

## 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. 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 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.

The goal of this course is to help Behavioral Health Professionals 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 reasons why HIPAA was enacted
- Know 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 patients
- 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 health care. The Act is divided into 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 health care information to improve health care.

**Title III Tax Related Health 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 and every one 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 which summarize the requirements of HIPAA. These rules are:

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

Again, while fascinating reading, this course will focus on the Privacy, Security, and Enforcement Rules which may have an impact on your duties as a Behavioral Health Professional.

### Slide 2.4 Acts Modifying HIPAA

Since 1996 a number of 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.
- 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 required compliance by September 23, 2013.

### Slide 2.5 Activity

Title \_\_\_ of the 1996 HIPAA is the section of the Act most relevant to you as a Behavioral Health Professional.

Options

I Health Insurance Reform

II Administrative Simplification

III Tax Related Health Provisions

IV Application and Enforcement of Group Health Plans Requirements

V Revenue Offsets

### Slide 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

## Slide 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 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. 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 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 (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.

### Slide 3.4 Storage of PHI

You may be wondering, how is protected health information stored? Organizations should have systems in place to limit access to protected health information based on who needs it to care for the patient.

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

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 employees 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 3.5 Activity

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

True/False

### Slide 3.6 Activity

After using Bob's full name in a conversation, two clinic workers in the cafeteria discuss coding his charges for billing. This cafeteria discussion would/would not be considered protected health information.

### Slide 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:

- Patients controlling 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, which may be needed to protect public health
- Patient rights to knowing how information is used and who it is released to
- Limits releasing of information to the minimum information need
- Patient rights to reviewing and receiving a copy of their own health records
  - And the right to request corrections
- Patient rights to controlling uses and release of their information

### Slide 4.3 Psychotherapy Notes

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

The Privacy Rule requires that a client 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).” (“HIPAA Privacy Rule and Sharing Information Related to Mental Health”, HHS)

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

### Slide 4.4 Talking with Family or Friends

There are three types of clients for purposes of relaying information to family or friends: adults, incompetent persons, and minors.

#### **Adults**

Mental health information may be shared with family, friends, or others involved in the client's care, if the client does not object. Information should be limited to what the person "needs to know about the patient's care or payment for the care." (HIPAA Privacy Rule and Sharing Information Related to Mental Health", US Department of Health and Human Services) The professional may share information about medication requirements, usage, and warning signs of improper usage if the professional feels there is an imminent threat or harm to the patient and it is in the best interest of the patient.

#### **Incompetent Persons**

If a person is unconscious or if in the judgment of a health care provider the person does not have the capacity to agree or object to information being shared at that time, if the professional believes it is in the best interest of the client, they may share information with family, friends, or others involved in the patient's care. Once the person has the capacity to object or agree, their consent must be obtained. Additionally, the same rules would apply as to any other adult as noted earlier.

#### **Minors**

The area of minors is a bit trickier and is more dependent the State's definitions of a minor's rights regarding their health care. Depending on the State and the age of the minor, they may have the same rights as adults or may be considered as incompetent persons. Minors as young as 12 years may have the right to consent. If a State does not define a specific age for a minor to make their own determinations regarding their health care, the age is 18.

The National District Attorneys Association has published a document "Minor Consent to Medical Treatment Laws" which can be accessed via the web to view state laws, including those for mental health treatment.

*Programming note: Make a note that the information on this slide is from "HIPAA Privacy Rule and Sharing Information Related to Mental Health", US Department of Health and Human Resources*

### Slide 4.5 Applicability of the Privacy Rule

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



### Slide 4.6 Entity Requirements

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

- Notifying 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.
- Designating an individual to be responsible for seeing that the privacy procedures are adopted and followed.
- Securing patient records containing individually identifiable health information so that they are not readily available to those who do not need them.

### Slide 4.7 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”

### Slide 4.8 Activity

Privacy Rule activities include: (select all that apply)

Notifying 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.

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

Securing patient records containing individually identifiable health information so that they are not readily available to those who do not need them.

## Slide 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 jot down your answer(s) to each situation. Compare your answer to the suggested answer. Keep in mind, there are multiple right 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 Answer

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 that 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 his 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 will be no extra charge to the parents.

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

#### Question

What should you do?

### Slide 5.7 Scenario 3 Solution

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 rooms have received 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 continued 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 6.1 Compliance

Compliance only abiding by the rules and 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.

Health care organizations that maintain or transmit electronic health information must comply with HIPAA. This includes health plans, health care 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 you have followed the rules so they can prove compliance.

## Slide 6.3 Rules/Regulation Development

Click each arrow proceeding number below to learn the step-by-step process on how HIPAA Rules/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 rules 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 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: 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 US 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	\$250,00	10 years

This means you personally could be subject to penalties, not just your employer.

## Slide 6.7 Self-Reporting

Reporting a HIPAA violation is bad enough given the costs of notice, 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.

## Slide 7.1 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.