Slide 1.1 Welcome

Welcome to today's training. Today's topic is HIPAA for Behavioral Health Professionals, 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. Please let each slide play to the end.

You can also navigate the course using the menu outline on the left. You will find the course script and other information relevant to the course by clicking the Resources tab located at the top.

When viewing the final slide of this course, please click the Exit Course button to proceed to the course assessment or click the Restart Course button to watch the course from the beginning. Prior to exiting to the assessment, you can review any slide or slides by clicking the slide in the menu outline on the left.

There may be some slides in the course that have an option to learn more by clicking a button, picture, or word. Clicking these elements take you to a sub-layer of the slide. You return to the main slide by clicking the red X in the corner.

Click the Next button to begin the course.

Slide 1.3 Overview

This course presents key information, highlighting Title II of the HIPAA law. The training incorporates updates to HIPAA required by additional legislation since 1996. This course is targeted to behavioral health professionals who are looking to gain an understanding of HIPAA and how this law relates to them either personally or how they must comply with it in their day-to-day operations. In this course, the words patient and consumer will be used interchangeably to refer to the person receiving services from the healthcare professional.

The goal of this course is to help those with exposure to protected health information (PHI) increase their awareness and knowledge of individual rights and responsibilities under HIPAA and to further improve the safe-guarding of health information.

Slide 1.4 Course Objectives

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

- Identify the reasons why HIPAA was enacted.
- Know consumers' rights under HIPAA.
- Identify various examples of protected health information.
- Know the requirements and safeguards for working with protected health information.
- Apply HIPAA rules appropriately (in various situations) to ensure a high level of care and respect for consumers.
- Understand HIPAA compliance and the penalties for not complying, as mandated by law.

Slide 2.1 HIPAA

This section gives you an overview of HIPAA and subsequent legislation affecting the Act.

Slide 2.2 HIPAA – The Act

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was passed to regulate a number of issues related to healthcare. The Act is divided in to five sections, called Titles.

- Title I – Health Insurance Reform: Addresses health insurance for workers and their dependents upon a job change, portability of health insurance coverage, and pre-existing conditions and health insurance.
- Title II – Administrative Simplification: Establishes standards for electronic healthcare records, security and privacy of healthcare records, and electronic exchange of healthcare information to improve healthcare.
- Title III – Tax Related Heath Provisions: Addresses deductions for medical insurance and changes to health insurance law.
- Title IV – Application and Enforcement of Group Health Plans Requirements: Addresses coverage of persons with pre-existing conditions and continuation of coverage for insureds.
- Title V – Revenue Offsets: Addresses company-owned life insurance, individuals who lose U.S. Citizenship for tax purposes, and financial institution interest allocation rules.

While you may find each of these titles fascinating, this course will focus on Title II, which addresses the privacy portion of the HIPAA Act.

Slide 2.3 HIPAA Rules

The Department of Health and Human Services (HHS) has issued a number of Rules that summarize the requirements of HIPAA. These rules are as follows:

- The Breach Notification Rule covers requirements for notification following the breach of unsecured protected health information.
- The Enforcement Rule covers requirements for compliance and penalties for non-compliance with HIPAA.
- The Privacy Rule covers requirements to protect individuals' medical records and other personal health information.
- The Security Rule covers what information is protected, who is covered, and required safeguards for information.
- The Transactions and Code Sets Rule covers standards for electronic data interchange (EDI) of healthcare data.
- The Unique Identifier Rule requires that the Employer Identification Number (EIN) issued by the Internal Revenue Service (IRS) be used to identify healthcare employers for standard transactions.

Again, this course focuses on only the Privacy, Security, and Enforcement Rules as they impact people who work in an environment where protected health information may be found.

Slide 2.4 Acts Modifying HIPAA

Since 1996, several additional acts and rules have modified the provisions of HIPAA. These are:

- The Health Information Technology for Economic and Clinical Health (HITECH) Act was included in the American Recovery and Reinvestment Act of 2009 (ARRA). The HITECH Act addresses Privacy, Security, Enforcement, and Breach Notification Rules.
- The Genetic Information Nondiscrimination Act of 2008 made additional changes to the Privacy Rule.
- Affordable Care Act of 2010 (ACA) had three goals: to make health insurance more affordable to more people, expand the Medicaid program, and to support innovative medical care delivery methods designed to lower the costs of healthcare. This Act included requiring the Department of Health and Human Services to issue operating rules for HIPAA's standard transactions.
- HHS released their Final Omnibus HIPAA Rule in January 2013 to clarify many of the modifications these Acts have made to the original HIPAA Act. This Omnibus HIPAA Rule required compliance by September 23, 2013.
- Medicare Access and Summary CHIP Reauthorization Act of 2015 or MACRA created the Quality Payment Program. Included in MACRA is the requirement that each participating organization perform the HIPAA Security Risk Analysis.
- Twenty-First Century Cures Act of 2016 addresses responses to opioid abuse, drug development, improving quality of care for consumers, Medicare savings, improvement of care for mental health and substance use disorder consumers. This act includes guidance for the compassionate communication of HIPAA information to the family, friends, and other involved in the care or payment for care of consumers with mental health or substance use disorders. In addition, this act addresses HIPAA and research, although we do not address specifics for research in this course.

Slide 2.5 Activity

Title ___ of the 1996 HIPAA is the section of the Act most relevant to you as a person with exposure to protected health information.

I. Health Insurance Reform
II. Administrative Simplification
III. Tax Related Heath Provisions
IV. Application and Enforcement of Group Health Plans Requirements
V. Revenue Offsets

2.6 Activity

HIPAA stands for:

Health Information Privacy, Administration, and Accountability Act

Health Insurance Portability and Accountability Act

Health Information Privacy and Accountability Act

3.1 Protected Health Information

Protected Health Information.

Slide 3.2 Protected Health Information Defined

Protected health information (PHI) is defined by HIPAA 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 regardless of its form – electronic, paper, oral, and so forth. 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 the condition of an individual. This information includes the provision of healthcare to an individual or payment for the provision of healthcare to an individual. Simply put, any information which could identify an individual or could reasonably be believed to identify an individual is considered individually identifiable health information.

Slide 3.3 PHI Examples

Examples of individually identifiable health information include:

- The consumer's name
- Geographical subdivision smaller than a state, except for the first three digits of a ZIP code
- All dates except year, including birth/death dates, admission/discharge dates, but all years for consumers over 89 years old (consumers 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 or 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
- Diagnosis
- Treatment plan

PHI also includes identifiable information of relatives, household members, and employers.

Slide 3.4 Storage of PHI

You may be wondering, how is protected health information stored? Organizations should have systems in place to limit protected health information access to only those who need the information to care for the consumer.

PHI is stored in secure locations and/or systems that allow only authorized individuals to view the 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.

PHI may be stored in several locations as well. For example, it may be in files created by a health insurance company to record healthcare claims. Then, it may also be in records kept by the doctors who provide care for the consumer. A consumer may also have protected health information on file with pharmacies for use with prescriptions.

Wherever protected health information is stored, it must be secured according to 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 3.5 Activity

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

True

False

3.6 Activity

After using Bob's full name in a conversation, two counselors in the cafeteria discuss his recent suicide attempt. This would/would not be considered protected health information.

4.1 Privacy Rule

The Privacy Rule is a subset of HIPAA.

Slide 4.2 Privacy Rule Protections

The Privacy Rule sets national standards to protect an individual's health information and allows the individual access to their information and how it is used.

The specific protections include:

- Giving consumers control of their health information
- Setting boundaries on how health information can be used
- Setting safeguards which must be used by entities who have access to the information
- Holding violators accountable – both entities and individuals
- Defining the balance between public responsibility and personal privacy in cases where information may be needed to protect public health
- Granting consumers the right to know how information is used and who it is released to
- Limiting the release of information to the minimum amount needed to treat the consumer
- Enabling consumer rights to review and receive a copy of their own health records, as well as the right to request corrections
- Enforcing consumers' rights to control use and release of their information

Slide 4.3 Psychotherapy Notes

While consumers have the right to review their health records, they do not have the right to review psychotherapy notes taken during conversations, whether in an individual or group session. These notes should be kept separate from all other medical and billing records of the consumer.

The Privacy Rule requires that a consumer give their authorization prior to releasing these notes for any reason, including to a health care provider other than the originator of the notes. “A notable exception exists for disclosures required by other law, such as for mandatory reporting of abuse, and mandatory ‘duty to warn’ situations regarding threats of serious and imminent harm made by the patient (State laws vary as to whether such a warning is mandatory or permissible).”

Psychotherapy notes do NOT include:

- Counseling session start and stop times,
- Functional status,
- Medication prescription and monitoring,
- Modalities and frequencies of treatment,
- Prognosis,
- Progress to date,
- Results of clinical tests,
- Summaries of diagnosis,
- Symptoms,
- Treatment plan, or
- Anything maintained in the client’s medical record.

Privacy Rule and Sharing Information Related to Mental Health”, HHS

Slide 4.4 Applicability of the Privacy Rule

The HIPAA Privacy Rule affects individuals, organizations, and agencies that both meet the definition of a covered entity and transmit health information in electronic form. These include health plans, healthcare providers, healthcare clearinghouses, and their business associates who have access to information.

Slide 4.5 Entity Requirements

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

- Notifying consumers 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 they understand the privacy procedures.
- Designating an individual to be responsible for ensuring that privacy procedures are adopted and followed.
- Securing consumer records that contain individually identifiable health information so the records are not readily available to those who do not need access to the information.

Slide 4.6 Personal Representative Exception

A consumer may designate a personal representative to act on their behalf in making healthcare related decisions. The personal representative has the same rights to view records and make decisions as the consumer.

Slide 4.7 Minors

In the case of an unemancipated minor, the parent, guardian, or other person acting in loco parentis would be the personal representative. While in most states, a minor reaches majority at age 18, the age of majority in Alabama, Delaware, and Nebraska is 19, and 21 in Mississippi. Further, Arkansas, Nevada, Ohio, Tennessee, Utah, and Wisconsin base the age of majority on graduation from high school.

In addition, minors are allowed to make certain healthcare decisions before they reach the age of majority. Primarily, these healthcare decisions are limited to specifically-aged minors, and the decisions relate to pregnancy, substance use disorder, and mental health.

Minors who live apart from their parent, guardian, or other person acting in loco parentis and who are supporting themselves financially, or minors who have married are also considered to be emancipated and can make their own healthcare decisions. Finally, if the parent, guardian, or other person acting in loco parentis is the perpetrator of criminal abuse or neglect, that person may not be the personal representative of the minor. You should become familiar with the laws of your state.

o parentis – A Latin term meaning "in [the] place of a parent" or "instead of a parent." Refers to the legal responsibility of some person or organization to perform some of the functions or responsibilities of a parent.

Reference: https://www.law.cornell.edu/wex/in_loco_parentis

Majority – The age of majority is the legally defined age at which a person is considered an adult, with all the attendant rights and responsibilities of adulthood.

Reference: https://definitions.uslegal.com/a/age-of-majority/

Minor – All states define an "age of majority," usually 18. Persons younger than this age are considered minors, and must be under the care of a parent or guardian unless they are emancipated. Minors are treated differently from adults for many legal purposes including privacy of official records, punishment in criminal matters, or the ownership or transfer of property.

Reference: https://www.law.cornell.edu/wex/minor

gal Dictionary," https://definitions.uslegal.com/

Slide 4.8 Mental Health Exception

The 21st Century Cures Act made it easier for providers to communicate information with family, friends, and other caregivers, even if that person has not been designated as a personal representative. The Act provides for this communication under two circumstances – mental health and substance use disorders.

"In recognition of the integral role that family and friends play in a patient's health care, the HIPAA Privacy Rule allows these routine – and often critical – communications between health care providers and these persons. Where a patient is present and has the capacity to make health care decisions, health care providers may communicate with a patient's family members, friends, or other persons the patient has involved in his or her health care or payment for care, so long as the patient does not object. See 45 CFR 164.510(b). The provider may ask the patient's permission to share relevant information with family members or others, may tell the patient he or she plans to discuss the information and give them an opportunity to agree or object, or may infer from the circumstances, using professional judgment, that the patient does not object. A common example of the latter would be situations in which a family member or friend is invited by the patient and present in the treatment room with the patient and the provider when a disclosure is made.

"Where a patient is not present or is incapacitated, a health care provider may share the patient's information with family, friends, or others involved in the patient's care or payment for care, as long as the health care provider determines, based on professional judgment, that doing so is in the best interests of the patient. Note that, when someone other than a friend or family member is involved, the health care provider must be reasonably sure that the patient asked the person to be involved in his or her care or payment for care.

"In all cases, disclosures to family members, friends, or other persons involved in the patient's care or payment for care are to be limited to only the protected health information directly relevant to the person's involvement in the patient's care or payment for care."

Privacy Rule and Sharing Information Related to Mental Health"

Slide 4.9 Substance Misuse Exception

Further, in response to the opioid crisis, HIPAA allows healthcare professional to disclose some health information without a patient's consent under certain circumstances. Click each XXX for specific situations.

ng health information with family and close friends who are involved in care of the patient if the provider determines that doing so is in the best interests of an incapacitated or unconscious patient and the information shared is directly related to the family or friend's involvement in the patient's health care or payment of care. For example, a provider may use professional judgment to talk to the parents of someone incapacitated by an opioid overdose about the overdose and related medical information, but generally could not share medical information unrelated to the overdose without permission."

ming persons in a position to prevent or lessen a serious and imminent threat to a patient's health or safety. For example, a doctor whose patient has overdosed on opioids is presumed to have complied with HIPAA if the doctor informs family, friends, or caregivers of the opioid abuse after determining, based on the facts and circumstances, that the patient poses a serious and imminent threat to his or her health through continued opioid abuse upon discharge."

respects individual autonomy by placing certain limitations on sharing health information with family members, friends, and others without the patient's agreement.

"For patients with decision-making capacity: A health care provider must give a patient the opportunity to agree or object to sharing health information with family, friends, and others involved in the individual's care or payment for care. The provider is not permitted to share health information about patients who currently have the capacity to make their own health care decisions, and object to sharing the information (generally or with respect to specific people), unless there is a serious and imminent threat of harm to health as described above."

anticipates that a patient's decision-making capacity may change during the course of treatment.

"Decision-making incapacity may be temporary and situational, and does not have to rise to the level where another decision maker has been or will be appointed by law. If a patient regains the capacity to make health care decisions, the provider must offer the patient the opportunity to agree or object before any additional sharing of health information."

IPAA Allows Doctors to Respond to the Opioid Crisis"

Slide 4.10 Other Providers, Case Management, and Care Coordination

"A health care provider may disclose a patient's PHI for treatment purposes without having to obtain the authorization of the individual. Treatment includes the coordination or management of health care by a health care provider with a third party. Health care means care, services, or supplies related to the health of an individual. Thus, health care providers who believe that disclosures to certain social service entities are a necessary component of, or may help further, the individual's health or mental health care may disclose the minimum necessary PHI to such entities without the individual's authorization. For example, a provider may disclose PHI about a patient needing mental health care supportive housing to a service agency that arranges such services for individuals.

"A covered entity may also disclose PHI to such entities pursuant to an authorization signed by the individual. HIPAA permits authorizations that refer to a class of persons who may receive or use the PHI. Thus, providers could in one authorization identify a broad range of social services entities that may receive the PHI if the individual agrees. For example, an authorization could indicate that PHI will be disclosed to 'social services providers' for purposes of 'supportive housing, public benefits, counseling, and job readiness.'"
ional FAQs on Sharing Information Related to Treatment for Mental Health or Substance Use Disorder—Including Opioid Abuse"

Slide 4.11 Research

The 21st Century Cures Act also allows some HIPAA information to be made available for research. If you are involved in a research project, you should obtain additional information about allowable exceptions from the Health and Human Services Department's Health Information Privacy page. Click the button to access the site.

RLINK "https://www.hhs.gov/hipaa/index.html" https://www.hhs.gov/hipaa/index.html

Slide 4.12 Activity

The Privacy Rule is _____ HIPAA.

Options for

Different than

A subset of

More important than

4.13 Activity

Privacy Rule activities include: (select all that apply)

Notifying consumers 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.

Designating an individual to be responsible for ensuring that privacy procedures are adopted and followed.

Securing consumer records that contain individually identifiable health information so that they are not readily available to those who do not need access to the information.

4.14 Activity

Select the statements which are true about psychotherapy notes.

May not be released without client consent, no exceptions

Are required to be released to the client

Are not required to be released to the client

May not be released without client consent, except in the case of mandatory child abuse and neglect reporting

May not be released without client consent, except in the case of mandatory “duty to warn”

5.1 Scenarios for Critical Thinking

The following slides present some scenarios for you to consider. Before you move on to the answer slide, take a minute to type your answer to each situation. Compare your answer to the suggested answer. Keep in mind, there are multiple correct answers and not all possible answers are listed on the answer slide.

Slide 5.2 Scenario 1

As a behavioral health professional working in a residential facility, you are making rounds with Dr. Smith.

Mrs. Jones tells the doctor that she did not rest well the previous night because the patient next door was yelling all night long, and she asks, “What’s his problem?”

You reply, “He is going through alcohol withdrawal and that can make him pretty restless.”

Question

Provide a response as to how this situation could have been handled appropriately.

Slide 5.3 Scenario 1 Solutions

Confidentiality concerning the patient next door was betrayed. A more appropriate response would be to simply state, "I'm sorry the patient next door kept you awake last night. He is not feeling well, and we are doing our best to make him better."

Slide 5.4 Scenario 2

You are an employee at St. John's Hospital. While on your lunch break in the cafeteria, your co-worker, Jean, joins you and begins talking about Mr. Williams, a patient who was admitted during the night shift. Jean shares with you that Mr. Williams is HIV positive and that none of his children are aware of his diagnosis.

You are not aware that Mrs. Williams and three ladies are having lunch at a table not far from you. Mrs. Williams recognizes Jean as her husband's nurse, approaches your table, and begins small talk. Mrs. Williams asks Jean if she has given medications to her husband. Jean answers Mrs. Williams by stating that she gave all but the medication for his HIV and she'll give it to him as soon as the pharmacy makes it available. The ladies accompanying Mrs. Williams are her daughters and they become highly emotional after learning their dad is taking HIV medication.

Question

How could you have prevented this scene?

Slide 5.5 Scenario 2 Solutions

When in public places, avoid all conversations related to patients.

If a family member approaches you, give as little information as possible until you are in a private area and have the permission of the patient or the patient representative.

Slide 5.6 Scenario 3

You are a licensed educational psychologist at a boarding school in California. The age of consent for mental health treatment in California is 12 years of age or older if, "(1) The minor, in the opinion of the attending professional person, is mature enough to participate intelligently in the outpatient services or residential shelter services." and "(2) The minor (A) would present a danger of serious physical or mental harm to self or to others without the mental health treatment or counseling or residential shelter services, or (B) is the alleged victim of incest or child abuse." Your services are included in the tuition cost and there is no extra charge to the students' parents.

A sixth-grade student, aged 12, comes into your office talking about having feelings of wanting to hurt herself, but you confirm she has not done any harm yet. The student will be at school for the next month and does not give consent for you to call her parents. You suspect there may be some abuse when the student is at home.

Question

What should you do?

Slide 5.7 Scenario 3 Solutions

You can respect the child's request not to call the parents at this time, as you feel you need additional time to evaluate if there is abuse in the home environment and the child is in a safe environment for the next month.

Slide 5.8 Scenario 4

You work in the emergency room as a clinical psychologist and the son of the state governor was just admitted for a possible psychotic break in public.

The emergency room receives multiple calls regarding his condition and the news media arrives at the hospital demanding information. A nurse, Inez, is approached by news media and she tells them what symptoms he is exhibiting and that he will be transferred to the psychiatric unit for further observation. Media requests continue regarding his condition

After work, coverage is on the evening news. You are knowledgeable about the governor's son's condition and give firsthand information to your family, including his symptoms, medications, and prognosis.

Question

How should you respond to special situations such as a public personality?

Slide 5.9 Scenario 4 Solution

Usually, reports regarding public officials and celebrities are referred to the hospital's office of public relations.

No information should be shared with anyone, regardless of their status.

Slide 5.10 Scenario 5

Shannon discovered her 23-year-old son, Jack, unresponsive in his bedroom in their home. She called the ambulance and is now at the emergency room of the hospital. Jack is delirious as a result of using opioids. The doctor has asked you, as the social worker on staff, to talk to Shannon about Jack's condition and to ask her for permission for treatment.

Question

Under the HIPAA Privacy Rule, are you allowed to talk to Shannon about Jack's condition and treatment?

Slide 5.11 Scenario 5 Solution

Under the clarifications provided by the 21st Century Cures Act, a doctor, nurse, or social worker may discuss protected health information with a patient's family, friends, or other caregiver if the patient is disoriented, delirious, unaware of their surroundings, or in some other way lacks capacity to make their own healthcare decisions. Once the patient has the capacity to make their own decisions, the patient must give permission or not object to their protected health information being discussed with others.

Slide 5.12 Scenario 6

You are a family therapist. You just concluded a session with Jenny where she disclosed she has had thoughts of harming herself with a gun. The gun belongs to Mark, her husband.

Question

As Jenny's therapist, are you allowed to speak to Mark about Jenny's thoughts and your concern about the availability of the gun?

Slide 5.13 Scenario 6 Solution

As Jenny's therapist, if you believe in your professional opinion that Jenny is at risk of harming herself or others, you have a duty to warn anyone who may be able to prevent that harm. This warning should be done in the narrowest possible way to both prevent harm and protect her information. In this case, as the owner of the gun, Mark is in the best position to remove the gun to a safer location. In addition, as her spouse, Mark should be aware of signs that she may harm herself so he can get her additional help. HIPAA allows this type of communication.

Slide 6.1 Compliance

Compliance is not only abiding by the rules, but also being able to prove it.

Slide 6.2 Compliance Requirements

The requirements outlined by the law and the regulations made known by the U.S. Department of Health and Human Services are far-reaching.

Healthcare organizations that maintain or transmit electronic health information must comply with HIPAA. This includes health plans, healthcare clearinghouses, and healthcare providers who submit claims electronically. Business associates of any of these organizations who also have access to PHI also must conform to the regulations.

For example, if you submit claims electronically, make referrals, or obtain authorizations by sending e-mail messages that contain individually identifiable health information, you are a covered entity and you must comply with HIPAA.

If your practice is paper based, don't automatically assume you're exempt from the regulation. For example, if you submit hard copies of claims to your billing company and it transmits them electronically to payers, the HIPAA rule applies to you.

Your organization will have policies and procedures regarding HIPAA. Compliance means that you and your organization not only follow the rules, but may also require you document that you have followed the rules to prove compliance.

Slide 6.3 Rules and Regulation Development

Click each arrow proceeding number below to learn the step-by-step process on how HIPAA rules and regulations are made.

1. HHS proposes a rule.
2. The rule is approved from within the government.
3. The public is given the opportunity to comment on the proposed rule.
4. Public comments are analyzed and considered in the development of the final rule.
5. The final rule is issued by HHS and has the force of federal law.

Slide 6.4 Enforcement

The Office for Civil Rights (OCR), the law-enforcement agency for HHS, oversees compliance of HIPAA and other civil rights laws. To promote and ensure compliance with civil rights laws, the OCR:

- Investigates complaints filed by individuals,
- Conducts compliance reviews of covered entities,
- Provides technical assistance to entities to help them into compliance, and
- Conducts outreach to help entities and individuals understand the civil rights laws that apply to recipients of federal financial assistance from HHS.

The OCR also works in conjunction with the Department of Justice (DOJ) to refer possible criminal violations of HIPAA.

Slide 6.5 Civil Penalties

There are four tiers of penalties for non-compliance with HIPAA. These penalties were significantly increased with the updates to HIPAA instituted by the 2013 Omnibus Rule. The table below summarizes the current penalties.

Violation Circumstance	Minimum per violation	Maximum per violation	Maximum for identical violations in a calendar year (1/1 – 12/31)
Tier A: Violation in which it is established that the covered entity or business associate did not know, and by exercising reasonable diligence, would not have known that the covered entity or business associate violated such provision.	$100	$50,000	$1,500,000
Tier B: Violation in which it is established that the violation was due to reasonable cause and not to willful neglect.	$1,000	$50,000	$1,500,000
Tier C: Violation in which it is established that the violation was due to willful neglect and was corrected during the 30-day period beginning on the first date the covered entity or business associate liable for the penalty knew, or by exercising reasonable diligence, would have known that the violation occurred.	$10,000	$50,000	$1,500,000
Tier D: Violation in which it is established that the violation was due to willful neglect and was not corrected during the 30-day period beginning on the first date the covered entity or business associate liable for the penalty knew, or by exercising reasonable diligence, would have known that the violation occurred.	—	$50,000	$1,500,000

The OCR does have some discretion in the amount of the penalty levied and each entity has the right to a hearing.

Slide 6.6 Criminal Penalties

The U.S. Code also provides for criminal penalties for a "person who knowingly and in violation of this part – (1) uses or causes to be used a unique health identifier; (2) obtains individually identifiable health information relating to an individual; or (3) discloses identifiable health information to another person..."

Violation Circumstance	Maximum Fine	Maximum Imprisonment
General	$50,000	1 year
Committed under false pretenses	$100,000	5 years
Committed with the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm	$250,000	10 years

This means you could be subject to penalties personally in addition to your employer.

Slide 6.7 Self-Reporting

Reporting a HIPAA violation is a strain on the organization given the costs of notice, time and effort responding to government investigations, and potential penalties, but the consequences for failure to report a known breach are likely worse. If discovered, such a failure would likely constitute willful neglect, thereby subjecting the covered entity or business associate to the mandatory civil penalties.

Given the increased penalties, lowered breach notification standards, and expanded enforcement, it is more important than ever for entities to comply with the regulations. At the very least, an organization should document good faith efforts to comply with the regulations to avoid a charge of willful neglect, mandatory penalties, and civil lawsuits.

Slide 6.8 Activity

Which statement is NOT true?

The maximum amount an entity can be fined for like violations in a calendar year is $1,500,000.

It is better to face the possibility of a fine by self-reporting rather than trying to hide non-compliance.

The maximum amount of prison time for a person found to have intentionally violated individually identifiable health information is ten years.

Only electronic and paper protected health information must be guarded from exposure to those who do not need to know.

7.1 HIPAA and Digital Security

HIPAA and Digital Security.

Slide 7.2 Breach Headlines

The HIPAA Journal reported the following compromises of digital PHI in a one-week period. (https://www.hipaajournal.com/category/hipaa-breach-news/) The reports listed for the week included phishing, ransomware, and unauthorized access. Click the headline to see a brief summary of the HIPAA Journal article.

ional Research Hospital … Discover PHI Compromised in Phishing Attacks"

> An email account was compromised in a phishing attack. The Breach contained information of current and former patients and employees. Information included dates of birth, Social Security numbers, driver's license numbers, employer ID numbers, health insurance information, disability codes, birth certificate information, marriage certificate information, passport information, banking and other financial information, medical record numbers, usernames and passwords, Medicare/Medicaid ID numbers, diagnosis and treatment information, and billing/claims information.
>
> https://www.hipaajournal.com/boys-town-national-research-hospital-northstar-anesthesia-phishing-attacks/

somware Attack Impacts 44,600 Patients"

> Ransomware was downloaded to a server containing the PHI of patients. According to the press release, "All client patient information must assume [sic] to be compromised."
>
> https://www.hipaajournal.com/golden-heart-administrative-professionals-ransomware-attack-impacts-44600-patients/

sician Notifies Patients of Exposure of their PHI"

> A physician's computer was accessed by an unauthorized individual during a three-week period from late 2017 to early 2018. Any individual who accessed the physician's computer could have gained access to the EMR [Electronic Medical Record] system. Information that may have been viewed and/or copied included names, addresses, birthdates, medical histories, diagnoses, treatment information, lab test results, medications, health insurance details, claims information, Medicare ID numbers, and Social Security numbers.
>
> https://www.hipaajournal.com/new-york-physician-notifies-patients-of-exposure-of-their-phi/

tigation Launched Over Snapchat Photo Sharing at …. Continuing Care Center"

> Certain employees of a nursing home used their smartphones to take photographs and video of at least one patient and shared these images and videos with others on Snapchat – a violation of HIPAA and serious violation of patient privacy.
>
> https://www.hipaajournal.com/investigation-launched-over-snapchat-photo-sharing-at-m-m-ewing-continuing-care-center/

al Email Accounts Compromised in … Phishing Attacks"

> Two more healthcare organizations reported phishing attacks that have resulted in cybercriminals gaining access to the protected health information of patients, both of which saw the attackers gain access to multiple email accounts.

https://www.hipaajournal.com/several-email-accounts-compromised-in-sunspire-health-and-upmc-cole-phishing-attacks/

Slide 7.3 Phishing

What is phishing? Phishing is a form of a cyber-attack where an individual is sent an email appearing to be from a trustworthy sender, but actually is sent by a person attempting to acquire log-in credentials and other personal information, or to install malware on a computer. This is a common way for criminals to gain access to protected health information. These emails often look to be from a friend or coworker with a link to click, from a financial institution asking you to provide security information, or from vendors or ecommerce sites requesting you click a link or download an attachment. If you receive any email, even from a trusted source, that is not typical of the correspondence you have with the emailer, do not click links, download attachments, or supply information until you have verified the email is legitimate.

Slide 7.4 Ransomware

What is ransomware? Ransomware is a specific type of malware which either denies a legitimate user access to data or threatens to distribute sensitive data publicly unless a ransom is paid. While your information security staff should have ransomware prevention measures in place on your computers and network, you can help prevent this by not clicking links or downloading software from questionable sources.

Slide 7.5 Inappropriate Use of Mobile Devices

Your organization should have policies and procedures in place for using mobile devices, such as smartphones or tablets, to access protected health information. The same is true for accessing your organization's network remotely. Do not violate these policies and procedures, as doing so may permit unauthorized access to consumer data.

Slide 7.6 One You May Not Have Thought About

You may not have thought about the digital printer or copier. These are multifunction machines which have a storage device and programs to allow the machine to function. Most of these machines have a secure or encrypted mode which encrypts the document sent to the printer, then requires a login at the machine to print the document. When printing, scanning, faxing, or emailing documents containing consumer PHI, use the encryption and secure print functions of the machine. Your information security team should have policies and procedures to permanently delete data from the machines' internal drives on a routine basis.

Slide 7.7 Digital Security Summary

It is critical that each individual with access to protected health information be aware of the threat to that information by people with malicious intent. Your organization should supply you with the relevant policies and procedures for your digital environment. Your vigilance and adherence to procedures will help keep the data safe.

Slide 7.8 Activity

Phishing is a form of a cyber-attack where an individual is sent an email appearing to be from a trustworthy sender, but actually is sent by a person attempting to acquire log-in credentials and other personal information, or to install malware on a computer.

True

False

7.9 Activity

The purpose of ransomware is to: (Select all that apply)

Deny a legitimate user access to data

Distribute sensitive data publicly

Pay a ransom to a cyber-criminal

Secure data on a mobile device

8.1 Conclusion

Conclusion

Slide 8.2 Summary

HIPAA is a multi-faceted federal law that addresses health information privacy. Since its passage in 1996, many are still learning just how comprehensive this law really is. HIPAA continues to serve as a protection for all individually identifiable or protected health information that is either maintained or transferred by a covered entity. It is your continued responsibility to uphold HIPAA law and regulations as they have been set forth. If you know of or witness cases where HIPAA is being violated, it is also your responsibility to report these violations to the proper authorities to ensure that corrective measures are taken and, in some cases, justice is served.

Slide 8.3 Objectives Recap

You should now be able to:

- Identify reasons why HIPAA was enacted.
- Know consumers' rights under HIPAA.
- Identify various examples of protected health information.
- Know the requirements and safeguards for working with protected health information.
- Apply HIPAA rules appropriately (in various situations), thus ensuring a high level of care and respect for consumers.
- Understand HIPAA compliance and the penalties for not complying, as mandated by law.

Slide 8.4 Exit or Review

Please click the Exit Course button to proceed to the course assessment or click the Restart Course button to watch the course from the beginning. Prior to exiting to the assessment, you can review any slide or slides by clicking the slide in the menu outline on the left.

