PROTECTED HEALTH INFORMATION (PHI)

Slide 1.1 Welcome

Welcome to today's training. Today's topic is Protected Health Information, a part of the myLearningPointe library.

Slide 1.2 Course Instructions

When viewing this course, you will need to click the Next button on the bottom right of this course player at the end of each slide. To view the last slide watched, click Previous. The Pause and Play buttons are on the bottom to the left of the green Progress bar. The Progress bar also performs the fast forward and rewind functions. Click in the Progress bar to move back or forward in the current slide. You can also navigate the course using the menu outline on the left. You might find other information relevant to the course in the Resources tab located at the top. When viewing the final slide of this course, please let it play to its end.

Slide 1.3 Introduction

This course reviews regulations regarding Protected Health Information, or PHI, as it's commonly referred to. Persons with access to PHI must abide by laws, regulations and organizational policies designed to safeguard and protect individually identifiable health information. In this training we will define what PHI is and outline specific ways to maintain its confidentiality, in electronic, paper, and verbal forms.

A special note to viewer, this course gives an overview of handling Protected Health Information, it does not replace or supersede your organization's policies and procedures.

Slide 1.4 Course Objective

By the time you complete this course, you should be able to:

- Comprehend and adhere to state and federal laws regarding PHI
- Identify PHI in its many forms
- Identify the parameters needed to properly safeguard PHI
- Understand the potential impact of PHI violations
- Understand the role and responsibilities of the Chief Information Officer

This course will use the term Chief Information Officer. Your organization may designate this person by another title, such as Information Technology Director or Chief Privacy Officer. This is the person in your organization who is responsible for the computer and information technology systems and the protection of the PHI they contain.

Slide 2.1 Federal Law

Federal Law

Slide 2.2 Federal Law Overview

The three primary laws at the federal level that regulate the handling, storage and transmission of PHI are:

- The Health Insurance Portability and Accountability Act of 1996, also known as HIPAA
- The Health Information Technology for Economic and Clinical Health Act, also known as the HITECH Act which supplements the HIPAA regulations
- Title 42 of the Code of Federal Regulations, Part 2 which relates specifically to confidentiality of alcohol and drug abuse patient records

Slide 2.3 HIPAA

Protecting individual privacy has always been a practice among health-care providers and public health professionals in the United States, however, previous legal protections at the federal, tribal, state, and local levels were inconsistent and inadequate. To improve and safe-guard patient privacy, HIPAA was enacted by Congress.

One of the main reasons HIPAA was enacted is to prevent inappropriate use and disclosure of individuals' health information, and to require organizations that use health information to protect that information and the systems which store, transmit, and process it. The transition of medical records from paper to electronic formats has increased the potential for individuals to access, use, and disclose sensitive personal health information.

HIPAA Title II “Administrative Simplification” establishes standards for electronic healthcare records, security and privacy of healthcare records, and electronic exchange of health care information to improve health care.

Slide 2.4 HITECH Act

The Health Information Technology for Economic and Clinical Health Act, or HITECH Act is part of the American Recovery and Reinvestment Act of 2009, or ARRA.

The HITECH Act widens the scope of privacy and security protections available under HIPAA and increases the potential legal liability for non-compliance.

Click each button to see the Act's key provisions that relate to HIPAA and PHI:

Enforcement

Under HITECH, mandatory penalties are imposed for "willful neglect" to protect PHI. The government can apply civil penalties for willful neglect. Those penalties increase significantly for repeat or uncorrected violations.

Under the Act the U.S. Department of Health and Human Services, or HHS, is now required to conduct periodic audits of covered entities and business associates.

Notification of Breach

The HITECH Act imposes data breach notification requirements for unauthorized uses and disclosures of "unsecured PHI." The Act requires that patients be notified of any unsecured breach. If a breach impacts 500 patients or more HHS must also be notified. Notification will trigger posting the breaching entity's name on the HHS' website. Under certain conditions local media will also need to be notified.

Business Associates and Business Associate Agreements

The HITECH Act applies HIPAA provisions directly to business associates. Before the HITECH Act, privacy and security requirements were imposed on business associates via contractual agreements with covered entities. Under the HITECH Act, business associates are now directly responsible for compliance since they are required to comply with the safeguards contained in HIPAA.

Slide 2.5 Title 42 CFR, Part 2

Many in the mental health community are also bound by Title 42 of the Code of Federal Regulations, Part 2, referred to as 42 CFR 2, which enforces the confidentiality of alcohol and drug abuse patient records. 42 CFR 2, as it is referred to, states that records of any patient which are maintained in connection with the performance of any drug abuse prevention shall be confidential and be disclosed only in special circumstances. It also outlines the penalties and fines for violations.

Slide 2.6 Federal Law Summary

By law, employees must abide by privacy policies and procedures defined by HIPAA, the HITECH Act and 42 CFR 2. Each of these federal laws emphasizes the importance of maintaining confidentiality of PHI and carries penalties for any violations.

Slide 2.7 What is Privacy?

Privacy is the right of individuals to keep information about themselves from being disclosed; that is, people have the right to control access by others to their personal and private information.

Slide 2.8 Protected Health Information (PHI)

Protected Health Information or PHI is defined by the HIPAA Act as individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. In plain English, this is any health information no matter what its form – electronic, paper, oral, etc. This even includes health information transmitted in a casual conversation.

Individually identifiable health information is defined as a subset of health information which includes an individual's demographic information, information created or received by a healthcare provider, health plan, employer, etc. that relates to past, present, or future physical or mental health or condition of an individual. This information includes the provision of health care to an individual or payment for the provision of healthcare to an individual. In plain English, any information which could identify an individual or could reasonably be believed to identify an individual is considered individually identifiable health information.

Slide 2.9 PHI Examples

Examples of information which could identify an individual includes:

- Name
- Geographical subdivision smaller than a state, except for the first three digits of a zip code
- All dates, except for year including birth/death dates, admission/discharge dates, all years for those over 89 who can be grouped into a category "over 90"
- Phone or fax number
- E-mail address
- Social Security Number
- Medical record number
- Health plan beneficiary number
- Account number
- Certificate/license number
- Vehicle identifiers and serial numbers, including license plates
- Device identifiers and serial numbers
- Web URL
- IP address
- Biometric identifier, for example a finger print
- Full face photographic and any comparable image
- It also includes identifiable information of relatives, household members, and employers.

To be individually identifiable health information, it would also include information created or received by a healthcare provider, health plan, employer, etc. that relates to past, present, or future physical or mental health or condition of an individual.

A list of PHI may be found under the resources tab of this course. You may save and/or print this document for your use.

Slide 2.10 Storage of PHI

You may be wondering, how is protected health information stored? Facilities have systems in place to limit access to protected health information to only those who need such information in order to perform their individual role responsibilities. In other words, if you don't need a patient's PHI in order to do your job, then you shouldn't have access to see it, print it, etc.

PHI is stored in secure locations and/or systems which only allow authorized individuals with a need to know to handle this information. Electronic access usually requires a password, paper files are locked, and conversations are held out of the hearing of individuals who do not have a need to know.

All or parts of the PHI may be stored in several locations as well. For example, it may be in files created by a health insurance company to record health care claims. It may also be in records kept by the doctors from whom individual and family members receive care. Protected health information is on file with pharmacies for use with prescriptions.

Wherever protected health information is stored, it must be secured in accordance with HIPAA privacy regulations, including any reasonably anticipated impermissible uses or disclosures. An entity must also ensure that policies and procedures are in place and enforced for their workers.

Slide 2.11 Activity

Protected health information and individually identifiable health information have the exact same meaning. True/False

Slide 2.12 Activity

The primary federal laws enacted to ensure privacy of health information are: (select all that apply)

Health Insurance Portability and Accountability Act (HIPAA)

Health Information Technology for Economic and Clinical Health Act (HITECH)

Title 42 of the Code of Federal Regulations, Part 2 (42 CFR 2)

Family Medical Leave Act (FMLA)

The Affordable Care Act (ACA)

Health and Human Services Act (HHS)

Slide 3.1 Privacy and You

Privacy and You

Slide 3.2 Why Does Privacy Affect Me?

Federal law protects the privacy and security of client identifiable information, including health-related data and educational records.

If you have access to PHI you are bound by law to keep that information secure and private.

Slide 3.3 Why Comply?

Failure to protect the health information of clients would seriously damage your organization's good will and reputation and could result in assessment of monetary damages, fines and/or penalties.

To ensure all employees meet the standards in both federal and state laws, the Chief Information Officer of your organization institutes policies and procedures which conform to the compliance laws.

Slide 3.4 Why Should I Comply?

Usually, organization policies require that employees safeguard and preserve all information relating to patients or others under their care. This includes Protected Health Information.

Customarily the organization's policies specify that confidential information is to be used only as necessary for the employee to perform their duties and is not to be removed from the premises, unless necessary for the performance of their duties. Further most organizations also require that after termination of employment, the employee will not communicate or divulge any confidential information to any person, firm, or corporation.

Knowledge and compliance with your organization's privacy policies is a serious matter. Intentional misuse of PHI could further subject you to federal or state prosecution.

Slide 3.5 Activity

As a healthcare employee you should comply with the company Personal Health Information polices because: (check all that apply)

My organization is required to comply under federal and state laws.

I can be prosecuted on a federal and state level if I disclose PHI.

My organization could face fines if I don't comply.

Slide 4.1 Privacy Safeguards

Privacy safeguards

Slide 4.2 Privacy Rules of Thumb

When working with PHI some basic steps can be taken to ensure confidentiality. Click each numbered thumbprint to see the steps.

First, determine whether access to PHI is necessary to fulfill the job. If it's not needed, then don't use it and alert your supervisor that you are receiving information that is not necessary for you to perform your responsibilities.

Next, if access to protected information is needed, determine whether de-identified information can be used instead. De-identified information refers to PHI from which all terms that might permit someone to identify the subject of the PHI have been removed. If patient specific identifiers are not necessary, then don't use them.

Finally, if protected information is needed, make sure it is being used or disclosed for business operations only and is consistent with the organization's policies regarding PHI. When you no longer have a need for access to the PHI, verify your access has been removed and that all physical copies of documentation are appropriately deleted and/or destroyed.

Slide 4.3 Safeguards

Safeguards must be in place to protect confidential information from inappropriate use or disclosure. Examples of safeguards include:

- Passwords to systems
- Education on organization policies, procedures, state and federal laws
- Proper storage, handling, and destruction of paper containing PHI
- Restrictions on sharing PHI
- Reporting unusual activity to supervisors per your organization's guidelines

Slide 4.4 Passwords to Systems

Passwords are used to restrict and limit access to persons who have a need to know the information. Passwords should always be kept confidential. This means not sharing a password with anyone. It also means not exposing passwords accidentally by writing them down where they can be seen, emailing them to third parties or posting them to public websites. Remember, you're responsible for all system activity that is performed with your username and password.

Passwords are assigned for things like:

- Network access
- Application access
- Database access

Slide 4.5 Storage and Handling of Paper

PHI is sometimes maintained on paper, such as claims forms that are used for data entry, and is stored on site.

Any document that includes PHI must be stored and filed properly in a secure repository. If you have a need to view PHI, your supervisor should review with you each area where PHI is stored and complete instructions for proper handling.

As these processes are being identified, be aware to not leave protected information accessible or viewable. If you are working with PHI at your desk and an unauthorized person approaches your desk, you should cover or otherwise obscure the PHI.

Shred any documents that are no longer being used or dispose of them as your supervisor instructs you.

Slide 4.6 Restrictions on Verbally Sharing PHI

Employees should comply with the guidelines on the disclosure of PHI, both inside and outside the organization.

Employees should only discuss client health information with authorized employees or individuals that have a legitimate need to know. Employees should not discuss PHI with other employees or individuals that do not have a need to have this information.

Examples might include: Discussing client information with a neighbor or gossiping about clients with co-workers.

Slide 4.7 Verification

Employees that work with PHI must verify the identity of anyone requesting disclosure of confidential information before providing any such information and the requestor's authority to request and receive the PHI.

If anyone other than a person known to have current access requests PHI or if the circumstances under which the request is submitted are unusual or suspicious, employees should immediately refer the person to their direct supervisor.

Slide 4.8 Reporting to a Supervisor

Employees should report to their supervisor anything out of the ordinary or if they suspect that confidentiality is being violated or there is a potential for violation.

If you think or know that confidential information has been given out improperly, even by mistake, inform your immediate supervisor via e-mail, by telephone, or in person per your organization's guidelines.

Slide 4.9 Individual Rights

Individuals or their legal personal representative, may have the right to their PHI. These individuals should work directly with their state and/or their healthcare providers to exercise these rights. If you do not know the appropriate contact, refer the individual to your supervisor.

Slide 4.10 Activity

It is acceptable to provide client PHI to: (select all that apply)

Authorized representatives of the client

Authorized organization employees

Anyone with an organization email address

Slide 5.1 Client Data Handling and Storage

Client Data Handling and Storage

Slide 5.2 Overview

Client data is considered to be of the highest confidential nature, and each individual is responsible for the appropriate use and protection of this data. Each employee of the organization should fully comply with all provisions of federal law, including HIPAA requirements, the HITECH Act, 42 CFR 2, and accepted industry guidelines.

Slide 5.3 Who Does this Apply To?

This applies to confidential information of all current, former, and potential clients of the organization, received at or stored in all organization facilities and business units. Additionally, it applies to all organization information systems including all data and hardware, software, workstations, and storage systems regardless of media type. Lastly, it applies to all employees, consultants, contract workers, and subcontractors of the organization.

Slide 5.4 Communication

Your emails, text messages, voice messages or any other type of communications should not contain any client PHI. If such communications are received by you, your supervisor should be notified and the communication should be appropriately deleted or destroyed per organization policy.

Regarding email messages, it may be permissible to attach an encrypted file containing PHI to an email, but the PHI should never be included in text of the body of the message. The encrypted file password should never be included in the same email as the encrypted file. Please refer to your organization policies.

Slide 5.5 Reports and Printing

Reports or documents that incorporate or display PHI should only be created or printed as needed for authorized purposes. This includes both paper and electronic documents. Best practice is to send documents to the printer using the secure print option if you are using a shared printer. If you do not know how to use the secure or locked print function for your printer, please contact your Help Desk or IT support.

Printed material created under appropriate circumstances should be handled and subsequently disposed of under appropriate organization policy. Destruction is normally shredding of paper documents and secure electronic erasure of electronic documents. Destruction could also include burning, pulping, or pulverizing the media so that PHI is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed.

Slide 5.6 Encrypting Client Data

When it is determined that client data is required at another facility for a valid reason, the data should be encrypted with the appropriate utility for the particular application or database prior to transferring it to another facility.

Slide 5.7 Client Data Handling

Employees should never leave the facility with un-encrypted PHI.

Paper copies should be redacted to remove all personally identifiable information so that the information is illegible or should be shredded.

Employees should not use real PHI for training material without altering names and numbers, and other personally identifiable information sufficiently to prevent recognition of the individuals whose data has been used. No notes or other reproductions of the data or training materials, even if the PHI has been de-identified, should be produced or taken from the training room once the purpose is served.

Slide 5.8 Storage and Management of Client Data

No client data should be permitted on any offsite computer or mobile device, laptop, smart phone, or any other portable or offsite appliance, device, or media type except as allowed by organization policy.

Client data should be stored in designated locations, and only authorized employees should have access.

Slide 5.9 Technical Oversight and Permissions

Your management team should provide you technical support and guidance regarding PHI, as well as granting permissions for employee access to PHI. Refer to organization policies and procedures for special circumstances or conditions.

Slide 5.10 Access

Access to client data storage locations is granted on an as-needed basis and cleared in advance with the Chief Information Officer or their designee. Access should only be granted to those employees who have a need to know in order to perform their specific job responsibilities.

Slide 5.11 Training

All appropriate and authorized employees handling client data should be trained in the use of the encryption utility, security measures, and appropriate file transfer protocols.

Slide 5.12 Auditing

Most organizations perform periodic audits on stored data and appropriate organization information technology resources to insure that measures being taken to protect PHI are adequate and that those measures are compliant with the law.

Slide 5.13 Activity

Access to client PHI is granted: (Select all that apply)

Upon request to the IT department

For only as long as it is needed

To all employees of the organization

On a need-to-know basis

Slide 5.14 Activity

You are training new staff on your electronic health records (EHR) system. In addition to clinicians who would input the data, several of the administrative support personnel will be viewing the training so they can train clinicians who are out on vacation this week. For this training the best choice of data to use is:

Live client data

Scrambled client data

Test data

Slide 6.1 Incident Response

Incident Response

Slide 6.2 Incident Response Actions

Most organizations have an established incident response policy that defines a structure for security incident response handling related to client data located on internal systems and internal company data. The goal of these policies are to assure the confidentiality, integrity, and availability of PHI and for the operational integrity of organization's information systems.

All employees and contractors should report any possible or suspected security breach incidents that may come to their attention following your organizations process or procedure.

All incidents should be documented as soon as they are received. Any actions taken in response to a potential or suspected security incident should also be documented in a secured form. All original security incident documentation should be kept by the Information Security Incident Response Team.

If employees, contractors, or agents are suspected or believed to be acting contrary to legal requirement of organization policy, the circumstances should be promptly reported to the Chief Information Officer or their designee.

Slide 6.3 Activity

Possible or suspected security breaches should be reported _____.

By the end of the week

By the end of the work day

Immediately

When I have time

Slide 7.1 Conclusion

As a healthcare employee, you have a responsibility to keep the PHI of clients confidential. In order to do this, you must first recognize PHI, then know and abide by all of organization's privacy policies and procedures. When working on each task and in every conversation, employees should consider federal regulations and act responsibly to ensure that no laws are being broken and security is not being breached.

