HIPAA Privacy Training

OSHAcademy™
Occupational Safety & Health Training

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

This page intentionally blank

Contents

This page intentionally blank

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.

Training Requirements

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)
- the company's business associates (including private sector vendors and third-party administrators)

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 all of its applicable requirements and should not rely on this summary as a source of legal information or advice.

After completing this course, you will have the knowledge of the following components:

- privacy and security rules
- protected healthcare identifiers (PHIs)
- wrongful disclosure of PHI
- personal rights under HIPAA
- protected information
- sharing health information
- how to file a HIPAA complaint
- covered entities
- electronic protected health information
- enforcement and penalties for non-compliance

Module 1: HIPAA Overview

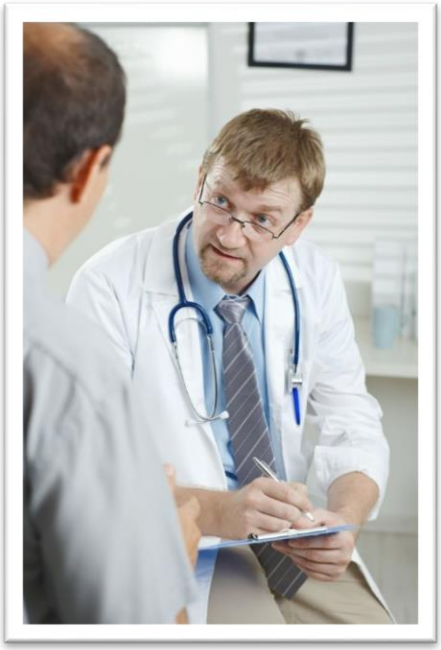
Privacy Rule

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.



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

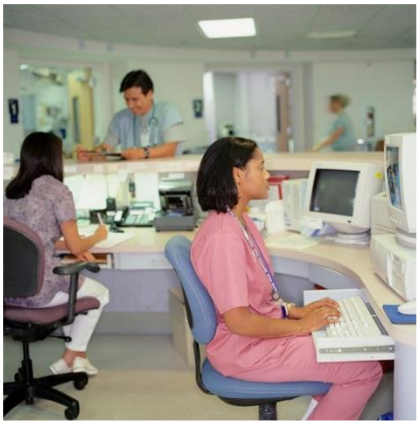
burden of complying with the requirements, the Privacy Rule gives needed flexibility for providers and plans to create their own privacy procedures, tailored to fit their size and needs.

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.

Security Rule

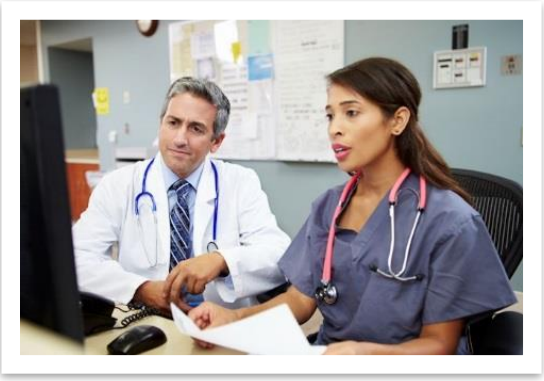
The Security Rule established a national set of security standards for protecting certain health information that is held or transferred in electronic form.

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 particular size, organizational structure, and risks to consumers' personal information.

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)

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), the majority of 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.

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

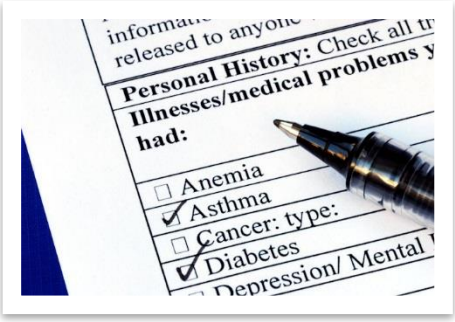
The HIPAA Privacy Rule says don't listen, tell, or show any client's PHI to anyone who does not have a legitimate right to see or hear that information.

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



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.

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 particular 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.

Scenario

Two doctors are eating lunch at a restaurant with many other patrons nearby. They are discussing a patient case that involves medical coverage and eligibility concerns. They are talking about confidential PHI regarding the patient. What should they do?

1. Ask one of the people nearby for an opinion on the case being discussed.
2. Stop talking about the case and move to a private location where their discussion cannot be overheard.
3. Announce they are talking about private information that contains PHI, so nearby patrons shouldn't listen.

The correct answer is: Move the discussion to a private location where it cannot be overheard.

Module 1 Quiz

Use this quiz to self-check your understanding of the module content. You can also go online and take this quiz within the module. The online quiz provides the correct answer once submitted.

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

2. **The _____ established a national set of security standards for protecting certain health information that is held or transferred in electronic form.**

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

3. **Which of the following are places where you might find confidential patient information?**

    a. financial records
    b. fax sheets
    c. social media sites
    d. both (a) and (b)

4. **Health information that contains at least _____ patient identifier is protected under HIPAA.**

    a. 1
    b. 5
    c. 10
    d. 15

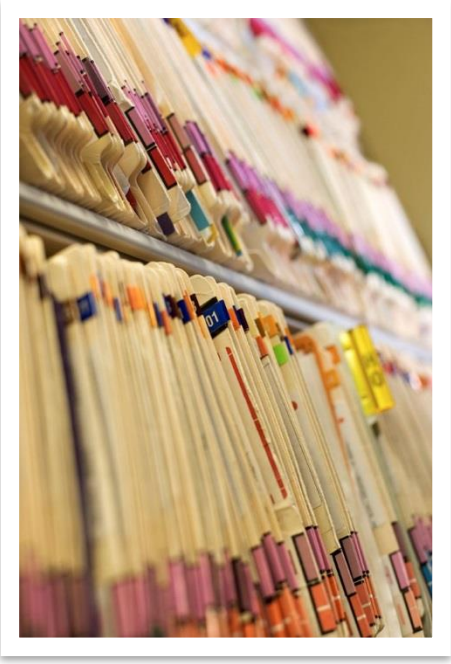
5. If you observe someone wrongfully disclosing PHI, what should you do FIRST?

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

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.

Individual Rights

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

1. Access to Information – A person can request and receive a copy of their 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 – A person may ask for their 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 – An individual may request a list of all the times their information was released improperly.

4. Notice of Privacy Practices – An individual has 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 HIPAA.

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.

Sharing Health Information

Under HIPAA, your health care provider may share your personal information face-to-face, over the phone, or in writing. 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.

HIPAA allows healthcare providers to give prescription drugs to any person you send to pick them up.

Examples

- An emergency room doctor may discuss your treatment in front of your friend when you ask your friend to come into the treatment room.
- Your hospital may discuss your bill with a family member or friend who is with you and has a question about the charges, if you do not object.
- Your doctor may discuss the drugs you need to take with your health aide who has come with you to your appointment.
- Your nurse may **not** discuss your condition with a family member or friend if you tell her not to.
- HIPAA also allows health care providers to give prescription drugs, medical supplies, x-rays, and other health care items to a family member, friend, or other person you send to pick them up.

A health care provider or health plan may also share relevant information if you are not around or cannot give permission when a health care provider or plan representative believes, based on professional judgment, that sharing the information is in your best interest.

For example, if you had emergency surgery and are still unconscious, your surgeon may tell your spouse about your condition, either in person or by phone, while you are unconscious.

Your doctor may discuss your drugs with your caregiver who calls your doctor with a question about the right dosage. However, a doctor may **not** tell your friend or family member about an unrelated past medical problem.

Communication & Patient Care

Even though HIPAA requires health care providers to protect patient privacy, providers are permitted, in most circumstances, to communicate with the patient's family, friends, or others involved in their care or payment for care.

Providing Information

If the patient is present and has the capacity to make health care decisions, a health care provider may discuss the patient's health information with a family member, friend, or other person if the patient agrees or, when given the opportunity, does not object. A health care provider also may share information with these persons if, using professional judgment, he or she decides the patient does not object. In either case, the health care provider may share or discuss only the information the person involved needs to know about the patient's care or payment for care.

Here are some examples:

- An emergency room doctor may discuss a patient's treatment in front of the patient's friend if the patient asks that her friend come into the treatment room.
- A doctor's office may discuss a patient's bill with the patient's adult daughter who is with the patient at the patient's medical appointment and has questions about the charges.
- A doctor may discuss the drugs a patient needs to take with the patient's health aide who has accompanied the patient to a medical appointment.
- A doctor may give information about a patient's mobility limitations to the patient's sister who is driving the patient home from the hospital.
- A nurse may discuss a patient's health status with the patient's brother if she informs the patient she is going to do so and the patient does not object. But, a nurse may NOT

a patient's condition with the patient's brother after the patient has stated she does not want her family to know about her condition.

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 as long as 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 particular 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.

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.

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 in the course of 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.

Module 2 Quiz

Use this quiz to self-check your understanding of the module content. You can also go online and take this quiz within the module. The online quiz provides the correct answer once submitted.

1. **Under HIPAA, your health care provider may NOT share your information in which of the following way?**

   a. face-to-face
   b. via telephone
   c. in a public place
   d. writing

2. **When can your health care provider give personal health information to your employer?**

   a. never
   b. only if you have authorized them to do so
   c. sometimes
   d. always

3. **If an employee believes he/she has been retaliated against for disclosing HIPAA-protected information, the worker can file a complaint with OSHA within _____ of the retaliation.**

   a. 20 days
   b. 30 days
   c. 50 days
   d. 60 days

4. **When can your health care provider or health plan share relevant information, if you are not around?**

   a. sharing the information is in your best interest
   b. when a family member gives consent
   c. they can only share it when you are unconscious
   d. both (a) and (c)

5. **When can a nurse tell a patient's friend about a past medical problem unrelated to the patient's current condition?**

    a. if they ask
    b. never
    c. always
    d. if they ask via email

Module 3: Health Care Provider Responsibilities

Covered Entities

Covered entities are defined in the HIPAA rules as the following:

- health plans
- health care clearinghouses
- health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards

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. Covered entities can be institutions, organizations, or persons. Let's take a closer look at each of the entities.

Health Care Plan

With certain exceptions, a health care plan is an individual or group plan which provides or pays the cost of medical care. The HIPAA law specifically includes many types of organizations and government programs as health plans.

Health Care Clearinghouse

A health care clearinghouse, which is either a public or private entity, is an organization that acts as a middleman between a provider and the entity that ultimately needs the information.

For example, when a hospital needs to get paid on an insurance claim, it must submit detailed medical information to the insurance company. When the hospital sends out this information, it goes through a health care clearinghouse so the information can be translated into a form that the insurance company can accept and understand.

Health Care Providers

Every health care provider, regardless of size, who electronically transmits health information in connection with 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 connection with 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.

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.

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 take a 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 as a result 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.

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 particular 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.

Risk Analysis and Management

The Administrative Safeguards provisions in the Security Rule require covered entities to perform risk analysis as part of their security management processes. The risk analysis and management provisions of the Security Rule are addressed separately here because, by helping to determine which security measures are reasonable and appropriate for a particular covered entity, risk analysis affects the implementation of all of the safeguards contained in the Security Rule.

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

- Evaluate the likelihood and impact of potential risks to e-PHI.
- Implement appropriate security measures to address the risks identified in the risk analysis.
- Document the chosen security measures and, where required, the rationale for adopting those measures.
- Maintain 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.

Administrative Safeguards

There are several administrative safeguards that should be put into place regarding e-PHI.

Here are a few examples of recommended safeguards:

- **Security Officer:** 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

A covered entity must limit physical access to its facilities while ensuring that authorized access is allowed. A covered entity must also implement policies and procedures to specify proper use of and access to workstations and electronic media.

A covered entity also must have policies and procedures in place regarding the transfer, removal, disposal, and re-use of electronic media. This will ensure the appropriate protection of e-PHI.

Scenario

An OB/GYN practice client ran into trouble when its receptionist recognized a woman from her neighborhood who came in for STD testing. The receptionist promptly posted a gleeful message on Facebook regarding the patient's medical issue after tracking down the test results, and common acquaintances on Facebook became privy to this confidential information. Improper access to patient information by office staff and dissemination of these details using social media are significant challenges that must be addressed.

The privacy rules created by HIPAA can seem cumbersome but every practice should evaluate its operations to make sure it is compliant.

Technical Safeguards

- **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.

Policies, Procedures, and Documentation Requirements

A covered entity must adopt reasonable and appropriate policies and procedures to comply with the provisions of the Security Rule. A covered entity must maintain written security policies and procedures and written records of required actions, activities or assessments.

These written security records must be maintained for six years after either the creation date or the last effective date, whichever is most recent.

NOTE: A covered entity must periodically review and update its documentation in response to environmental or organizational changes that affect the security of e-PHI.

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 Money Penalties

Unintentional HIPAA violations could result in:

- $100 fine per violation
- up to $25,000 for multiple violations of the same standard in a calendar year

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 may result in:

- $50,000 fine
- imprisonment of not more than one year
- both a fine and imprisonment

Offenses which include false pretenses may result in:

- $100,000 fine
- imprisonment of not more than 5 years
- both a fine and imprisonment

An offense with the intent to sell information may result in:

- $250,000 fine
- imprisonment of not more than 10 years
- both a fine and imprisonment

The U.S. Department of Justice will enforce the criminal sanctions.

Scenario

Hunter is 21 years old and receives medical assistance because he has AIDS. Adrian works at a local insurance agency in the billing department. At lunch one day, Adrian told a coworker, who has no involvement with the case, that Hunter has AIDS.

Which is the correct penalty for this violation?

1. $100 fine per violation, up to $25,000 for multiple violations of the same standard in a calendar year for unintentional offenses.
2. $50,000 fine, imprisonment of not more than one year, or both for knowingly making an unauthorized disclosure of PHI.
3. $100,000 fine, imprisonment of not more than 5 years, or both for offenses which include false pretenses.
4. $250,000 fine, imprisonment of not more than 10 years, or both for an offense with intent to sell information.

Answer: $50,000 fine, imprisonment of not more than one year, or both, for knowingly making an unauthorized disclosure of PHI. Adrian made a deliberate disclosure of PHI.

Module 3 Quiz

Use this quiz to self-check your understanding of the module content. You can also go online and take this quiz within the module. The online quiz provides the correct answer once submitted.

1. **A covered entity must designate a security officer. Which of the following is the responsibility of a security officer?**

   a. escorting workers to their car after their shift
   b. developing security policies and procedures
   c. protecting patients
   d. protecting workers from combative patients

2. **Covered entities can be which of the following?**

   a. government leaders
   b. organizations
   c. health care plans
   d. both (b) and (c)

3. **An offense with the intent to sell information may result in which of the following?**

   a. $250,000 fine
   b. $150,000 fine
   c. $100,000 fine
   d. $25,000 fine

4. **Unintentional HIPAA violations could result in which of the following?**

   a. $200 fine
   b. $100 fine per violation
   c. $50 fine per violation
   d. $500 fine

5. **Written security records must be maintained for ____ after the creation date or the last effective date.**

   a. 3 years
   b. 1 year
   c. 6 years
   d. 6 months

Endnotes

1. Occupational Safety and Health Administration. (2014). HIPAA and OSHA: Whistleblower Complaints. Retrieved from: https://www.osha.gov/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