The Health Insurance Portability and Accountability Act (HIPAA) - 2014

Introduction

Case Study 1

Bob Brent, a truck driver is called into his Human Resources office. He receives a pink slip, stating that after contacting his health insurance company, his employer had discovered that he had sought treatment drinking for a problem five years previously. The detailed records also stated that he had relapsed several times. Bob argues, to no avail, that he has been sober for 3 years.

Case Study 2

Barbara is a 55-year-old woman with chronic depression who has been seeing Dr. Hart in weekly therapy for the past year. Dr. Hart has seen some improvement in Barbara’s symptoms, but as much of her depression is related to childhood issues and has been longstanding, Dr. Hart has continued to see Barbara weekly. Barbara’s husband has recently changed jobs, and Dr. Hart is now billing her new healthcare plan. Dr. Hart receives an explanation of benefits denying coverage for Barbara’s treatment and with the explanation code “preexisting condition.” Distraught and unable to pay for services without insurance, Barbara leaves treatment.

Prior to 1996, scenarios such as the one detailed above were all too common. There were no universal standards pertaining to the privacy of health information. Additionally, insurance companies could deny consumers coverage for needed treatment if a mental health or medical condition preceded the coverage date for the insurance plan, or insurance carriers imposed lengthy waiting periods on coverage. The Health Insurance Portability and Accountability Act (HIPAA) was enacted in 1996 and focused on protecting employees and their families from insurance practices such as these. The initial version of HIPAA focused primarily on health care coverage, specifically ensuring that employees are not in danger of not having coverage if they lose or change their jobs. In 2003, the Federal government expanded the scope of HIPAA to include Privacy and Security standards.

Although maintaining client privacy and confidentiality has always been a hallmark of mental health treatment, HIPAA has resulted in practitioners being held accountable for privacy practices under Federal law. Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and addresses the security and privacy of health data. This will mean changes to existing procedures for many mental health providers.
These training materials will focus on HIPAA and the implications for mental health practitioners. Additional resources are provided in at the end of the training material.

Objectives:

After finishing this course, the participant will be able to:

- Define HIPAA and list its components
- Discuss portability of health plans
- Define Protected Health Information (PHI)
- Discuss incidental uses of health information and reasonable safeguards
- Discuss changes to the informed consent procedure, including the Notice of Privacy Practices
- Distinguish between psychotherapy notes and the clinical record
- Describe patient access to information
- Discuss HIPAA implications for forensic services
- Describe the HIPAA Security Rule, including core areas of compliance
- Describe the term "breach," and rules for reporting security breached

Components of HIPAA

Although many mental health providers have heard the term “HIPAA” they are uncertain what HIPAA actually entails or whether HIPAA rules apply to them. HIPAA is the acronym for the Health Insurance Portability and Accountability Act. HIPAA was initially introduced in 1996. The HITECH Act (“Health Information Technology for Economic and Clinical Health Act of 2009”, part of the “American Recovery and Reinvestment Act of 2009”) expanded the scope of HIPAA.

HIPAA has several components:

- **Portability standards** that ensure the continuity of healthcare
- **Privacy standards** that govern the disclosure of protected health information
- **Security standards** that protect health information, including information maintained electronically
- **Notification rules** that requires notification following a breach
- **Enforcement standards** that establish civil and monetary penalties for violations

Health Care Portability

As initially enacted in 1996, HIPAA was devised to ensure portability of employee health coverage. HIPAA:

- Limits the ability of a new employer plan to exclude coverage for preexisting conditions
- Provides individuals with the opportunity to enroll in a group health plan if they lose other coverage or experience certain life events
HIPAA, 3

- Prohibits discrimination against employees and their dependent family members based on any health factors they may have, including prior medical conditions, previous claims experience, and genetic information.

One of the most important protections under HIPAA is that it helps those with preexisting conditions get health coverage. Previously some group health plans limited or denied coverage if a new employee had such a condition before enrolling in the plan. Under HIPAA such denials are not allowed. If a plan generally provides coverage but denies benefits to an individual because they had a condition before coverage began, this is a HIPAA violation.

Under HIPAA, a plan is allowed to look back only 6 months for a condition that was present before the start of coverage in a group health plan. The law says that a preexisting condition exclusion can be imposed on a condition only if medical advice, diagnosis, care, or treatment was recommended or received during the 6 months prior to that individual's enrollment date in the plan. Take, for example, if a person that was diagnosed in the past with anxiety but did not receive treatment for the anxiety in the 6 months before they enrolled in the plan. Because there had been no treatment, the anxiety cannot be subject to a preexisting condition exclusion.

HIPAA limits the preexisting condition exclusion period for most people to 12 months, although some plans may have a shorter time period or none at all. In addition, many plans allow people who have had prior health coverage to reduce the exclusion period even further. This is called a “creditable coverage” provision. Despite the fancy moniker, this simply means that a person was enrolled in another health plan prior to becoming enrolled in the new plan. Most health coverage can be used to establish creditable coverage, including participation in a group health plan, COBRA continuation coverage, Medicare and Medicaid, as well as coverage through an individual health insurance policy. It is advisable that individuals try to avoid a significant break in coverage (63 days) if they want to be able to count their previous coverage. Most of the time employers will provide an individual with a certificate of creditable coverage after termination of employment or individuals can request this should the new plan deny coverage based on a preexisting condition clause.

Case Study (continued)

Dr. Hart, concerned by Barbara's abrupt termination of treatment further researches HIPAA guidelines. He asks Barbara's husband to request a certificate of coverage from his previous employer, and Barbara's husband submits this to the new health care plan. This allows Barbara's previous claims to be covered and she resumes treatment.

Protected Health Information (PHI)

Prior to looking at the HIPAA privacy and security standards it is important to define the term protected health information (PHI). Protected health information is
any information about health status, provision of health care, or payment for health care that can be connected to a person. One way to determine whether health information is protected is to determine if there can be an association between the health condition and the individual. If a name or other identifier can be connected with a health condition, diagnosis, or financial status, the information comes under the HIPAA Privacy Rule and must be protected.

Thus any information about a person’s past, present or future mental health status is considered protected health information when it is connected with:

- Client names
- Client address information other than their state of residence
- Dates (except year) related to an individual, including birth date, admission date, discharge date
- Client phone or fax numbers
- E-mail address
- Social Security numbers
- Client photographs
- Psychotherapy notes (known to many as “process notes”)

A name alone, an address alone, a photograph alone does not constitute PHI.

It is important to note than many mental health agencies have specific guidelines on confidentiality that are unique to them. While confidentiality is an important factor in HIPAA’s rules on privacy, mental health standards are often more stringent. For example, many psychiatric hospitals do not allow patients to have cell phones due to the camera function.

Case Study

The HIPAA compliance officer at the Buena Vista mental health center was concerned about the center’s policy of asking people to sign in when they arrived at the clinic. This policy applied to patients, visiting physicians, and other people who visited the busy center. He was more at ease when he learned that a client’s name itself does not constitute PHI, it is its pairing with other mental health related information. Thus, the center was in compliance with HIPAA standards. If the forms, however, stated that Joe Smith was a patient in the drug and alcohol program, they would not have been in compliance with HIPAA.

Case Study

A hospital was set up so that a specific group of rooms was allotted only for Alzheimer’s patients. The nursing station contained a board with client first and last names. This constituted a disclosure of PHI because the diagnosis and full name was clearly linked. Changing the policy to having only the client first name and last initial brough the center into compliance.
HIPAA Privacy Standards

It is important to distinguish HIPAA Privacy Standards from the ethical concept of "Confidentiality," which is a broader term. Confidentiality refers to both the nature of information shared in therapy sessions as well as contents of a patient's medical records. Confidentiality is central to the practice of mental health professionals (Bond, 2011, Knapp & VandeCreek, 2012).

HIPAA sets more specific guidelines on how medical information can be disclosed to clients and third parties, and the ways in which providers must communicate and enforce these disclosures. These standards are considered minimum standards.

The disclosure of PHI is considered "the release, transfer, divulging of, or providing access to PHI to an outside entity" (Krager & Krager, 2008). In contrast, the use of PHI refers to sharing information within an organization.

The HIPAA Privacy Rule creates national standards to protect individuals' medical records and other personal health information.

- It sets boundaries on the use and release of health records.
- It enables clients to find out how information may be used, and about certain disclosures of their information that have been made.
- It gives patients the right to examine and obtain a copy of their health records and to request corrections if data is incorrect.
- It establishes appropriate safeguards that health care providers and others must achieve to protect the privacy of health information.
- It enforces civil and criminal penalties if there is a violation of clients' privacy rights

Although this may sound daunting, in actuality the requirements for most mental health providers are fairly straightforward. The Privacy Rule requires activities, such as:

- Notifying clients about their privacy rights and how their information can be used. Providers are required to notify clients about Privacy Practices during their first session (notice of privacy practices)
- Adopting and implementing privacy procedures
- Training any employees that work for them (such as billing specialists and administrative personnel) so that they understand the privacy procedures. It is important that new employees be appropriately trained and that organizations and clinicians maintain training logs.
- Designating an individual to be responsible for seeing that the privacy procedures are followed
Securing client records containing individually identifiable health information so that they are not readily available to those who do not need them

Who is a “Covered Entity”? 

If you are an individual mental health provider or work for a hospital, health plan or health care clearinghouse that transmits information electronically you are affected by HIPAA. HIPAA provisions call these individuals or institutions “covered entities.”

The term “covered entity,” includes health plans (or any groups that pay for medical coverage) as well as any mental health provider who submits billing information to managed care companies or other third parties. Currently HIPAA does not apply to providers who bill clients directly, receive out-of-pocket payments, or ask clients to submit reimbursement requests to third parties on their own. Please note that if there is even a single electronic transmission to an insurance carrier or other third party, the HIPAA requirement states that you must immediately become compliant with all guidelines. Those providers who do bill insurance companies may have noted that there has been a trend away from paper submission of billing information. It is important, then, that all mental health professionals be familiar with HIPAA and, if indicated, take steps to become compliant with the guidelines. Other examples of covered entities include hospitals, laboratories and pharmacies and health plans.

Business associates are defined as persons or organizations that perform certain functions or activities on behalf of, or provide certain services to, a Covered Entity that involve the use or disclosure of protected health information. HIPAA guidelines extend to business associates that create, receive, maintain, or transmit protected health information.

One person in each covered entity must be the designated HIPAA officer who coordinates and oversees HIPAA compliance.

Since the Privacy Rule became effective in 2003, many mental health professionals have integrated these regulatory requirements into their existing procedures. These regulations may change procedures related to informed consent, therapy notes, forensics, and psychological testing. Each of these areas will be considered later in this training module.

Case Study

Dr. Carter is a psychologist who runs a practice in which clients pay directly for psychotherapy and testing services. He routinely provides clients with receipts and many of them submit their expenses to insurance companies. Many of his clients have mentioned that they then submit requests for reimbursement online. Dr. Carter wonders whether he needs to conform with HIPAA guidelines.
At the present time, Dr. Carter is not considered a “covered entity” under HIPAA guidelines and does not need to change his already ethical practices for ensuring confidentiality and security of records. This may change in the future should the definition of who is affected by HIPAA broaden, or if Dr. Carter changes his billing practices to include any electronic transmission of information. In that case, HIPAA guidelines require immediate compliance with all privacy and security standards.

**Incidental Uses of Health Information**

Many practices play an important role in ensuring that clients receive effective mental health care, and the goal of HIPAA is not to hamper the providers ability to communicate with clients, to engage in treatment planning or to coordinate care with other professionals. HIPAA policies recognize that there may be instances in which protected health information may be disclosed inadvertently. This is called “incidental disclosure” of protected health information. Many health care providers, for example, have been in a position in which someone other than the client has overheard portions of a provider’s conversation with a client, despite safeguards that they have put into place. There may also be the need to share some aspect of a client’s information with someone not directly involved in the patient’s clinical care, such as the fact that a person doing the provider’s billing will need access to a diagnostic code. The Privacy Rule permits these incidental disclosures of health information when the provider takes reasonable safeguards to protect an individual’s privacy. Examples of reasonable safeguards include:

- Speaking quietly when discussing a client’s condition with family members in a less secure or public area;
- Avoiding using clients’ names in public hallways and elevators
- Using passwords on computer files containing personal information
- Using sound/white noise machines to mask information.

It is also helpful to note that there are more subtle ways that PHI can inadvertently be disclosed. For instance, if patient names are displayed on the outside of rooms in the wing of a clinic that treats specific conditions (e.g., substance abuse, Alzheimers) this would be considered a disclosure of PHI and the institution would be liable.

**Case Study**

*Jane is the director of a Partial Hospital Program. The program is based in a hospital that submits information electronically, thus falling under HIPAA provisions. In the PHP, clients are assigned to various therapy groups, including drug and alcohol-specific programming. Jane places a whiteboard with clients’ names at the front of the main therapy room, and color-codes the groups a client is to participate in. Is this a HIPAA violation? If so, how can Jane change this procedure?*
This example is a good one to look at the ambiguities that may be evident in applying HIPAA guidelines. Although the whiteboard displaying information may be considered an “incidental disclosure,” the key question to answer here is whether the PHP has taken adequate precautions to safeguard the client’s confidentiality. In this situation, other clients are privy to who is struggling with addiction issues. In this situation, minimal changes in procedure, such as handing each client a sheet specifying the groups that they should attend, could serve as a safeguard.

The minimum necessary standard requires covered entities to evaluate their practices and enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of protected health information.

It is also important to note that HIPAA does not restrict providers from communicating with one another. For example, a psychologist or social worker can discuss information with a client’s psychiatrist or with other members of a client’s treatment team. In fact, disclosures for treatment are explicitly exempted from the minimum necessary requirements. Uses of protected health information for treatment are not exempt from the minimum necessary standards, however. The Privacy Rule does provide substantial discretion with respect to how providers implement the minimum necessary standards.

Disclosures for Public Interest or to Benefit the Public

There are also disclosures that are allowable to due to law or to benefit the public in some way. Examples of these disclosures include:

- As required by law, under specific state law or when ordered by court.
- In reporting victims of abuse. The clinician, who is legally responsible to report abuse, is not in violation of HIPAA standards for doing so.
- When required by a judicial system or subpoena.
- For law enforcement purposes, such as to identify a suspect or missing person
- If there is a threat to the health or safety of a person or the public.

Notice of Privacy Practices

Rationale and Required Information

One change that has occurred as a result of HIPAA is the need for individual providers and hospitals that are covered under HIPAA to provide clients with a Notice of Privacy Practices. This document details client rights involving release of information. The Notice of Privacy Practices should be incorporated into the informed consent process, and the provider must obtain a signature showing that the Privacy Notice was received. If for any reason a client refuses to sign the Privacy Notice, a note indicating
that the form was offered and that the client refused to sign is sufficient. If the client is a minor, the parent is required to sign the notice of Privacy Practices.

An issue that complicates providing a Notice of Privacy Practices as well as other HIPAA policies involves the interaction between state law and HIPAA. In general, HIPAA **preempts** state law that is “contrary” to the federal rule. A provision of state law is contrary to HIPAA if:

- The provider would find it impossible to comply with both the state and federal law provisions.
- The provision of state law would be an obstacle to the accomplishment and execution of the goals of HIPAA

Many providers, then, ask the question “Can I comply with both state law and HIPAA?” The answer is generally that they can. It is helpful to look at which presents a stronger standard: state law or HIPAA. For example, if state law gives a provider 10 days to respond to a patient’s request for a copy of his medical records, and HIPAA allows 30 days, you can comply with both state and federal law by responding within 10 days.

As evident from the above discussion, the content of the Privacy Practices notice will vary. In general, this document details routine uses and disclosures of protected health information as well as an individual’s rights and the provider or hospital’s duties with respect to protected health information. The discussion below will describe some issues common to mental health care. It is not intended to provide an exhaustive list of what can be included but some general guidelines.

- **Treatment Issues:** Many mental health providers disclose PHI to provide, coordinate, or manage health care and any related services. This includes the coordination or management of PHI with a third party. For example, PHI may be provided to a health provider to whom a client has been referred to ensure that the provider has the necessary PHI to diagnose or treat them. Clients must be made aware that such disclosures will occur, and should be asked to sign an authorization allowing this disclosure.

- **Payment:** PHI is often used to obtain payment for mental health services. This may include speaking to representatives of health insurance plans before it approves or pays for the health care services. Depending on the client’s level of care, more or less PHI may be provided for coverage decisions. Routine requests by insurance companies include information about diagnosis, dates of service, and type of service provided (e.g., individual or family therapy.) Per HIPAA guidelines, a valid patient authorization is required when disclosing PHI for remuneration purposes. Thus providers should obtain authorization to communicate with insurance providers.
• Authorizations must be obtained for disclosing PHI for other reasons as well. While this is an evolving area with HIPAA, when communicating with others about PHI, the safest alternative is to receive client consent. A rule of thumb is that disclosure of PHI is permitted if a clinician is asked outright to disclose the information.

• To be valid, the authorization must include: specific information to be disclosed, who is authorized to disclose/receive information, purpose of disclosure, expiration date, signed and dated by the client. The authorization must be written in plain language, and include a statement about the patient’s right to revoke it at any time. Having a valid authorization to disclose information (“when permission to disclose is received”) is one of the permitted uses and disclosure of PHI.

• Exceptions to Confidentiality: This is both an ethical and HIPAA mandate. The Notice of Privacy Practices should include information about instances when providers may need to disclose protected health information and do not specifically need to inform clients about these. These vary by state law but may include disclosing PHI when there is a threat to self or others or when the professional is ordered to do so by law.

• Sensitive Health Information: This mandate involves how details about psychological information is disseminated, such as removing patient identifiers when able to do so, as well as treatment of particularly sensitive information such as HIV/AIDS information, disability status, alcohol and drug information. The Notice of Privacy Practices must detail steps that are taken to protect this information.

• Right of Access: The Notice of Privacy Practices should also describe how patient access to medical records. The following section on psychotherapy notes will provide additional information on what is considered a medical record. It is important to know state laws with regard to access (these can sometimes be more inclusive than HIPAA guidelines). Providers should include a statement indicating “ownership” of medical records. Clients should be informed of their right to access their medical record and to amend or correct errors in medical records. A patient has the right to access, inspect, and copy his/her PHI and to have it sent to a third party upon request. Under the HITECH Act, a patient has the right to an electronic copy of his/her PHI.

• Right to restrict disclosures. A patient has the right to prohibit disclosures to health insurers of information related to services that were paid for out-of-pocket and in full.

• Rights of decedents. People who are deceased also have a right to privacy protections. New HIPAA provisions apply to persons who have been deceased for 50 years or less. Disclosures related to a decedent’s
health information are permitted if made to family members or others who were involved in the decedent’s health care or payment for care prior to death, unless doing so would be inconsistent with any prior expressed preference of the individual that is known to the covered entity or business associate.

- Prohibition of sale of PHI without express written authorization of the individual
- Duty of covered entity to notify affected individuals of breach of unsecured PHI

The Notice of Privacy Practices must be placed in a prominent location in the provider’s facility. The new Notice of Privacy Practices must also be displayed in a prominent location on the provider’s/health plans’ website (only applicable if the covered entity has a website).

The primary criticism of the Privacy Practices is the sheer amount of information that is covered in these documents. Many clients do not read these documents and a verbal explanation of confidentiality continues to be helpful. There are many excellent examples of Privacy Practices Notices available online and through the APA Practice Organization.

Case Study

Dr. Gold, a psychologist in private practice, receives a phone call from a case manager at Magellan Behavioral Health requesting information about a current patient. The patient is being treated for PTSD secondary to childhood trauma, and is very private about the treatment. Dr. Gold is not a Magellan provider, and the patient paid in full for services. He politely informs the case manager that he cannot provide any information. When he later talks to the client, he reassures her she does not have to provide any information to the insurance company.

Health Plan and Third Party Disclosures

Case Study

Dr. Braun, a psychologist, received a request from a client’s disability company requesting a copy of the medical record. The client’s disability status was based on a physical issue, and after speaking with the client, he drafted a letter to the company stating that the client’s psychological records had no bearing on the physical issue. Dr. Braun offered to write a summary of the client’s treatment, keeping any privacy issues carefully protected.

There are times when mental health providers must disclose information to
various third parties. The case study above, for example, is one common situation. Some common requests involve the disclosure of PHI for treatment, payment and health care operations. While new HIPAA guidelines require client authorizations for these disclosures, a good rule of thumb is the “minimum necessary” concept. For example, it would not be prudent for a clinician to release a complete medical record to verify he or she performed specific services. For example, if a third party is questioning whether an appointment on specific date was medically necessary, the clinician may choose to release an overall treatment plan and that day’s progress note only.

The minimum necessary concept can also be helpful for other reasons. Consider the following case:

Case Study

Kelly Taylor, LSW, receives a request from a life insurance company, who is reviewing a client’s treatment history prior to writing them a policy.

Patient Access to Records

The HIPAA Privacy Rules allow clients to view their medical records. Previously access was dependent on state laws, however, HIPAA sets Federal standards for such access. HIPAA allows clients to view copies of records only and does not require that practitioners provide clients with the original chart. It does not require that a practitioner be given written notice of the request for medical records, but providers can establish such standards if the client is apprised of this in the Notice of Privacy Practices.

The Privacy Rules recognize that there are situations in which access to records would be contraindicated. An individual’s request to access PHI can be denied for the following reasons:

- If access is reasonably likely to endanger the life or physical safety of the individual or another person
- The PHI refers to another person (except for a health care provider) and access is reasonably likely to cause substantial harm to that person; or
- If PHI is created during research, the access to PHI may be temporarily suspended if the individual is notified in advance
- If the PHI was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would reveal the source of the information

As will be described in the following section, the Privacy Rule does not require that clients have access to psychotherapy notes. Although rules about access to psychotherapy notes do vary from state to state, in general it is assumed that such notes belong to the provider, and that a provider may restrict access to them. Some states may require that a summary of such notes be provided if clients request them. It is always advisable to know the rules of the particular state in which you practice.
Under the HIPAA privacy regulation, providers are faced with deadlines for responding to requests for medical records, and the regulation establishes a procedure for reviewing denials of these requests. Providers are allowed to charge reasonable fees for copying and postage. The practitioner has 30 days to reply to the request. HIPAA does not include a record retention period. It does specify, however, that clients can request an accounting or report of who has accessed their records for six years prior to the date of the request.

The HIPAA guidelines generally apply to requests that originate from the client. Clients may designate a friend or relative to receive information related to care and treatment. Permission should be given in writing and filed with the care provider or facility. This is important in the case of elderly or impaired clients.

HIPAA provides parents with the right to access their minor child’s medical records. There are some exceptions to allowing access:

- When the minor is the one who consents to care and the consent of the parent is not required under State or other applicable law.
- When the minor obtains care at the direction of a court or a person appointed by the court.
- When, and to the extent that, the parent agrees that the minor and the health care provider may have a confidential relationship.

HIPAA also allows clients to amend information in medical records that they consider inaccurate. Clients must detail any amendment in writing. Providers do have the right to refuse changes to the medical records, but must respond within 60 days verifying the correction or disputing the information. Clients can ask to have it noted in their chart that there is a disagreement on information.

Although this training material is primarily concerned with HIPAA mandates it is also important to consider the clinical implications of a client viewing his or her medical record. A recent review article published in the Journal of the American Medical Association found that there were no adverse consequences associated with allowing patients to review records in medical settings, however, there were more risks for psychiatric patients. In one case series, for instance, a psychotic patient’s paranoia was further entrenched when a minor piece of information, which she regarded as vital to proving her sanity was missing from the record. In a study of psychiatric inpatients, a substantial minority (32%) felt more pessimistic after reading their records. From 12% to 50% of psychiatric patients report becoming upset when they read their medical records (see Ross, MD & Chen-Tan Lin, 2003). In situations in which a practitioner is concerned about client requests to access medical records, it is important for the provider to discuss his or her concerns with the client in advance, and to limit access should the provider determine that this would cause substantial harm. More suggestions will be provided in the section on therapy notes versus the clinical record.

Case Study
Lena, a clinical social worker in a hospital setting received a phone call from a former patient of the hospital requesting his records. The patient had previously been treated for bipolar disorder, and made allegations during the course of the conversation that lead Lena to suspect that he was in an active manic state. Concerned about HIPAA regulations with regard to patient access, Lena discussed the case with her supervisor, and together they called the patient to inform him such access would not be possible. They followed up on this conversation with a letter.

**Therapy Notes vs. The Clinical Record**

A concern that is commonly expressed by mental health professionals is how HIPAA guidelines affect access to psychotherapy notes. It is important for providers to be familiar with state rules governing access to psychotherapy notes. Under HIPAA, psychotherapy notes are defined as "notes recorded in any medium by a mental health professional documenting or analyzing the contents of conversation during a private counseling session." The Privacy Standards provide particular protection for psychotherapy notes by enabling some types of information in mental health notes to remain confidential, notably the content and process of a therapy session, as well as the provider’s impressions about the client or session. Many providers refer to such notes as process notes.

In addition to providing protections on access to psychotherapy notes, HIPAA specifically states that insurance companies may not predicate coverage on the review of therapy notes. Thus, health plans cannot refuse to provide reimbursement if a patient does not agree to release information covered under the psychotherapy notes provision.

There is another caveat to the psychotherapy notes provision. The HIPAA definition of psychotherapy notes specifically states that such notes must be kept separate from the rest of an individual's record. If the provider keeps therapy notes in a patient's general chart, or if it's not distinguishable as separate from the rest of the record, access to the information doesn't receive specific protections. Many providers have chosen to keep a separate set of more general notes as a “clinical record.”

An important question to consider, then, is what to keep in the clinical record versus the psychotherapy notes. A good rule of thumb is that the clinical record must contain information to meet minimum documentation guidelines. The HIPAA guidelines specifically list the following as being separate from psychotherapy notes:

- modalities and frequencies of treatment furnished
- dates of treatment
- results of clinical tests
- treatment plan
- symptoms
- prognosis
- progress to date
Case Study

Robert is a psychologist in private practice. He is working with Mark, a gay male, who is HIV positive. Knowing that this information is sensitive, Robert chooses to keep written documentation related to the HIV diagnosis only in his psychotherapy notes on the patient, rather than in the general medical record he keeps for broader use. When Mark discovered this, he was relieved that this information could not find its way to third parties such as his employer.

Forensic Services

Although HIPAA has caused some confusion among mental health providers that provide forensic services it has not generally had a great impact on forensic services. To understand why that is, it is important to think back to the definition of protected health information discussed previously in these training materials: any information about health status, provision of health care, or payment for health care that can be connected to a person.” Forensic services are intended to serve a legal purpose, and are not related to an individual’s treatment. Such services are generally unable to be submitted to third party health insurers for payment. In addition, although clients are able to access and amend their medical records, HIPAA specifically exempts “information compiled in reasonable anticipation of, or use in, a civil, criminal, or administrative action or proceeding” from client review. This information would continue to be subject to state laws concerning access to forensic information. Providers who engage in both clinical and forensic activities must comply with HIPAA in non-forensic areas of practice.

Although forensic services do not generally fall under HIPAA guidelines, it is still necessary to have clients sign an informed consent agreement.

HIPAA Security Standards

The final HIPAA practicality for mental health practitioners concerns the HIPAA Security Rule. This rule establishes standards to help keep client information safe and to protect information from unintended disclosure. For example, in some larger group practices with administrative personnel, computer monitors containing confidential client information may be visible to others. The HIPAA Security Rule requires mental health providers to anticipate threats to, or inappropriate uses of, confidential information.

Unlike the Privacy Rule, which applies to all protected health information the Security Rule applies only to “electronic protected health information” or EPHI. EPHI is protected health information that is transmitted or maintained in electronic form rather and does not include hand-written or orally transmitted information. Examples of EPHI include:
• Health care payment and remittance advice
• Electronic requests for coordination of benefits
• Electronic treatment request forms

The Security Rule discusses administrative, physical, and technological safeguards. These include access to offices, computers and files needed to keep electronic health care information confidential and secure. Thus it looks at a practitioner or facility’s administrative procedures, the way that data on computers is secured and identified, and how information is transmitted.

The first step in the compliance process involves the provider doing a “risk analysis” of his or her practice. This analysis is a thorough assessment of the potential security risks and vulnerabilities related to EPHI. The analysis entails reviewing established security procedures, and it provides the basis for making appropriate modifications to these procedures. The Security Rule requires that practitioners conduct a formal, structured analysis to determine what security measures are appropriate and to implement these measures. In determining risk, it is advisable to use a broad definition in looking at the impact and likelihood of an adverse event.

All healthcare providers must comply with the Security Rule in four core areas (Krager & Krager, 2008):

• Confidentiality, integrity and availability of all EPHI they create, receive, maintain or transmit
• Protecting against anticipated uses or disclosures of electronic information that are not permitted under the Privacy Rule
• Protecting against any anticipated threats or hazards to security and integrity of EPHI
• Ensuring compliance with the Security Rule by their workforce

Many of the changes that a provider or facility may need to make may be simple ones; but others may be more complex. Security requirements are organized into a number of different areas, which will be discussed in more detail. These areas include administrative, physical and technical safeguards, organizational requirements, policies, procedures and documentation.

Administrative safeguards are policies and procedures designed to clearly show how the covered entity will comply with HIPAA. For example, covered entities (entities that must comply with HIPAA requirements) must adopt a written set of privacy procedures and designate a privacy officer to be responsible for developing and implementing all required policies and procedures, covered entities must provide training on safeguarding EPHI, and should have instructions for managing security breaches.
Physical safeguards are those concerned with controlling physical access to protect against inappropriate access to protected data. Examples are policies to address proper workstation use, and limited Access to hardware and software.

Technical Safeguards are those concerned with controlling access to computer systems and enabling covered entities to protect communications containing PHI transmitted electronically over open networks from being intercepted by anyone other than the intended recipient. Documented risk analysis and risk management programs are required.

It is important for covered entities to be aware of and to implement security measures for EPHI. Examples of security measures appropriate to mental health professionals include:

- Ensuring that rooms in which computers are placed are locked when not in use
- Security and risk management plans
- Making certain that computer files contain passwords known only to those who need to access data
- Ensuring that workstations cannot be viewed by those who pass them
- Setting strong passwords for devices and wifi
- Using anti-virus software
- Using encryption or secure transmission systems for transmitting data. Encryption is the conversion of data into a systematically scrambled format that is very difficult for an unauthorized person to decode. For a full description, see APA Practice Organization, 2014.
- Data backup and storage.

The Security Rule applies to large organizations, as well as smaller physician offices and solo practitioners. The Security Rules take into account the concept of scalability. This means that a solo practitioner will not be expected to take the same steps to comply as will a large practice or a health care facility.

If security is compromised, HIPAA requires breach notification. Notification required should be made later than 60 days after breach discovery or when the breach should have been known. HIPAA requires written notice to affected individuals, and if more than 500 individuals are affected, notice to Health and Human Services.

In summary, basic elements of the Security Rule are:

- Conduct a risk assessment
- Identify, respond to, and document security incidents
- Implement a data back up plan, disaster recovery plan, and emergency mode operation plan
- Adopt physical, technical, and administrative safeguards
- Develop and maintain policies and procedures to ensure compliance
Under HIPAA, it is also important that covered entities develop a Business Associate Contract that specifies how the Business Associate will appropriately safeguard EPHI it receives and transmits. The contract between the covered entity and Business Associate must provide that the Business Associate will:

- Implement safeguards that are appropriate to protect the confidentiality of EPHI it receives and transmits
- Ensure that staff members that are entrusted with such data agree to these safeguards
- Report to the covered entity any security incident of which it becomes aware
- Authorize termination if the contract if the covered entity determines that the Business Associate has violated the contract

Case Study

Dr. Robb, a psychologist in private practice has just become familiar with the HIPAA Security Rules. He does a risk analysis and takes steps to make changes to administrative procedures. In completing his risk analysis, Dr. Robb notes that his assistant will often take files home to work on billing and will submit payment requests on her home computer. As Dr. Robb cannot ensure the security of offsite transmissions, Dr. Robb asks his assistant to only work on client information and needs in the office.

Clinician Identifiers/Unique Identifiers

Another change that has come about as a result of HIPAA concerns the unique identifiers that providers now must use. HIPAA covered entities including any providers completing electronic transactions must use a National Provider Identifier (NPI) to identify themselves to insurers (private insurance companies and government agencies such as Medicare and Medicaid). These identifiers help to streamline and standardize transactions as well as contribute to security of transmitted data. The use of NPI numbers for electronic transactions became effective in May of 2007. Despite the fact that these unique identifiers (EIN, NPI) have been used for some time, many clinicians are still confused them.

An employer identification number (EIN) is a nine-digit code with a hyphen after the second digit. It is sometime referred to as a tax identification number since it also appears on the IRS form W-2. The use of this identifier is required when used for enrolling and disenrolling from a health plan.

The health care provider identifier or national provider identifier (NPI) is a 10-digit number unique to the clinician. The NPI is part of HIPAA’s Simplification Standard. Each covered health care provider must have a unique NPI.

An NPI-1 is issued to providers who are individuals, and an NPI-2 is issued to an
organization. Solo practitioners who have incorporated for tax purposes may need to maintain both an NPI-1 and NPI-2 number if conducting Medicare billing.

**Enforcement Rule**

Another aspect of HIPAA that clinicians should be aware of is the HIPAA Enforcement Rule. The Enforcement Rule sets civil money penalties for violating HIPAA rules and establishes procedures for investigations and hearings for HIPAA violations. Prior to about 2006, prosecutions for violations were rare. From 2003 to 2013, the state of Rhode Island was the top enforcer of HIPAA violations and has the only state in which more than 40% of violations result in corrective action. Other top enforcers were listed as Alaska, Washington, Oregon, Idaho, Wyoming and New Hampshire. Corrective action was associated with between 30% and 40% of HIPAA violations in those states (Kim, 2014).

The HIPAA Enforcement Rule applies to organizations as well as individuals, and non-compliance with HIPAA standards can result in corrective actions that range from putting new procedures into place to fines. In 2014 for example, a doctor in a nursing home in Texas texted a nurse some lab results. The nursing home was required to revising its HIPAA policies and procedures, including training on identity theft, higher an external contractor to educate employees, designating a HIPAA compliance officer for the facility, and sending a letter to all residents and families notifying them of the HIPAA violation and the steps the facility is taking to fix and prevent new occurrences (Healthcare Security and Privacy, 2014). This proved very costly. In another situation that also occurred in Texas a former hospital employee was criminally indicted for HIPAA violations, including unauthorized access of medical charts. Depending on the outcome, the employee could be fined between $50,000-250,000 and face incarceration (National Law review, 2014). As of March 2013, the U.S. Dept. of Health and Human Resources (HHS) has investigated over 19,306 cases that have been resolved by requiring changes in privacy practice or by corrective action.

According to the HHS website (www.hhs.gov), the following lists the issues that have been reported according to frequency:

- Misuse and disclosures of PHI
- No protection in place of health information
- Patient unable to access their health information
- Using or disclosing more than the minimum necessary protected health information
- No safeguards of EPHI

These examples underscore the importance of understanding HIPAA. While there have been some examples applied to mental health, they remain fewer in number.
Summary

HIPAA has changed the way that many mental health providers approach a client’s confidential health information. Although confidentiality has always been essential in the practice on mental health, the Federal guidelines increase accountability to ensure such privacy. It is important for practitioners to note:

- HIPAA standards apply to protected health information: “information about health status, provision of health care, or payment for health care that can be connected to a person.” This broadly includes any part of a client’s medical record or payment history.
- HIPAA sets boundaries on the use and release of health records.
- HIPAA patients the right to examine and obtain a copy of their own health records and request corrections.
- It establishes appropriate safeguards that health care providers and others must achieve to protect the privacy of health information.
- Providers must notify clients about their privacy rights and how their information can be used.
- Mental health practitioners must adopt and implement privacy procedures.

Resources

APA Online. Patient Protections: The Core of the Privacy Rule.  


Connell, M. & Koocher, G.P. HIPAA & Forensic Practice  
http://www.kspope.com/ethics/hipaa.php


Daw Holloway, J. (Feb. 2003). What takes precedence: HIPAA or state law?  
http://www.apa.org/monitor/jan03/hipaa.html


HIPAA for Psychologists - Questions and Answers
http://www.apait.org/apait/resources/hipaa/faq.aspx


Overview of HIPAA – General Information http://www.cms.hhs.gov/hipaaGenInfo/
