

HIPAA ORIENTATION TRAINING MODULE

OVERVIEW

In 1996, Congress enacted the Health Insurance Portability and Accountability Act (HIPAA) for the purpose of developing national patient record privacy standards. The regulations were drafted by the Department of Health and Human Services (HHS) and the final rule was published in December 2000. The effective date for implementation was April 14, 2001, with full compliance by April 14, 2003.

HIPAA's privacy section applies to the protection of all individually identifiable health information in all forms, including oral and written communication. These oral and written communication regulations directly affect all employees, students and volunteers of Steele County Public Health Nursing Service.

KEY TERMS

Confidentiality- A means of protecting health information and safeguarding it from unauthorized distribution.

PHI- Protected health information (PHI) includes any electronic, paper, or oral data that can be used to identify a patient's health.

Consent – A patient's agreement with the release or disclosure of personal health information.

TPO- HIPAA states that when treatment, payment, and health care operations (TPO) are necessary, PHI may be used and disclosed without the patient's written authorization. See Notice of Privacy Practices.

Need-to-know and minimum-necessary principles- Discussing a patient with someone who has a specific reason, or need, for the information, and providing only what is necessary.

FACTS

HIPAA is a federal law that protects the privacy of a person's health information, making health care communication confidential. Minnesota has had the Minnesota Data Privacy Rule since the 1970s and has required client/patient consent. Because the most restrictive law/rule must be implemented by a health professional in Minnesota, both Minnesota Data Privacy and HIPAA must be considered in each situation.

The HIPAA privacy rule creates the first national standard to protect individual's medical records and other personal health information. HIPAA gives us a set of guidelines for protecting the confidentiality of individually identifiable health information (client information). HIPAA covers:

- 1) What is considered confidential information;
- 2) How do we use client information;
- 3) Who do we share information with; and

4) How much information are we allowed to read and to share?

The Act's Privacy Rule requires health professionals to balance the protection of a patient's health information with the need to protect public health. The Privacy Rule allows a health professional to provide private information without a patient's authorization to public health authorities in order to prevent or control disease, injury, or disability or when legally required, for example as a mandated reporter.

CONFIDENTIALITY AND PRIVACY

Privacy of information requires that anything said or written about a client must not be obtained by any unauthorized person. The client authorizes who may have access to the information.

Protected health information (PHI) is one aspect of information privacy. PHI includes any electronic, paper, or verbal data that can be used to identify a client's health, medical condition, or treatment, such as visit notes, assignment sheets, etc. Items including a client's name, address, and other personal information must remain confidential.

1. Consent

To disclose PHI for treatment, payment, and health care operations (TPO), an agency must have the patient's agreement, or consent. This type of consent is not the same required for treatment. This agreement or consent is achieved through the Notice of Privacy Practices (see Steele County Public Health Nursing, Notice of Privacy Practices)

The Notice of Privacy Practices includes the following:

- Patient's privacy rights and how to exercise them
- Agency's privacy practices, and
- Agency's use and disclosure of PHI without written authorization.

Prior to care, the clinician who admits the patient must provide him or her with a copy of the Notice of Privacy Practices, and obtain written acknowledgement that the client received the notice. One of the most important aspects of consent is gaining insight into the client's situation. This ensures that client's health information is used and disclosed appropriately, and helps agency staff handle PHI disclosure. ***Example:** The admitting nurse makes an admission visit. One of the first things she does is discuss the notice with the client, and obtain the signed acknowledgement form. She also asks the patient about emergency contacts, who visits the client, and who listens to messages on the client's answering machine.*

2. Computers

An agency's computer-based system (workstations, laptops, and hand-held devices) can increase the risk of unauthorized disclosure of information. Physical, technical, and administrative safeguards apply to servers, personal computers, electronic client records, billing systems, and modems. To protect the integrity, availability, and

confidentiality of information, those who work on computers must follow these simple steps:

- Guard your password.
- Do not post or share your password.
- Change your password regularly.
- Don't leave information on the computer screen if you need to step away.
- Log out of the computer if you leave for an extended period.
- When traveling to a client's home, do not access other client's files.
- Don't let others use your computer or hand-held device.

3. Communication

There are many ways an agency and its staff may need to communicate or disclose client health information. Therefore, it is important to consider client privacy and confidentiality at all times.

FAX

The agency should keep the fax machine in a private place, out of public view. Pre-printed cover pages that explain the agency's confidentiality and disclosure terms should be available. When faxing, always double check the fax number for accuracy, dial carefully, and confirm that the fax was received.

E-MAIL

Staff must know and follow the agency's security measures for e-mailing PHI. Always verify e-mail addresses before sending private information.

WRITTEN COMMUNICATION

In the office, keep file drawers locked & shred client-sensitive information.

VERBAL COMMUNICATION

When discussing client health information, follow the need-to-know and minimum-necessary principles, meaning do not discuss a client with anyone who does not have a specific reason, or need, for the information. If a person does need the information, provide only what is necessary. Do not expand on the vital information or use a client's information or condition to gossip. Never discuss information with neighbors, friends, relatives, or others unless the client provides authorization.

When visiting a client, never talk about other clients. Even if the clients are friends, neighbors, etc., do not discuss any clients' situation with another client. Staff must also be careful when discussing other clients with staff members (either on the phone or in person) while in another client's home.

PRIVACY AND HIPAA FUNDAMENTALS

HIPAA has made health care privacy a client's fundamental right, and it is staff's job to help enforce that right. A client now has more control over personal health information and can prevent information from being spread to unauthorized recipients. All staff has a professional obligation to maintain confidentiality of PHI by following agency privacy protocol.

As a staff member, student or volunteer, you may review, discuss, and handle confidential client information. Therefore, you must pay careful attention to HIPAA policies and your agency's procedures, manage client data with care, and report any violations or questions to your supervisor.

Be very careful providing and receiving information over the phone. Always verify to whom you are speaking, their relationship to the client or situation, and share only the necessary information. Follow agency procedures regarding leaving client –specific information on answering machines and voicemail.

It is rare, but an attorney or member of the media may contact you regarding a client. When this occurs, say “ I cannot discuss anyone who may or may not be a client of my agency.”

Minimum Necessary or Need-To-Know

Minimum necessary deals with looking at information, using that information or sharing that information on a “need to know” basis in order to get your job done. Working in a health care organization does not automatically give a person the right to use or even to see any and all client records. You should only be able to look at information you need to know to get YOUR job done.

The minimum necessary does not apply to the client. They can have access to all of their protected health information. If you are unsure about what information you can see and what information is restricted in your agency, check with your supervisor.

Client Rights

1. The right to know what their rights are under the HIPAA regulation.
2. The right to receive a paper copy of the “Notice of Privacy Practices”.
3. The right to “Request Restrictions”-who will not be allowed to see parts of their record.
4. The right to have “Confidential Communication” between the client and persons caring for the client. For example, they can request that no family member is present when discussing their health.
5. The right to access their health record and inspect and copy their health record. If a client asks you if they can see their record or asks you to copy a portion of the record for them, sit with them and help with the interpretation of the record. **Always notify your supervisor of this request before you proceed.**

6. The right to “Amend Records”. This means they can add some written information to the record making a correction to something they don’t agree with. The original charting is not changed. This request can be denied-agency policy and procedure will be followed. **Again, always notify your supervisor of this request before you proceed.**
7. The right to an “Accounting of Disclosures”/ The right to know what health information has been sent and to whom and why it was sent. There are very few types of ”disclosures” that the organization needs to track.
8. The right to complain if they believe their privacy has been violated.
9. The right to “opt-out” future communication on marketing and fundraising activities.

Communicate Client Information

Phone conversations

- Do not talk about a client over the phone if there is anyone who might overhear. If another staff member calls you at a client’s home, never say anything that might identify any clients.
- When you call to report an observation about a client, do not allow anyone besides the caregivers to hear you.
- If you receive work-related messages on your home answering machine, do not allow your family to listen to them.
- Do not leave messages on the client’s answering machine unless the client requests it.
- Use your cellular phone carefully. Never use the phone to relay client information in an area where others could overhear the conversation.

Face-to-face conversations

- Follow the need-to-know and minimum-necessary principles.
- Never discuss a client in a common area of the office. This includes hallways, open areas, the bathroom, or the reception area.
- Do not discuss one client inside another client’s home, even if you are talking with someone who cares for both clients.
- Never discuss a client’s condition with anyone, such as a neighbor or family member, without the client’s consent. If you are unsure of whom the client has authorized check the client file and/or ask the appropriate staff member or supervisor.

Written communication

- Guard your visit notes and other papers so that no one else can see them. Don’t leave papers lying around your house, car, or office.
- All paperwork taken into a home should be kept confidential.
- Do not put papers containing information into the garbage. Shred all documents.

Follow agency policies

It is your job to closely follow your agency's policies regarding security and confidentiality of patient information. Steele County and Steele County Public Health Nursing Service have many policies that relate to confidentiality, privacy, communication, computers, etc. During your orientation and periodically during your employment or service with us these policies will be reviewed.

You are required to report any known or suspected breach of confidentiality without fear of revenge or retaliation. If you have a question or concern related to these policies, go to your supervisor for advice.

When to share TPO

HIPAA regulations allow the use and disclosure of PHI for the purposes of TPO without the client's prior written consent. You must know when you may share PHI, and when you must obtain authorization. In all cases abide by the need-to-know and minimum-necessary principles.

Treatment

An agency may share PHI with another health care provider for treatment purposes as long as that provider has a direct treatment relationship with the client. *Examples: An intake coordinator receives a discharge client's referral information, a social worker coordinates a community service referral, or a registered nurse talks to the emergency room nurse.*

Payment

A client's PHI is often shared with other health care providers who make or receive payments related to that client's care. *Example: A nurse shares information with a benefits coordinator to find out about a client's coverage.*

Operations

Entities that have a relationship with the same client can share PHI for limited operational purposes. *Example: An agency shares PHI with the compliance committee, surveyors, its ethics committee, and the performance improvement committee to improve health care operations.*

OUTCOMES

Your job in relation to HIPAA is two-fold. First, you must ensure the confidentiality of your client's health information through proper communication and care processes. Second, by providing consistent care, you will help your agency comply with HIPAA regulations.

Protecting health information and safeguarding it from unauthorized distribution, is just the start of providing your clients with quality care. Using the three C's-consent, computers, and communication-will help you accomplish these goals.

Often the hardest part of the job is determining TPO situations. By always obtaining a client's consent, discussing tough situations with your supervisor, and following the need-to-know the minimum-necessary principles, you should have no problem providing HIPAA-compliant client care.



Public Health
Prevent. Promote. Protect.

Steele County Public Health

Steele County Public Health
635 Florence Ave, PO Box 890
Owatonna, MN 55060
507-444-7650
Fax 507-444-7668
scphn@co.steele.mn.us

HIPAA ORIENTATION TRAINING MODULE REVIEW

NAME: _____ DATE: _____

True False

- _____ 1. PHI includes any electronic, paper, or oral data that can be used to identify a patient's health.
- _____ 2. An agency's computer-based system increases the risk of unauthorized disclosure of information.
- _____ 3. E-mails are not considered secure.
- _____ 4. Do not discuss client information with anyone who does not have a specific reason or need for the information. If a person does need the information, provide only what is necessary. These are the need-to-know and minimum necessary principles of HIPAA.
- _____ 5. Client rights are listed in the Notice of Privacy Practices. This notice is reviewed and signed by clients of Steele County Public Health.
- _____ 6. Every employee, student or volunteer is required to report any actual suspected breach of confidentiality.
- _____ 7. Every employee, student or volunteer is expected to ask questions and/or express concerns to his/her instructor/lead person.