

HIPAA PRIVACY TRAINING

Date: _____

Name: _____

Please indicate which modules you have completed by checking the appropriate boxes, sign this document and turn the document in to Randy Brooks, Privacy Officer.

TRAINING MODULES

Introduction

HIPAA PRIVACY – What is it about?

Information Security and Confidentiality

Health Information Privacy

Privileged Information

Role of the Privacy Officer

Client Rights with Regard to Protected Health Information

Minimum Necessary

Transmission of Confidential Information

Disclosure of Confidential Information without a Release

Business Associate Contracts

Documentation of Disclosures

Delay or Denial of Release Information

Release of Information to Protective Services

Notice of Privacy Practices and Acknowledgment of Same

Handling and Disposal of Media Containing Confidential Information

Research Activities

I have completed the HIPAA Privacy Training modules checked above.

Signature

Date

HIPAA PRIVACY TRAINING INSTRUCTIONS

HOW TO USE THIS MANUAL

The Privacy Training Manual consists of:

- Table of contents
- Introduction
- Modules containing a summary of each policy/procedure or practice that addresses HIPAA privacy

Everyone is required to read:

1. The Introduction
2. Each Module

HIPAA PRIVACY

What is it about

- A. The Privacy Rule** became effective April 14, 2001. Health care providers must comply with the new requirements by April 14, 2003.

The Privacy Rule for the first time creates national standards to protect individual's medical records and other personal health information by:

1. Giving the clients more control over their private health information.
2. Setting boundaries on the use and release of health records.
3. Establishing appropriate safeguards that providers and affiliates must achieve to protect the privacy of health information.
4. Holding violators accountable, with civil and criminal penalties that can be imposed if they violate client's privacy rights.
5. Striking a balance when public responsibility requires disclosure of some forms of data - for example, to protect public health.

For clients it means being able to make informed choices when seeking care based on how their personal health information may be used.

1. It enables clients to find out how their information may be used and what disclosures of their information have been made.
2. It generally limits release of information to the minimum reasonably needed for the purpose of disclosure.
3. It gives clients the right to examine and obtain a copy of their own health records and request corrections.

For those working as an EAP affiliate it is important to remember that application of the most restrictive rule should be used in every situation.

- B. When it comes to personal information** that moves across agencies, hospitals, doctors' offices, insurers or third party payers, and state lines, our country has relied on a patchwork of federal and state laws. Under the current patchwork of laws, personal health information can be distributed, without either notice or consent, for reasons that have nothing to do with a person's medical treatment or health care reimbursement. In today's world, the old system of paper records in locked filing cabinets is not enough. With information broadly held and transmitted electronically, the Rule provides clear standards for all parties regarding protection of personal health information. Our organization has chosen to comply with the most restrictive privacy rules to ensure confidentiality for our clients.

- C. The regulations require:**
The Privacy Rule requires activates such as:

1. Providing information to clients about their privacy rights and how their information can be used.
2. Adopting clear privacy policies and procedures for a health care provider's practice, hospital or health.
3. Training employees so that they understand that privacy policies and procedures.
4. Designation an individual to be responsible for seeing that the privacy policies and procedures are adopted and followed.

5. Securing client records containing individually identifiable health information so that they are not readily available to those who do not have a need to know.

Clients have been given new rights with regard to their protected health information. Clients under the HIPAA Privacy Rule will have the right to:

- Get access to and copies of their Protected Health Information (PHI).
- Request Amendments or corrections to PHI they believe to be inaccurate.
- Receive an accounting of all disclosures made of their PHI treatment, payment or health care operations.
- Receive an accounting of all disclosures made of their PHI that were made for reasons other than treatment, payment or health care operations.
- Request Restrictions on who can access to their PHI.
- Receive communications by alternative means or alternative locations.
- Receive a copy of our Notice of Privacy Practices which will explain the uses and disclosures MHC is allowed or required to make with their PHI.
- Sign an Acknowledgement that they received our Notice of Privacy Practices.

D. Who is covered by this rule:

The Privacy Rule covers health plans, health care clearinghouses, and those health care providers who conduct certain financial and administrative transactions electronically. Employing electronic transactions such as electronic billing and fund transfers is what is used to designate someone as a "covered entity." These "covered entities" are bound by the new privacy standards even if they contract with others called "business associates" to perform some of their essential functions. Although our organization does not utilize electronic billing or fund transfers, we will comply with all relevant rules pertaining to protection of PHI.

E. How will Department of Health and Human Services (HHS) enforce compliance?

Enforcement will be through penalties for non-compliance. HIPAA calls for some of the severest penalties ever imposed on health care. Fines begin at up to \$25,000 per year for unintentional multiple violations of the same standard in a calendar year. Then up to \$50,000 and 1 year in prison for knowing violation. SO, if you knew of any non-compliance and did not take action this fine can be applied. Then it escalates up to \$100,000 and 5 years in prison for violations involving false pretenses. Finally, up to \$250,000 and 10 years in prison for obtaining PHI with intent to sell, transfer or use if for personal gain, or to cause malicious harm.

F. The goal of our organization is to be compliant with the HIPAA Privacy Rules.

Information Security and Confidentiality

Information security is the protection of all EAP client information. This is done by assuring confidentiality, integrity, and availability.

Confidentiality means that only certain people get certain information, and no one else does. Confidentiality is based on the "need to know." This means that you have information only when you "need to know" the information in order to do your job.

Integrity means you can trust that NO ONE has changed information inappropriately.

Availability means that information is available whenever it is needed to do your job.

Information security includes information on computers, disks, file servers, or information in transit such as emails and faxes.

Security is important for client information and for EAP clinical information. It is also important for many other types of information. Examples of other confidential information: computer passwords, affiliate records, and anything an employee or affiliate does NOT "need to know" in order to get his or her job done.

There is a difference between client information and EAP clinical information. *Both are confidential.*

Client information includes the client name, age, place of employment, address, telephone, insurance company etc. EAP clinical information includes what the client is seen for, diagnoses, assessments, progress notes etc. Sharing ANY information about a client (even his or her name) with someone else who does not "need to know" is wrong. This information needs to be kept confidential.

Confidential information should be discussed ONLY with those who "need to know" in order to get their job done. Never discuss confidential information in public areas, such as hallways, elevators, restrooms, the kitchen etc. Do not leave confidential information in a voice mail message or sent it in e-mail outside of the agency.

We are committed to information security. There are several types of information security controls that should be in place in all EAP service locations. These include policies and procedures, computer controls, locks and protected areas, and education. Even with all of these controls in place, someone may see or hear confidential information.

You might utilize the information on a computer screen, in a report, at the fax or copier machine that is confidential. You may overhear a conversation that is confidential. When this happens, you may want to remind others to keep confidential information secure. You should never share confidential information that you have seen or heard.

Our organization has policies regarding information security and computer use. Information security includes confidentiality, integrity and availability for computerized information. You will find the specific policies and procedures in the organization's manuals.

Privacy and the Release of Information

There are rules and laws about the release of client information and EAP clinical information. We support these rules and laws.

All clients have rights. Client's rights include the right to privacy; the right to see their own health information; and the right to limit who will obtain their health information. Health information cannot be given out to anyone unless the client has signed a release of information authorization. Upon receipt of a signed release of information authorization staff will follow the policies and procedures as outlines in the EAP policy.

Certain types of EAP clinical information are considered "strictly" confidential. Strictly confidential information may not be disclosed without a signed release of information specifically authorizing the information to be released. Strictly confidential information includes information about:

- Child and elder abuse
- Sexual abuse
- Alcohol and drug abuse
- Highly communicable diseases – HIV, Tuberculosis, Hepatitis and sexually transmitted diseases
- Mental Health

Appropriate uses for EAP clinical information in our organization include:

- Information necessary to carry out treatment, payment or healthcare operations.
- When a client has signed a release of information.
- Information needed for certain public health activities (vital statistics; prevention or control of disease, injury or disability; reporting child or elder abuse or neglect).
- Release following a court order in which the client is a party, and his/her medical condition or history is at issue.
- Release to coroners and medical examiners.
- Release to law enforcement officials if following a warrant, subpoena, etc.
- Release in certain emergency circumstances based upon reasonable belief that disclosure is necessary to lessen or prevent a serious and imminent threat to the health and safety of an individual or the public.

Whenever authorized release of information is being made, release the "minimum necessary." This simply means releasing the minimum amount of health information that is necessary. "Minimum necessary" also applies to information released for treatment, payment, and healthcare business.

Discipline

Our Corporate Compliance policy describes the disciplinary process that will be implemented if there is misuse of information by employees or affiliates.

Conclusion

Information privacy is the responsibility of everyone. You are required to follow policies, procedures and work practices designed to protect information. If you know of someone misusing information, you are required to report that misuse. You should report this to Randy Brooks, Privacy Officer. You can report misuse anonymously.

Procedures and Practices for Protecting the Rights of Individuals with Regard to Their Health Information

Health Information Privacy

- A.** All information regarding the health care of an individual must be kept confidential. Including but not limited to:
- EAP clinical records, billing records, any correspondence, phone calls; health information in any form (oral, paper, and electronic communications).
 - Client information generated or received by the EAP
 - Information entrusted by a client to an employee or affiliate, and
 - Any knowledge the employee or affiliate has regarding a client.
- B.** Protected Health Information, (PHI) also includes name, address and all information that we learn about, collect or maintain on individuals:
1. Client information collected or generated within the EAP shall be kept so that:
 - Access to it is restricted to only those with a need to know.
 - All use and disclosure is restricted to only those with a legal right to know.
 2. Every affiliate provider, clinical staff member, other staff member, business associate, and vendor of this organization shall be responsible for maintaining the confidentiality of all client information entrusted to them and to exercise due care in any discussion, use or disclosure of client information.
- C.** PHI and client confidential are essentially the same.

Privileged Information

A. Definition – Privileged communications means a communication made to a psychiatrist, psychologist, or social worker in connection with the examination, diagnosis, or treatment of a patient, or to such other persons while they are participating in such examination, diagnosis, or treatment.

B. Disclosure of Privileged communications

Privileged communications shall not be disclosed in civil, criminal, legislative, or administrative cases or proceedings unless the client has waived privilege, except as follows:

1. When the privileged communication is relevant to a physical or mental condition of the client which the he or she has introduced as an element of his claim or defense in a civil, criminal or administrative case.
2. When the client has been informed that any communication could be used in proceedings governed by the Mental Health Code or in a court-ordered examination.
3. In civil or criminal actions against the psychologist, psychiatrist, or social worker for malpractice.

Role of the HIPAA Privacy Officer

The Privacy Officer's main responsibilities are:

1. To develop and implement policies and procedures required by the Federal Privacy Regulation (HIPAA), to protect the confidentiality of health information.
2. To educate the staff members and affiliates with regard to these policies and procedures.
3. To be responsible for receiving all consumer complaints regarding the privacy procedures or alleged breaches of the privacy procedures. The Privacy Officer or designee will also be responsible for investigation all complaints and recommending whether disciplinary actions should be taken against the employee(s), or affiliate as appropriate.

Client Rights with regard to Protected Health Information (PHI)

Everyone we collect health information on has certain rights regarding the control of that information. An individual has the right to:

1. Access to their PHI, which means the individual can see and get a copy of their PHI for as long as the EAP maintains it, with some exceptions. This requires a written request for the information. There may be a charge for copies.
2. Amend to correct inaccurate PHI, which means the individual can request the EAP to amend PHI, or a record about them that they believe is inaccurate, for as long as the EAP maintains it. Requests to amend records may be denied if the record was created by another agency or person.
3. Receive an account of disclosures of their PHI, which means an individual may request and receive an accounting of disclosures made using their PHI by the EAP.
4. Request restrictions on giving access to their PHI, which means an individual may request a restriction on who has access to their PHI. The EAP does not have to agree to that request, but if the EAP does agree then it is binding for as long as the PHI is kept or the agreement is dissolved then the lifted restriction applies to information collected from that day forward and does not apply to any PHI already collected.
5. Request confidential communications at alternate locations or means, which means that the EAP must permit individuals to request and must accommodate reasonable requests for individuals to receive communications of PHI by alternative means or at alternative locations. Such as:
 - i. Calling the individual at work instead of home.
 - ii. Sending PHI to a specified address.
 - iii. Discussing their clinical issues with them in a more private area.
 - iv. Electronic communication instead of phone or mail.

6. Get a copy of our Notice of Privacy Information Practices, which means the EAP must give individuals a copy of our Notice of Privacy Information Practices that will explain:
 - How we will use and disclose of their PHI.
 - Their rights regarding their PHI.
 - What our duties are with regard to their PHI.
 - How to file a complaint.

Confidentiality of client's records is determined by the relevant state and Federal Substance Abuse Confidentiality Laws. Detailed information regarding confidentiality of client information and the client's right to access their information are contained in the Confidentiality Policy.

Minimum Necessary (access to PHI)

- A.** When using or disclosing Protected Health Information (PHI) everyone at the EAP must make reasonable efforts to ensure that only the minimum necessary PHI is used or disclosed to accomplish the purpose of the use, disclosure or request.
Except disclosures:
 - To a health care provider for treatment purposes.
 - To the individual who is the subject of the information with some exceptions and in compliance with state laws.
 - To the Department of Health and Human Services for privacy investigations.
 - Disclosures required by law.
- B.** The EAP may not use, disclose or request the entire client record, except when the entire client record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request.
- C.** EAP staff may not access or share PHI unless it is necessary to carry out the functions of their duties as a staff member.

Transmission of Confidential Information

- A.** Only staff specifically authorized by the President, Vice President or designee may transmit confidential information. The staff will assure that there is either a valid "Authorization for Release of Information" or that the conditions for release without consent that are contained in the applicable state laws are met.
- B.** Unauthorized disclosure of confidential information, which includes otherwise permissible transmission by a staff not authorized to do so, will result in disciplinary action up to and including discharge.

Disclosure of Confidential Information without a Release

The agency may disclose confidential information without consent pursuant to applicable state or federal laws only.

Business Associate Contracts

When the EAP uses another business or an independent contractor to perform a function for or on behalf of the EAP and in doing so shares Protected Health Information (PHI), there must be a written contract between the EAP and the business associate. The contract must establish the permitted and required uses and disclosures of PHI that the business associate can make with the information. There are specific requirements that must be met in the contract. If the business associate violates the contract or commits a breach of confidentiality, the EAP must try and stop the misuse of information and if unsuccessful, terminate the contract and report the problem to the US Department of Health and Human Services.

Documentation of Disclosures

- A.** All disclosures of clinical information, whether voluntary or involuntary shall be noted in the clinical record, and shall include; the date of the disclosure, a description of the information released, the name and address of all who receive the information and the purpose for which it was released.
- B.** A client may ask for a record of disclosures of information. This request must be in writing. The request must specify the time period and recipient of the disclosures sought. The agency will provide a listing of all disclosures that meet the criteria of the request. The listing will include; the date of the disclosure, a description of information released the name and address of all who receive the information and the purpose for which it was released.

The actual cost of the accounting to the client may be charged if they are requesting a second accounting within a 12 month period. A response to a request for an accounting of disclosures must be made within 60 days of receiving the request, except in circumstances where the request is delayed or denied.

Delay or Denial of Release of Information

Any decision to delay or deny a release of information requested by the client or by any legal or administrative entity must have the approval of the President or Vice-President.

Release of information to Protective Services

- A.** Only written requests recognized state protective service authorities will result in a review of the record. If oral requests are received, the person making the request will be requested to place the request in writing so that the EAP may respond promptly.
- B.** A written request shall immediately be copied to the President or Vice-President for approval prior to the review of the record.
- C.** The President or Vice-President shall contact the provider as soon as possible, but no later than 24 business hours after receipt of a written request. Both shall review the record to determine if it is a substance abuse record. If the record is a substance abuse record, the record shall only be released with the written consent of the client or a valid court order in accordance with the procedures established in the Federal Confidentiality Regulations 42CFR, Part 2.
- D.** If the record is a non-substance abuse record, the President or Vice-President shall review the written record to determine whether any portions are pertinent to the investigation as specified in the written request. IF any are found, copies shall be extracted from the record and sent to the requesting state authority with proper identification of the information (date of interview, clinician conducting interview). This response shall be completed within 14 days after receipt of the written request.
- E.** Delivery of the information to the Protective Services shall include obtaining from that authority a signed receipt for the information and signed acknowledgement of responsibility to use the information only for the purposes for which it was sought and to refrain from re-disclosure of the information except for the purpose specifically stated in the request.

If for any reason the EAP staff are unable to respond within the specified times lines, the President or Vice-President shall immediately be notified and shall seek and extension of time from Protected Services.

Notice of Privacy Practices – How we use and Protect Your Personal Information

All clients must be given a Notice of Privacy Practices, which will give them information about the following:

- The ways in which the EAP will use and disclose the client's personal health information.
- The client's rights under the HIPAA Privacy Rule.
- Our duties under the HIPAA Privacy Rule.

The Notice must be provided on or before the first visit, usually at intake. It only needs to be provided once unless there is a change in the Notice. It also must be provided to anyone upon request. It may be delivered electronically but must also be provided in paper form if requested.

At the time the client is provided with the Notice, EAP staff and affiliates must make a good faith effort to obtain a signed or initialed Acknowledgement from the client or the client's legal representative (guardian or parents if the child is a minor) indicating that they received a copy. This acknowledgement only needs to be obtained once unless the Notice changes.

The Notice must be revised if there is a material change to any of the following:

- The EAP uses and disclosures of protected health information.
- The EAP or affiliate's duties under the HIPAA Privacy Rule.
- Any significant changes to our policies and procedures affecting our privacy practices.

The Privacy Officer must keep copies of all versions of the Notice of Privacy Practices for seven years from the date it was last in effect. All acknowledgements must be kept for the same time period.

Handling and Disposal of Media Containing Confidential Information

Media is any format on which information is contained, including paper (documents, reports, and any copies), magnetic (diskettes, hard drives), and optical (CD'S).

Staff members and affiliates who create, store, or use media containing confidential information shall take all necessary precautions to prevent access to the media by others who do not have a need to know the information. This includes:

- Securing media in locked cabinets or drawers.
- Limiting reproduction to copies intended for only those with a need to know.
- Transmitting copies with care between each other.
- Proper disposal when it is no longer needed.

Disposal of paper documents containing confidential information shall NOT be placed in normal waste containers. It shall be placed in the shredding and disposal containers placed throughout the building by the end of each business day.

RESEARCH ACTIVITIES

Clients have the right to complete privacy regarding their EAP services, and outcomes. Any evaluations or research done by staff or students of the organization shall follow the guidelines established in the Research Policy.