HIPAA

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 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 (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 pateint 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 organizaiton, request restrictions on how their PHI is used and disclosed, receive confidential communciaitns, receive a report of certain disclosures of their PHI, and request amendments to their informaiton. The privacy notice must also let patients know how to file a complaint with your organization 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. 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
- 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 personal 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.

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.

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 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 you 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.

TEST HIPAA

Name _____ **Date** _____ **Score** _____

Directions: Circle the best answer. (Seven correct answers required.)

1. HIPAA stands for:
   a. Health Inclusion Portability and Assurance Act
   b. Health Information Protection and Assurances Act
   c. Health Identification Protection and Accountability Act
   d. Health Insurance Portability and Accountability Act

2. _____ refers to preventing someone from hearing or seeing a person's private health records and information unless he or she has the proper authorization.
   a. Privacy
   b. Confidentiality
   c. Security
   d. None of the above

3. HMOs are *not* considered "covered entities" under HIPAA.
   a. True b. False

4. The patient record is included in the protected health information (PHI).
   a. True b. False

5. If a frontline staff member wants to disclose a person's PHI for puposes of providing healthcare, the provider needs to obtain the person's _____.
   a. electronic health record
   b. authorization
   c. consent
   d. none of the above

TEST HIPAA (cont.)

6. A covered entity must allow a person to view and photocopy his or her PHI if that person submits a request.

   a. True b. False

7. Home health agencies and other covered entities are required to do all of the following *except*:

   a. Notify patients of their privacy rights
   b. Maintain all patient records in print under lock and key
   c. Train employees so that they are fully aware of the privacy procedures
   d. Implement safeguards to prevent intentional or accidental misuse of PHI

8. A cover sheet marked "Confidential" should accompany all faxed information.

   a. True b. False

9. Even if frontline staff are certain that the person they are speaking with is permitted to hear certain information, they should not discuss a patient's PHI _____.

   a. on Facebook
   b. at parties
   c. in restrooms of public buildings
   d. all of the above

10. If uncertain as to whether a family member needs to know information about a patient, frontline staff should _____.

    a. consult with other frontline staff
    b. notify the patient
    c. check with their supervisor
    d. ask the family member whether they are permitted to know the information

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 learners take the test. Review test answers together. Each participant who answers 70% correctly (seven correct answers out of 10 questions) may receive a certificate.

Test answers

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