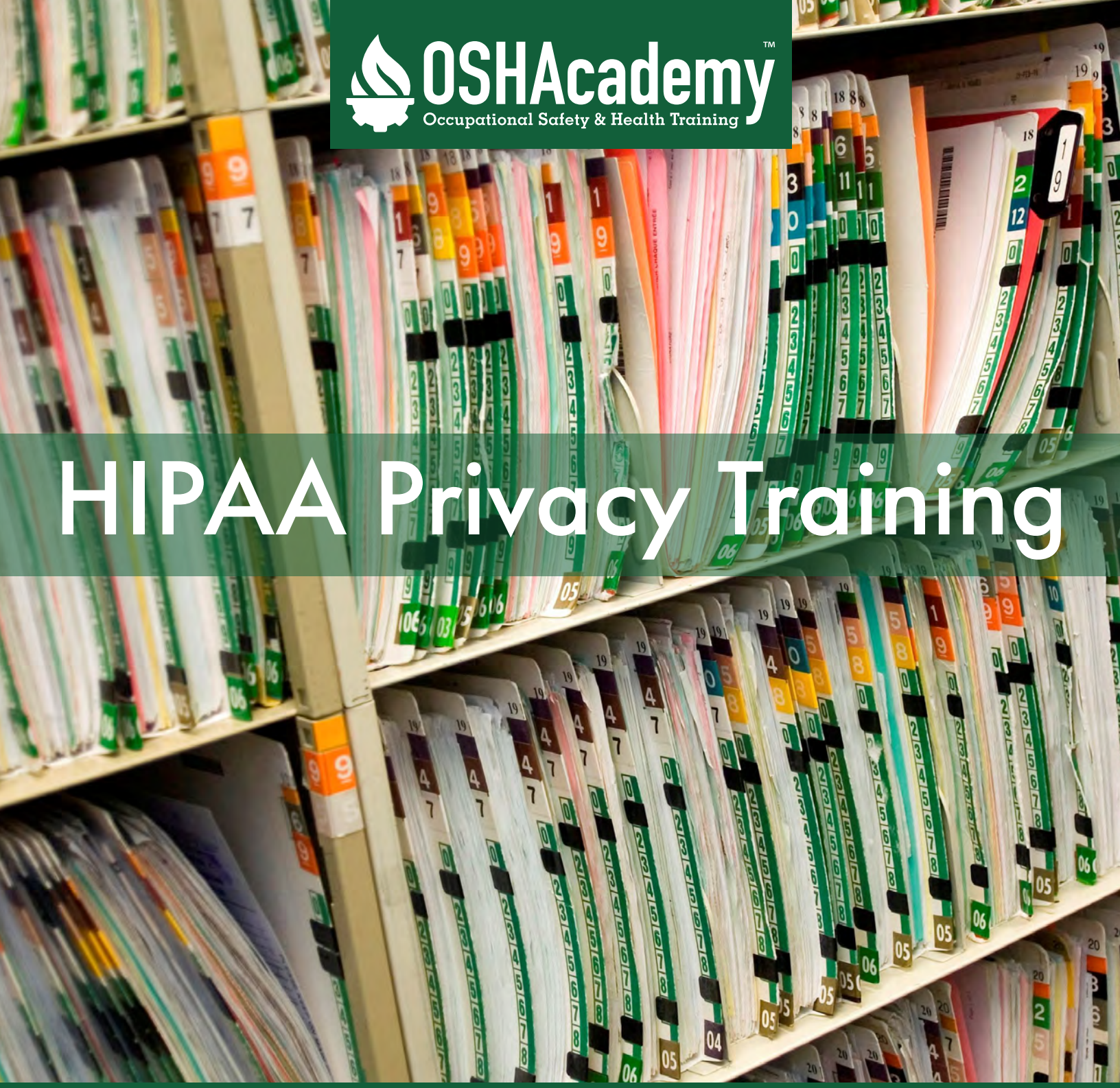
OSHAcademy™
Occupational Safety & Health Training



HIPAA Privacy Training

HIPAA stands for "Health Insurance Portability and Accountability Act" (HIPAA). President Bill Clinton signed the bill into law on August 21, 1996. It is said to be the most significant act of Federal legislation to affect the health care industry since Medicare and Medicaid were rolled out in 1965. The law officially became effective on July 1, 1997. HIPAA required the Secretary of the U.S. Department of Health and Human Services (HHS) to develop regulations to protect the privacy and security of certain health information. Healthcare providers and employees should take this important course to receive a summary of key elements of the HIPAA rules.

This page intentionally blank

OSHAcademy Course 625 Study Guide

HIPAA Privacy Training

This study guide is designed to be reviewed off-line as a tool for preparation to successfully complete OSHAcademy Course 625.

Read each module, answer the quiz questions, and submit the quiz questions online through the course webpage. You can print the post-quiz response screen which will contain the correct answers to the questions.

The final exam will consist of questions developed from the course content and module quizzes.

We hope you enjoy the course and if you have any questions, feel free to email or call:

OSHAcademy

15220 NW Greenbrier Parkway, Suite 230
Beaverton, Oregon 97006
www.oshatrain.org
instructor@oshatrain.org
+1 (888) 668-9079

Revised: October 4, 2019

This page intentionally blank

Contents

Course Introduction

HIPAA Law

HIPAA stands for "Health Insurance Portability and Accountability Act" (HIPAA). President Bill Clinton signed the bill into law on August 21, 1996. It is said to be the most significant act of Federal legislation to affect the health care industry since Medicare and Medicaid were rolled out in 1965. The law officially became effective on July 1, 1997.

HIPAA required the Secretary of the U.S. Department of Health and Human Services (HHS) to develop regulations to protect the privacy and security of certain health information.

Who Must Follow These Laws

The following is a specific list of who needs to be HIPAA compliant:

- **covered healthcare providers** (hospitals, clinics, regional health services, individual medical practitioners) who carry out transactions in electronic form
- **healthcare clearinghouses** (billing services, repricing companies, community health management information systems, information systems, and value-added networks)
- **health plans** (including insurers, HMOs, Medicaid, Medicare prescription drug card sponsors, flexible spending accounts, public health authority, in addition to employers, schools or universities who collect, store or transmit EPHI, or electronic protected health information)
- **business** associates of covered entities (including private sector vendors and third-party administrators)

Who Is Not Required to Follow These Laws

Many organizations that have health information about you do not have to follow these laws. Examples of organizations that do not have to follow the Privacy and Security Rules include:

- life insurers
- employers
- workers compensation carriers
- most schools and school districts

- many state agencies like child protective service agencies
- most law enforcement agencies
- many municipal offices

Course Components

This course is a summary of key elements of the HIPAA rules and not a complete and comprehensive guide to compliance. Entities regulated by the Rule are obligated to comply with its applicable requirements and should not rely on this summary as a source of legal information or advice.

Module 1: HIPAA Overview

Privacy Rule

The Privacy Rule establishes national standards for the protection of certain health information. It applies to all forms of individuals' protected health information, whether electronic, written, or oral. The major goal of the Privacy Rule is to make sure an individuals' health information is properly protected while allowing the flow of health information needed to provide high quality health care and to protect the public's health and well-being. The Rule strikes a balance that permits important uses of information, while protecting the privacy of those who need care.

The Privacy Rule covers a health care provider whether it electronically transmits these transactions directly or uses a billing service or other third party to do so on its behalf.

For the average health care provider or health plan, the Privacy Rule requires activities, such as:

- Notify patients about their privacy rights and how their information can be used.
- Adopting and implementing privacy procedures for its practice, hospital, or plan.
- Training employees so that they understand the privacy procedures.
- Designate an individual to be responsible for seeing that the privacy procedures are adopted and followed.
- Secure patient records containing individually identifiable health information so that they are not readily available to those who do not need them.

1. The major goal of the Privacy Rule is to _____.

a. protect the provider
b. protect an individuals' health information
c. keep documents sealed
d. protect the insurance company

Protecting Patients' Privacy

Responsible health care providers and businesses already take many of the kinds of steps required by the Rule to protect patients' privacy. To ease the burden of complying with the

requirements, the Privacy Rule gives needed flexibility for providers and plans to create their own privacy procedures, tailored to fit their size and needs.

The scalability of the Rule provides a more efficient and appropriate means of safeguarding protected health information than would any single standard.

Here are some examples:

- The privacy official at a small physician practice may be the office manager, who will have other non-privacy related duties; the privacy official at a large health plan may be a full-time position, and may have the regular support and advice of a privacy staff or board.

- The training requirement may be satisfied by a small physician practice's providing each new member of the workforce with a copy of its privacy policies and documenting that new members have reviewed the policies; whereas a large health plan may provide training through live instruction, video presentations, or interactive software programs.

- The policies and procedures of small providers may be more limited under the Rule than those of a large hospital or health plan, based on the volume of health information maintained and the number of interactions with those within and outside of the health care system.

2. To ease the burden of complying with HIPAA requirements, the Privacy Rule _____.

a. has specific requirements for each provider
b. mandates clear instructions on all procedures
c. gives providers flexibility to create their own privacy procedures
d. relies on each provider self-check their compliance

Security Rule

The HIPAA Security Rule establishes a national set of security standards for protecting certain health information that is held or transferred in electronic form.

Prior to HIPAA, no generally accepted set of security standards or general requirement for protecting health information existed in the healthcare industry. At the same time, new technologies were being created, and the health care industry began to move away from paper processes and rely more heavily on the use of electronic information systems to pay claims,

answer eligibility questions, provide health information, and conduct a host of other administrative and clinically based functions.

A major goal of the Security Rule is to protect the privacy of individuals' health information while allowing covered entities to adopt new technologies to improve the quality and efficiency of patient care. The health care marketplace is so diverse; therefore, the Security Rule is designed to be flexible so a covered entity can implement policies, procedures, and technologies appropriate for the entity's size, organizational structure, and risks to consumers' personal information.

3. The HIPAA _____ establishes a national set of standards for protecting certain health information that is held or transferred in electronic form.

a. Protection Rule
b. Non-compete Rule
c. Privacy Rule
d. Security Rule

Security Rule Coverage

The Security Rule applies to health plans, healthcare clearinghouses, and any health care provider who transmits health information in an electronic form.

Covered entities include individual and group plans who provide or pay the cost of medical care. Health plans include the following:

- health
- dental
- vision
- prescription drug insurers
- health maintenance organizations ("HMOs")
- Medicare, Medicaid, Medicare+Choice and Medicare supplement insurers
- long-term care insurers (excluding nursing home fixed-indemnity policies)

4. The HIPAA Security Rule applies to each of the following, EXCEPT _____.

a. health plans
b. employers who provide employment information
c. healthcare clearinghouses
d. providers transmitting health information electronically

Health Plans

Health plans also include employer-sponsored group health plans, government and church-sponsored health plans, and multi-employer health plans. There are exceptions—a group health plan with less than 50 participants that is administered solely by the employer that established and maintains the plan is not a covered entity.

The following two types of government-funded programs are not health plans:

1. those whose principal purpose is not providing or paying the cost of health care, such as the food stamps program

2. those programs whose principal activity is directly providing health care, such as a community health center, or the making of grants to fund the direct provision of health care

Certain types of insurance entities are also not health plans, including entities providing only workers' compensation, automobile insurance, and property and casualty insurance.

Privacy vs. Security

Privacy and security go hand-in-hand. Privacy is the "what." It says patients have the right to have their health information protected from unauthorized disclosures. Security is the "how." In other words, agencies must determine the procedures they will put into place to protect health information.

According to the Department of Health and Human Services (HHS), most Security Rule violations occur as a result from a covered entity not having adequate policies and procedures in place to safeguard personal information contained on its information systems.

5. Privacy is the _____ and security is the _____.

a. what, when
b. when, where
c. how, what
d. what, how

HIPAA Privacy

This part of the law prohibits the disclosure of Protected Health Information (PHI) in any form except as required or permitted by law.

The HIPAA Privacy rule mandates how PHI may be used and disclosed.

The Privacy Rule protects PHI in any form including but not limited to:

- e-mail
- fax
- information on the computer
- voice
- paper

The HIPAA Privacy Rule says don't listen, tell, or show any client's PHI to anyone who does not have a legitimate right to see or hear that information.

6. The Privacy Rule protects Protected Health Information (PHI) _____.

a. as required by OSHA
b. in any form
c. when in transmission
d. in writing only

Protected Healthcare Identifiers (PHI)

The Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form of media, whether electronic, paper, or oral.

HIPAA protects information that alone or combined may identify a patient, the patient's relatives, employer or household members. Health information that contains even one patient identifier is protected under HIPAA.

Here are some examples:

- name
- address
- birthdate
- telephone numbers
- fax numbers
- email addresses
- social security number
- medical record number
- health plan beneficiary number
- account number
- voice recordings
- photographic images
- other characteristics which may identify the person, such as the individual's past, present, or future physical or mental health or condition

7. Health information that contains at least _____ patient identifier(s) is protected under HIPAA.

a. 1
b. 2
c. 5
d. 10

PHI Locations

Here are some examples of other places you might find patient information:

- patient status boards
- financial records
- fax sheets
- data used for research purposes
- patient's identification bracelet
- prescription bottle labels
- photograph or video recording of a patient

Wrongful Disclosure of PHI

If you observe someone wrongfully disclosing PHI, you should do the following:

1. First, talk to the person who is disclosing PHI. Tell them what you heard or saw and why you believe PHI has been wrongfully disclosed.

2. Then talk with your supervisor about the situation immediately.

If you wrongfully disclose PHI, you should do the following:

1. Write down the following information:
    - whose PHI was disclosed
    - how it was disclosed
    - to whom
    - what day and time
    - what was done to correct the problem
2. Inform your supervisor immediately.

8. If you observe someone wrongfully disclosing PHI, what should you do FIRST?

a. Talk with your supervisor about the situation
b. Talk to the person who is disclosing PHI
c. Confront the patient
d. Delete any personal information from your computer

Good Privacy Practices

There are several things that can be put into place to protect a patients' privacy. Here are just a few examples:

- Do put papers with PHI in a secured area
- Don't leave PHI exposed where other can see the content.
- Do discuss cases in private.
- Don't discuss a case in a public area where other people can overhear you.
- Use passwords to keep other people from accessing your computer files.
- Make sure your computer is locked when you leave your desk.
- Minimize PHI in e-mails. Include as little as possible.
- Protect fax machines that will be receiving PHI by putting them in secure and private locations.

9. Two doctors are eating lunch at a busy restaurant, and discussing a patient case that involves confidential PHI regarding the patient. What should they do?

a. Ask others what they think
b. Move to a private location
c. Announce they are discussing PHI
d. Don't use the name of the patient

To review your questions, go online, answer the questions and on the last section, click on the "Check Quiz Answers" button, and follow the instructions.

Module 2: Your Personal Rights Under HIPAA

Most of us believe our medical and other health information is private and should be protected. Most of us also want to know who has access to this private information. The Privacy Rule gives you rights over your health information and sets rules and limits on who can look at and receive your health information.

Protected Information

The following information is protected for each individual:

- information your doctors, nurses, and other health care providers put in your medical record
- conversations your doctor has about your care or treatment with nurses and others
- information about you in your health insurer's computer system
- billing information about you at your clinic
- most other health information about you held by those who must follow these laws

Covered entities must put in place safeguards to protect your health information and ensure they do not use or disclose your health information improperly. They must also have procedures in place to limit who can view and access your health information, as well as implement training programs for employees about how to protect your health information.

1. When are conversations your doctor has about your care or treatment with nurses and others protected?

a. Never
b. Always
c. Sometimes
d. Rarely

Individual Rights

Under HIPAA, patients are entitled to more information about and more control over their individual health information.

Under HIPAA, you are entitled to more information about and more control over your individual health information.

1. **Access to Information** – You can request and receive a copy of your health information and may request that copy be in electronic form. The covered entity may charge a reasonable fee for providing the copy either in paper or electronic form.
2. **Amend information** – You may ask for your information to be amended to correct errors but covered entities are only responsible for making changes in the records that they created.
3. **Accounting of disclosures** – You may request a list of all the times your information was released improperly.
4. **Notice of Privacy Practices** – You have the right to receive a written notice of privacy practices from covered entities that details rights of the individual and duties of the covered entity under HIPPA.

2. Under HIPAA, an individual may request each of the following, EXCEPT _____.

a. written notice of privacy practices from covered entities
b. a list of all times their information was released improperly
c. copies of their health information in electronic form
d. cancellation of any fees for copies of health information

Employers and Health Information in the Workplace

The Privacy Rule controls how a health plan or covered health care provider discloses protected health information to an employer, including your manager or supervisor.

Employer Requests

The Privacy Rule does not prevent your supervisor, human resources worker or others from asking you for a doctor's note or other information about your health if your employer needs the information to administer sick leave, workers' compensation, wellness programs, or health insurance.

If your employer asks for your health care provider directly for information about you, your provider cannot disclose the information without your authorization. Covered health care providers must also have your authorization to disclose this information to your employer, unless other laws require them to disclose it.

Generally, the Privacy Rule applies to disclosures made by your health care provider, not to the questions of your employer.

Employment Records

The Privacy Rule does not protect your employment records, even if the information in those records is health-related. Generally, the Privacy Rule also does not apply to the actions of an employer, including the actions of a manager in your workplace.

If you work for a health plan or covered health care provider:

- The Privacy Rule does not apply to your employment records.
- The Rule *does* protect your medical or health plan records if you are a patient of the provider or a member of the health plan.

3. The HIPAA _____ controls how a health plan or covered health care provider discloses protected health information (PHI) to an employer, including your manager or supervisor.

a. Protection Rule
b. Non-compete Rule
c. Privacy Rule
d. Security Rule

Sharing Health Information

Under HIPAA, your health care provider may share your personal information face-to-face, over the phone, or in writing. However, a central aspect of the Privacy Rule that a covered entity must make reasonable efforts to only the minimum amount of protected health information needed to accomplish the intended purpose a request. A health care provider or health plan may share relevant information if:

- You give your provider or plan permission to share the information.
- You are present and do not object to sharing the information.

- You are not present, and the provider determines based on professional judgment that it's in your best interest.

4. A health care provider or health plan may share relevant information if any of the following apply, EXCEPT _____.

a. you are present and do not object to sharing the information
a. you are not present, but the provider believes you will not object
b. you are not present, but the provider believes it is in your best interest
c. you give the provider permission to share the information

Sharing Information with a Family Member or Friend

HIPAA requires most doctors, nurses, hospitals, nursing homes, and other health care providers to protect the privacy of your health information. However, if you don't object, a health care provider or health plan may share relevant information with family members or friends involved in your health care or payment for your health care in certain circumstances.

Examples

- An emergency room doctor may discuss your treatment in front of your friend if you ask that your friend comes into the treatment room.

- A doctor's office may discuss your bill with your adult daughter who is with you at your medical appointment and has questions about the charges.

- A doctor may discuss the drugs you need to take with your health aide who has accompanied you to a medical appointment.

- A doctor may give information about your mobility limitations to your sister who is driving you home from the hospital.

- A nurse may discuss your health status with your brother if you inform her you are going to do so and you do not object. But, a nurse may **NOT** discuss your condition with your brother after you have stated you do not want your family to know about your condition.

5. When may a health care provider discuss a patient's health information with a family member, friend, or other person?

a. If the family member signs a non-disclosure agreement (NDA)
b. If the patient is under the age of 18 and does not object
c. If parental permission has been received by the health care provider
d. If the patient gives the provider permission to share information

Incapacitated or Not Present Patient

If the patient is not present or is incapacitated, a health care provider may share the patient's information with family, friends, or others when the health care provider determines it is in the best interest of the patient.

When someone other than a friend or family member is involved, the health care provider must be reasonably sure the patient asked the person to be involved in his or her care or payment for care. Again, the health care provider may discuss **only** the information the person involved needs to know about the patient's care or payment.

Here are some examples:

- A surgeon who did emergency surgery on a patient may tell the patient's spouse about the patient's condition while the patient is unconscious.
- A pharmacist may give a prescription to a patient's friend who the patient has sent to pick up the prescription.
- A hospital may discuss a patient's bill with her adult son who calls the hospital with questions about charges to his mother's account.
- A health care provider may give information regarding a patient's drug dosage to the patient's health aide who calls the provider with questions about the prescription.

However, a nurse may not tell a patient's friend about a past medical problem unrelated to the patient's current condition. Also, a health care provider is not required by HIPAA to share a patient's information when the patient is not present or is incapacitated, and can choose to wait until the patient has an opportunity to agree to the disclosure.

6. Generally, a health care provider may discuss _____ about the patient's care or payment.

a. any information
b. need-to-know information
c. information that seems reasonable
d. unclassified information

Disclosing PHI to Law Enforcement

The HIPPA Privacy Rule is balanced to protect an individual's privacy while allowing important law enforcement functions to continue. The Rule permits covered entities to disclose protected health information (PHI) to law enforcement officials, without the individual's written authorization, under specific circumstances including, but not limited to:

- To comply with a court order or court-ordered warrant, a subpoena or summons issued by a judicial officer, or a grand jury subpoena.
- To respond to a request for PHI about a victim of a crime, and the victim agrees.
- To report PHI to law enforcement when required by law to do so.
- To alert law enforcement to the death of the individual, when there is a suspicion that death resulted from criminal conduct.

For a complete understanding of the conditions and requirements for these disclosures, please review the exact regulatory text at the HHS FAQ Page for this topic.

7. In which situation may a health care refuse to disclose protected health information (PHI) to law enforcement individuals?

a. When they request PHI about a medical condition unrelated to a crime
b. When required by law to do so
c. If it is necessary to comply with a court order or court-ordered warrant
d. When the request is for PHI about a victim of a crime, and the victim agrees

How to File a Complaint

An employee, or representative of an employee, who believes he or she has been retaliated against for disclosing HIPAA-protected information when reporting or complaining about a workplace safety or health issue, may file a complaint with OSHA within 30 days of the retaliation. The complaint should be filed with the OSHA office responsible for enforcement activities in the geographical area where the employee resides or was employed. It also may be filed with any OSHA officer or employee. For more information, contact your closest OSHA Regional Office.

8. An employee, or representative of an employee, who believes he or she has been retaliated against for disclosing HIPAA-protected information may file a complaint with OSHA _____.

a. at the time the retaliation occurs
b. within 30 days of the retaliation
c. within any reasonable time period
d. after first conferring with the HIPAA administrator

To review your questions, go online, answer the questions and on the last section, click on the "Check Quiz Answers" button, and follow the instructions.

Module 3: Health Care Provider Responsibilities

Covered Entities

As we mentioned in the course introduction, covered entities can be institutions, organizations, or persons, and include the following:

- **Health Plans** - including health insurance companies, HMOs, company health plans, and certain government programs that pay for health care, such as Medicare and Medicaid.
- Health care clearinghouses - entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa.
- **Health care providers** - those that conduct certain business transactions electronically, such as electronically billing your health insurance - including most doctors, clinics, hospitals, psychologists, chiropractors, nursing homes, pharmacies, and dentists.
- **Business associates** - including private sector vendors and third-party administrators.

Generally, these transactions concern billing and payment for services or insurance coverage. For example, hospitals, academic medical centers, physicians, and other health care providers who electronically transmit claims transaction information directly, or through an intermediary to a health plan, are covered entities. Let's take a closer look at each of the entities.

1. Under HIPAA, all the following are covered entities that are required to follow HIPAA laws, EXCEPT _____.

a. health plans
b. workers' compensation insurers
c. health care providers
d. Health care clearinghouses

Health Care Providers

Every health care provider, regardless of size, who electronically transmits health information in certain transactions, is a covered entity. These transactions include the following:

- claims

- benefit eligibility inquiries
- referral authorization requests
- other transactions for which HHS has established standards under the HIPAA Transactions Rule

Using electronic technology, such as email, does not mean a health care provider is a covered entity; the transmission must be in a standard transaction.

The Privacy Rule covers a health care provider whether it electronically transmits these transactions directly or uses a billing service or other third party to do so on its behalf. Health care providers include all "providers of services" (e.g., institutional providers such as hospitals) and "providers of medical or health services" (e.g., non-institutional providers such as physicians, dentists and other practitioners) as defined by Medicare, and any other person or organization that furnishes, bills, or is paid for health care.

2. Which of the following is considered a covered entity regardless of its size?

a. Health care plan
b. Health care insurance company
c. Health care clearinghouse
d. Health care provider

Electronic Protected Health Information

The HIPAA Privacy Rule protects the privacy of individually identifiable health information, called protected health information (PHI), as explained in the Privacy Rule.

The Security Rule protects the information covered by the Privacy Rule, which is all individually identifiable health information a covered entity creates, receives, maintains or transmits in electronic form. The Security Rule calls this information "electronic protected health information" (e-PHI). The Security Rule does **not** apply to PHI transmitted orally or in writing.

General Rules

The Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI.

Specifically, covered entities must:

- Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit.
- Identify and protect against reasonably anticipated threats to the security or integrity of the information.
- Protect against reasonably anticipated, impermissible uses or disclosures.
- Ensure compliance by their workforce.

3. Covered entities must ensure the confidentiality, integrity, and availability of all electronic protected health information (e-PHI) _____.

a. transmitted orally or in writing
b. they develop and distributed to customers
c. regulated by HIPAA and distributed
d. they create, receive, maintain, or transmit electronically

The Security Rule defines “confidentiality” to mean that e-PHI is not available or disclosed to unauthorized persons. The Security Rule's confidentiality requirements support the Privacy Rule's prohibitions against improper uses and disclosures of PHI.

Let’s look at a scenario about disclosing information to others inappropriately.

Scenario

Situation: Joan works in a cardiology practice. The physicians in the practice admit patients to a local hospital. Joan schedules a hospital admission for a friend, Nell, who attends the same church as Joan. At church the following Sunday, several members ask Joan if she knows anything about Nell’s condition. How should Joan respond?

Response: Joan must not disclose any information about Nell obtained because of her work in the cardiology practice, not even with Joan’s family or friends. Joan should politely inform the concerned church members that federal laws prohibit the sharing of confidential information about patients without their expressed permission.

4. The Security Rule defines "confidentiality" to mean that e-PHI is _____

a. withheld from external covered entities
b. not available or disclosed to unauthorized persons.
c. not disclosed to other health care professionals
d. prevented from being transmitted electronically

Integrity vs. Availability

The Security Rule also promotes the two additional goals of maintaining the integrity and availability of e-PHI. Under the Security Rule:

- "integrity" means e-PHI is not altered or destroyed in an unauthorized manner.
- "Availability" means e-PHI is accessible and usable on demand by an authorized person.

HHS recognizes covered entities range from the smallest provider to the largest, multi-state health plan. Therefore, the Security Rule is flexible and scalable to allow covered entities to analyze their own needs and implement solutions appropriate for their specific environments. What is appropriate for a covered entity will depend on the nature of the covered entity's business, as well as the covered entity's size and resources.

Therefore, when a covered entity is deciding which security measures to use, the Rule does not dictate those measures but requires the covered entity to consider:

- its size, complexity, and capabilities
- its technical, hardware, and software infrastructure
- the costs of security measures
- the likelihood and possible impact of potential risks to e-PHI

Covered entities must review and modify their security measures to continue protecting e-PHI in a changing environment.

5. Under the Security Rule, _____ means e-PHI is not altered or destroyed in an unauthorized manner.

a. portability
b. confidentiality
c. availability
d. integrity

Risk Analysis and Management

The Administrative Safeguards provisions in the HIPAA Security Rule require covered entities to perform a risk analysis as part of their security management processes.

A risk analysis process includes, but is not limited to, the following activities:

- Evaluating the likelihood and impact of potential risks to e-PHI.
- Implementing appropriate administrative, physical, and technical security measures to address the risks identified in the risk analysis.
- Documenting the chosen security measures and, where required, the rationale for adopting those measures.
- Maintaining continuous, reasonable, and appropriate security protections.

Risk analysis should be an ongoing process, in which a covered entity regularly reviews its records to track access to e-PHI and detect security incidents, periodically evaluates the effectiveness of security measures put in place, and regularly reevaluates potential risks to e-PHI.

6. As required by the HIPAA Security Rule, which of the following must be accomplished by a covered entity as part of their security management processes?

a. A safety inspection
b. A risk analysis
c. Formal reporting to OSHA
a. A phase hazard analysis

Safeguards

There are several administrative, physical, and technical safeguards that should be put into place to protect the security of e-PHI.

Administrative Safeguards: Here are a few examples of recommended administrative safeguards:

- **Security Management Process**: A covered entity must identify and analyze potential risks to e-PHI, and it must implement security measures that reduce risks and vulnerabilities to a reasonable and appropriate level.
- **Security Personnel**: A covered entity must designate a security official who is responsible for developing and implementing its security policies and procedures.
- **Information Access Management**: Consistent with the Privacy Rule standard limiting uses and disclosures of PHI to the "minimum necessary," the Security Rule requires a covered entity to implement policies and procedures for authorizing access to e-PHI only when such access is appropriate based on the user or recipient's role (role-based access).
- **Workforce Training and Management**: A covered entity must provide for appropriate authorization and supervision of workforce members who work with e-PHI. A covered entity must train all workforce members regarding its security policies and procedures, and must have and apply appropriate sanctions against workforce members who violate its policies and procedures.
- **Evaluation**: A covered entity must perform a periodic assessment of how well its security policies and procedures meet the requirements of the Security Rule.

Physical Safeguards: Here are examples of physical safeguards that can be implemented:

- **Facility Access and Control**: A covered entity must limit physical access to its facilities while ensuring that authorized access is allowed.
- **Workstation and Device Security**: A covered entity must implement policies and procedures to specify proper use of and access to workstations and electronic media. A covered entity also must have in place policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of electronic protected health information (e-PHI).

7. Which of the following is an example of an Administrative Safeguard to protect electronic protected health information (e-PHI)?

a. Designate a security official responsible for policies and procedures
b. Limit physical access to facilities to authorized persons only
c. Implement technical measures to guard against unauthorized access to e-PHI
d. Implement electronic measures to confirm e-PHI has not been improperly altered

Technical Safeguards. Here are examples of technical safeguards that can be implemented to protect e-PHI:

- **Access Control:** A covered entity must implement technical policies and procedures that allow only authorized persons to access electronic protected health information (e-PHI).

- **Audit Controls:** A covered entity must implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use e-PHI.

- **Integrity Controls:** A covered entity must implement policies and procedures to ensure that e-PHI is not improperly altered or destroyed. Electronic measures must be put in place to confirm that e-PHI has not been improperly altered or destroyed.

- **Transmission Security:** A covered entity must implement technical security measures that guard against unauthorized access to e-PHI that is being transmitted over an electronic network.

Organizational Requirements

If a covered entity knows of an activity or practice of the business associate that constitutes a material breach or violation of the business associate's obligation, the covered entity must take reasonable steps to cure the breach or end the violation. Violations include the failure to implement safeguards that reasonably and appropriately protect e-PHI.

8. Which of the following technical safeguards ensures e-PHI is not improperly altered or destroyed?

a. Access Controls
b. Audit Controls
c. Integrity Controls
d. Transmission Security

Policies, Procedures, and Documentation Requirements

HIPAA provisions require covered entities to develop and maintain policies, procedures, and documentation to comply with the Security Rule. A covered entity must:

- adopt reasonable and appropriate policies and procedures to comply with the provisions of the Security Rule.
- maintain written security policies and procedures and written records of required actions, activities or assessments.
- maintain written security policies, procedures, and records of required actions, activities or assessments for six years after the date of creation or last effective date, whichever is later.
- periodically review and update its documentation in response to environmental or organizational changes that affect the security of electronic protected health information (e-PHI).

9. How long must written security policies, procedures, and records of required actions, activities or assessments be maintained by covered entities?

a. A minimum of five years from date of creation
b. Six years after creation or last effective date
c. For the life of the original document
d. As long as the document has not been archived

State Law

In general, state laws contrary to the HIPAA regulations are pre-empted by the federal requirements, which means the federal requirements will apply. “Contrary” means it would be

impossible for a covered entity to comply with both the state and federal requirements, or the provision of state law is an obstacle to accomplishing the full purposes and objectives of the HIPAA provisions.

Enforcement and Penalties for Non-Compliance

If a covered entity's employees and/or volunteers do NOT follow the rules set out by HIPAA, the federal government has the right to do the following:

- conduct an investigation
- impose fines and/or jail sentences, if found guilty

Civil Penalties

Unintentional HIPAA violations could result in monetary penalties. Health and Human Services may not impose a civil money penalty under specific circumstances, such as when a violation is due to reasonable cause and did not involve willful neglect and the covered entity corrected the violation within 30 days of when it knew or should have known of the violation.

Criminal Penalties

Knowingly making unauthorized disclosure of PHI, intentionally selling information, and offenses that include false pretenses may result in substantial fines ($50,000 - $250,000) and/or imprisonment. The U.S. Department of Justice will enforce the criminal sanctions.

10. If a covered entity cannot comply with both HIPAA and federal requirements, the covered entity _____.

a. must comply with federal requirements
b. should comply with state requirements
c. must comply with the requirements that are more restrictive
d. may comply with either state or federal requirements

To review your questions, go online, answer the questions and on the last section, click on the "Check Quiz Answers" button, and follow the instructions.

Endnotes

1. Occupational Safety and Health Administration. (2014). HIPAA and OSHA: Whistleblower Complaints. Retrieved from: https://www.oshgov/Publications/OSHA-factsheet-HIPPA-whistle.pdf

2. U.S. Department of Health & Human Resources. (2014). HIPAA Privacy Rule: What Employers Need To Know. Retrieved from: http://www.twc.state.tx.us/news/efte/hipaa_basics.html

3. Government of Kansas. (2014). HIPAA Retrieved from: http://www.dcf.ks.gov/Agency/Documents/HIPAA-Training.pdf

4. U.S. Department of Health & Human Resources. (2006). Health Information Privacy. Retrieved from: http://www.hhs.gov/ocr/privacy/hipaa/faq/privacy_rule_general_topics/189.html

5. U.S. Department of Health & Human Resources. (2014). Summary of the HIPAA Privacy Rule. Retrieved from: http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf

6. U.S. Department of Health & Human Resources. (2014b). Health Information Privacy. Retrieved from: http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/

7. U.S. Department of Health & Human Resources. (2014c). Sharing Health Information With Family Members and Friends. Retrieved from: http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/sharing-family-friends.pdf

8. U.S. Department of Health & Human Resources. (2014d). A Health Care Provider's Guide to the HIPAA Privacy Rule. Retrieved from: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/provider_ffg.pdf