HIPAA

Lesson 1: Objectives

After completion of this course, you will be able to:

- Describe the HIPAA Privacy Rule, including the permitted uses and disclosures of protected health information by covered entities and business associates, uses and disclosures that require individual authorization, the privacy practices notice, and administrative requirements;
- Describe the HIPAA Security Rule, including a risk analysis and the maintenance of administrative, physical, and technical safeguards;
- Identify the role of the Office for Civil Rights in enforcement and penalties for noncompliance; and
- Describe the Breach Notification Rule.

Introduction

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the Secretary of the U.S. Department of Health and Human Services (HHS) to develop regulations protecting the privacy and security of certain health information. To meet this requirement, HHS created what are commonly known as the HIPAA Privacy Rule and the HIPAA Security Rule. The Privacy Rule set up national standards for the use and disclosure of protected health information (PHI), by covered entities, as well as standards for providing individuals with rights to understand and control how their health information is used. The Security Rule set up national standards for the protection of an individual's health information that is created, received, maintained or transmitted, in electronic form.

The Health Information Technology for Economic and Clinical Health (HITECH) Act was signed into law in 2009 to promote the adoption and meaningful use of health information technology. The HITECH Act addresses the privacy and security concerns associated with the electronic transmission of health information by strengthening the enforcement of the HIPAA rules and requiring HIPAA covered entities and their business associates to provide notification following a breach of unsecured PHI.

Lesson 2: The Privacy Rule

The Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this "protected health information (PHI)". PHI includes information related to the individual's past, present, or future physical or mental health or condition; the health care provided; or the past, present, or future payment for health care; and identifies the individual. PHI includes many common identifiers such as name, address, and birth date.

De-identified information is PHI stripped of identifiers in a manner that results in information that is no longer protected by the Privacy Rule. There are two de-identification methods: formal determination by a qualified expert or the removal of 18 specified identifiers, also known as the safe harbor method.

Quiz Question:

Drag the correct words from the word bank to define Protected Health Information (PHI).

PHI includes information related to the individual's past, present, or future ***physical or mental health or condition**; the health care ***provided**; or the past, present, or future **payment** for health care; and ***identifies** the individual.

Lesson 3: Covered Entities and Business Associates

The Privacy Rule applies to "covered entities" such as health plans, health care clearinghouses, and health care providers. Health plans are individual and group plans that provide or pay the cost of medical care, including health, dental, and vision insurers. Health care clearinghouses process nonstandard information into a standard or vice versa, such as billing services. Health care providers include all providers of services (such as hospitals) and providers of medical and health services (such as physicians) and any other person or organization that delivers, bills, or is paid for health care. Every health care provider who electronically transmits health information in connection with certain transactions (such as claims, benefit eligibility questions, and referral authorization requests) is a covered entity.

A business associate is a person or organization that performs certain functions on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of PHI. When "business associate" services are used an agreement must be obtained which addresses safeguards for PHI. If the business associate delegates or outsources services or functions to a subcontractor, that subcontractor becomes a business associate if they need to access, use, or disclose PHI to perform their services. Entities that store PHI, either electronic or in hard copy, are also business associates even if they don't access, use, or disclose that information, however entities that merely transport PHI are not business associates.

Quiz Question:

Match the following covered entity with their description:

Health plans = *Individual and group plans that provide or pay the cost of medical care.

Health care clearinghouses = *Process nonstandard information into a standard or vice versa.

Health care providers = *All providers of services and providers of medical and health services and any other person or organization that delivers, bills, or is paid for health care.

Lesson 4: Uses and Disclosures of PHI

A covered entity is permitted to use and disclose PHI, without an individual's authorization, to the individual who is the subject of the information; for treatment, payment and health care operations; with opportunity to agree or object; with incident to an otherwise permitted use or disclosure; for limited data set; and for public interest and benefit activities.

Treatment, Payment, and Health Care Operations

Treatment is the delivery, coordination, or management of health care for an individual by health care providers. Payment includes, but is not limited to, activities of a health care provider to obtain payment or be reimbursed for providing health care. Health care operations include, but are not limited to, quality assessment and improvement activities. An exception to this rule applies to psychotherapy notes, which in fact require individual authorization for use or disclosure.

Opportunity to Agree or Object

A health care provider may rely on an individual's informal permission to list in its facility directory the individual's name, condition, religion, and location in the facility; to disclose to family members or others PHI directly relevant to that person's involvement in the individual's care or payment for care; to notify family members or others of the individual's location, condition, or death; and to notify entities authorized by law to assist in disaster relief efforts.

Incidental Use and Disclosure

Use or disclosure of information that occurs as a result of an otherwise permitted use or disclosure is allowed as long as the covered entity has adopted reasonable safeguards and the information being shared was limited to the "minimum necessary" to accomplish the intended purpose.

Limited Data Set

Limited data set is PHI from which certain direct identifiers of individuals and their relatives, household members, and employers have been removed.

Public Interest and Benefit Activities

The Privacy Rule permits use and disclosure of PHI for the following purposes:

- as required by law
- for public health authorities to collect or receive information for preventing or controlling disease, injury, or disability and receive reports of child abuse and neglect; entities subject to U.S Food and Drug Administration (FDA) regulation; individuals who may have contracted or been exposed to a communicable disease; for information concerning a work-related illness or injury or workplace related medical surveillance; for proof of immunization of a student or prospective student to a school that is required by State or other law to have such proof prior to admission and the entity receives and documents the agreement to the disclosure from either a parent, guardian, or the individual (as applicable).
- to government authorities regarding victims of abuse, neglect, or domestic violence
- to health oversight agencies
- in a judicial or administrative proceeding
- to law enforcement officials
- to funeral directors, and to coroners or medical examiners to identify a deceased person, determine the cause of death, and perform other functions
- to facilitate the donation and transplantation of organs, eyes, and tissue
- for research purposes
- to prevent or lessen a serious and imminent threat to a person or the public
- for government functions
- to comply with workers' compensation laws

A covered entity must obtain the individual's written authorization for any other use or disclosure of PHI, including the marketing and sale of PHI. Individual authorization must be received before using PHI for marketing communications that encourage recipients to purchase or use a product or service. This is also required if the covered entity receives payment from a third party whose services are being marketed, unless it falls under an exclusion such as communications promoting good health or providing information about government programs.

Covered entities are prohibited from receiving direct or indirect financial compensation in exchange for the sale of PHI unless they receive individual authorization. All authorizations must be in plain language and contain specific information regarding what is to be disclosed or used, the person disclosing and receiving the information, expiration, the right to revoke, and other data.

Genetic Information

In accordance with the Genetic Information Nondiscrimination Act of 2008 (GINA) genetic information is health information and group health plans, health insurance issuers, and issuers of Medicare supplemental policies are which prohibited from using or disclosing genetic information for underwriting purposes.

Quiz Question:

A covered entity is permitted to use and disclose PHI, without an individual's authorization: (Select all that apply)

a. ***To the individual who is the subject of the information.**
b. ***For treatment, payment, and health care operations.**
c. ***With opportunity to agree or object.**
d. ***With incident to an otherwise permitted use or disclosure.**
e. ***For limited data set.**
f. ***For public interest and benefit activities.**
g. For marketing of PHI.
h. For sale of PHI.
i. For the disclosure of psychotherapy notes.

Lesson 5: Privacy Practices Notice

Each covered entity must provide a notice of its privacy practices. The notice must describe the ways in which the entity may use and disclose PHI. The notice must also describe the individuals' rights, including the right to review their PHI, obtain a copy of or electronic access to their PHI, or change information that is inaccurate or incomplete in their designated record set; the right to a list of disclosures; the right to request that a covered entity restrict the use or disclosure of PHI, including the disclosure to a group health plan of a service or item that the individual has paid in full and out of pocket; the right to request an alternative means or location for receiving communications; and the right to complain to HHS and to the entity if it is believed a right has been violated. Individuals must also be informed that they will be notified of a breach of unsecured PHI; that written authorization is required for uses or disclosures for marketing purposes, the sale of PHI, as well as for the disclosure of psychotherapy notes; that the use or disclosure of PHI that is genetic information for underwriting purposes is prohibited; and they may opt-out of fundraising communications. In an emergency treatment situation, the health care provider may present the notice as soon as it is reasonable to do so.

A health care provider must also make a good faith effort to obtain written acknowledgement of the receipt of the privacy practices notice and document the reason for any failure to obtain the acknowledgement. Health care providers are not required to obtain a written acknowledgment from individuals in an emergency treatment situation.

Quiz Question:

An individual has the right: (Select all that apply)

a. ***To review their PHI, obtain a copy of or electronic access to their PHI, or change information that is inaccurate or incomplete in their designated record set.**
b. ***To a list of disclosures.**
c. ***To request that a covered entity restrict the use or disclosure of PHI.**

d. ***To request an alternative means or location for receiving communications.**
e. ***To complain to HHS and to the entity if it is believed a right has been violated.**

Lesson 6: Administrative Requirements

A covered entity must meet the following administrative requirements:

- develop, implement, and enforce privacy policies and procedures
- designate a privacy official responsible for developing and implementing its policies and procedures, and a contact person or contact office responsible for receiving complaints and providing individuals with information on its privacy practices
- train all workforce members on its policies and procedures and take action against those who violate it
- lessen any harmful effect caused by use or disclosure of PHI by its workforce
- maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent deliberate or accidental use or disclosure of PHI and limit its incidental use and disclosure
- establish procedures for individuals to complain about its compliance with its privacy policies and procedures, including to the Secretary of HHS
- avoid retaliation against a person for exercising their rights, assisting in an investigation by HHS or another appropriate authority, or opposing an act or practice that the person believes in good faith violates the Privacy Rule
- maintain until six years after the date of their creation or last effective date, its privacy policies and procedures, its privacy practices notices, disposition of complaints, and other actions and activities that the Privacy Rule requires to be documented

Lesson 7: The Security Rule

The Security Rule requires covered entities and business associates to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting electronic protected health information (e-PHI). Covered entities and business associates must ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain, or transmit; identify and protect against anticipated threats to the security or integrity of the information; protect against anticipated, unpermitted uses or disclosures; and ensure compliance by their workforce.

Quiz Question:

The Security Rule requires covered entities and business associates to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting electronic protected health information.

***True** or False

Lesson 8: Risk Analysis and Management

The Security Rule requires covered entities and business associates perform a risk analysis as part of their security management processes. The risk analysis process includes, but is not limited to, the evaluation of the likelihood and impact of potential risks to e-PHI; implementation of security measures to address the risks identified in the risk analysis; documentation of the chosen security measures with rationale; and maintenance of continuous, reasonable, and appropriate security protections. Risk analysis is an ongoing process, in which a covered entity or business associate regularly reviews its records to track access to e-PHI and detect security incidents, evaluates the effectiveness of security measures put in place, and reevaluates potential risks to e-PHI.

Lesson 9: Administrative, Physical, and Technical Safeguards

A covered entity or business associate must maintain the following administrative, physical, and technical safeguards for protecting e-PHI.

Administrative Safeguards

A covered entity or business associate must:

- designate a security official who is responsible for developing, implementing, and enforcing its security policies and procedures
- authorize access to e-PHI only when appropriate based on the user or recipient's role and terminate access when the employment of a workforce member ends
- provide for appropriate authorization and supervision of workforce members who work with e-PHI
- train all workforce members regarding its security policies and procedures and take action against workforce members who violate them
- perform a periodic assessment of how well its security policies and procedures meet the requirements of the Security Rule
- maintain until six years after the date of creation or last effective date, security policies and procedures and records of required actions, activities, or assessments
- periodically review and update its documentation in response to environmental or organizational changes that affect the security of e-PHI

Physical Safeguards

A covered entity or business associate must:

- limit physical access to its facilities while ensuring that authorized access is allowed
- specify proper use of and access to workstations and electronic media

- implement policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media

Technical Safeguards

A covered entity or business associate must:

- allow only authorized persons to access e-PHI
- implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use e-PHI
- ensure that e-PHI is not improperly altered or destroyed
- guard against unauthorized access to e-PHI that is being transmitted over an electronic network

Quiz Question:

What are the three safeguards for protecting e-PHI?

a. ***Administrative, Physical, Technical.**
b. Safety, Health, Occupational.
c. Accountability, Portability, Timing.
d. Compliance, Testing, Observation.

Lesson 10: Enforcement and Penalties for Noncompliance

The HHS, Office for Civil Rights is responsible for administering and enforcing the HIPAA Privacy Rule and HIPAA Security Rule and may conduct random audits and investigate complaints and breach reports. Covered entities and business associates that fail to comply with the HIPAA rules may be subject to civil money penalties. The HITECH Act significantly increased the penalty amounts the HHS Secretary may demand for violations, up to $1.5 million per year for each violation and encourages quick corrective action by the covered entity or business associate.

Quiz Question:

The Office for Civil Rights is responsible for administering and enforcing the HIPAA rules.

***True** or False

Lesson 11: Breach Notification Rule

In addition to enforcing new civil money penalty amounts for HIPAA rule violations, the HITECH Act requires covered entities and their business associates to provide notification following a breach of unsecured PHI (discovered on or after September 23,

2009), to the affected individual(s), the HHS Secretary, and, in certain circumstances, the media. PHI that is used or disclosed in violation of the Privacy Rule requires breach notification unless one of the following three exceptions apply: unintentional access or disclosure by employees authorized to access PHI and acting in good faith within the scope of that authority, inadvertent disclosure between employees authorized to access PHI, and/or instances in which it is reasonable to believe the disclosed PHI has not actually been viewed or retained applies. The covered entity or business associate may also conduct a risk assessment to determine if there is a low-probability that the PHI has been compromised by considering the following factors: the nature and extent of the PHI involved, the unauthorized person who used the PHI or to whom the PHI was disclosed, whether the PHI was actually acquired or viewed, and the extent to which the risk to the PHI has been lessened. Unsecured PHI is information that has not been rendered unusable, unreadable, or indecipherable through the use of a technology or methodology such as encryption and destruction. If electronic PHI is encrypted it is considered to be secured under the Breach Notification Rule.

Quiz Question:

Electronic PHI that is encrypted is secured.

***True** or False

Lesson 12: Conclusion

(NOTE: You may wish to display the contact information for the appropriate personnel within your organization.)

Your organization is committed to protecting the privacy and security of PHI. And it takes your help! If you have any questions regarding the HIPAA Privacy Rule, HIPAA Security Rule or Breach Notification Rule, contact the appropriate personnel within your organization for guidance and assistance.

Test Questions (10 questions Pre-Test or 5 questions Post-Test)

Pool 1 (6 or 3 questions)

MULTIPLE CHOICE

1. A covered entity must obtain the individual's written authorization to use or disclose:
    a. PHI for treatment, payment, and health care operations.
    b. PHI to the individual who is the subject of the information.
    c. Psychotherapy notes.
    d. PHI for public interest and benefit activities.

2. An individual has the right:
    a. To obtain a copy of or electronic access to their PHI.
    b. To a list of disclosures.
    c. To request an alternative means or location for receiving communications.
    d. To request that a covered entity restrict the use or disclosure to PHI.
    e. All of the above.

3. The Security Rule set up national standards for the protection of an individual's health information that is:
    a. Transmitted in electronic form.
    b. Received in electronic form.
    c. Maintained in electronic form.
    d. All of the above.

4. The HITECH Act:
    a. Addresses the privacy and security concerns associated with the electronic transmission of health information.
    b. Strengthens the enforcement of the HIPAA rules.
    c. Requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured PHI.
    d. All of the above.

5. PHI is an acronym for:
    a. Protected Health Information.
    b. Personal Health Information.
    c. Permitted Health Information.
    d. Primary Health Information.

6. Which of the following is not a protected identifier?
    a. Name.
    b. Favorite color.
    c. Address.

d. Birth date.

7. Individuals must be informed of which of the following:
   a. A breach of unsecured PHI.
   b. The use and disclosure of PHI that is genetic information for underwriting purposes is prohibited.
   c. They may opt-out of fundraising communications.
   d. All of the above.

8. Written authorization is required for:
   a. Uses or disclosures of PHI for marketing purposes.
   b. Sale of PHI.
   c. Disclosure of psychotherapy notes.
   d. All of the above.

Pool 2 (4 or 2 questions)

TRUE/FALSE

9. Hospitals are “covered entities” and therefore must comply with the Privacy Rule.

10. Covered entities must ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain, or transmit.

11. The Office for Civil Rights is responsible for administering and enforcing the HIPAA rules.

12. The Security Rule set up national standards for the use and disclosure of PHI.

13. The HITECH Act was signed into law to promote the adoption and meaningful use of health information technology.

14. Only the Emergency Department must provide a notice of its privacy practices.

15. Covered entities that fail to comply with the HIPAA rules may be subject to civil money penalties.

16. De-identified information is PHI stripped of identifiers in a manner that results in information that is no longer protected by the Privacy Rule.

17. Entities that transport PHI, but do not access, use, or disclose the information are business associates.

18. The use or disclosure of genetic information for underwriting purposes is prohibited.

19. Individual authorization must be received before using PHI for marketing.

20. Individual authorization must be received before the sale of PHI.