remember is: The right

    ________________________, to the right _________________________, for the

    right _________________________.

11. Is the organization you work for a Covered Entity? Yes or No

Certificate of Completion

Awarded to: ________________________________
(Name of Participant)

For Completing the One-Hour Course Entitled

The Health Insurance Portability and Accountability Act

Date of Course: ________________________________

Organization: ________________________________

Presented by: ________________________________
(Signature of presenter, or write "self-study")