SHIAWASSEE
Health & Wellness

HIPAA Training

A training course by Shiawassee Health & Wellness

What is HIPAA

HIPAA is an acronym that stands for Health Insurance Portability and Accountability Act.

It is a Federal Law that protects consumer's health information from people who aren't involved in the consumer's direct treatment.

HIPAA covers virtually all Protected Health Information (PHI). This includes information in any format including written, electronic, or oral.

Privacy and Confidentiality

Privacy is the right of an individual to decide how much, when, and in what manner personal information can be shared with others.

Confidentiality - As a professional you are legally and ethically required to make sure that consumer information communicated to you stays private and confidential.

What is PHI?

PHI stands for Protected Health Information and is any health information that may identify the consumer.

There are 19 identifiers and any health information that includes even one identifier is PHI and is protected by HIPAA.

19 PHI Identifiers

1. Name
2. Address
3. Dates directly related to the consumer
4. Telephone number
5. Fax number
6. Email address
7. Social Security Number
8. Medical Record Number
9. Health Plan Beneficiary Number
10. Case Number
11. Certificate/license number
12. Vehicle or device serial number
13. Web URL
14. IP Address
15. Finger or Voice Prints
16. Photographic images
17. Any other unique identifying number, characteristic or code
18. Age greater than 89
19. Genetic Information

HIPAA Privacy Rules

Consumers have the right to inspect and receive copies of their health information.

However, if a health care professional believes that the information could be harmful the consumer can be denied access.

Consumers can also request an amendment or restrictions.

HIPAA is Intended to Protect the Use and Disclosure of PHI

Disclosure means the release, transfer, or divulging in any manner of PHI to anyone outside of

Shiawassee Health & Wellness.

All disclosures require consumer authorization except the following:

Treatment (including coordination of care and referrals to other providers)

Payment (activities related to reimbursement)

Operations (training programs, accreditation, credentialing, and quality improvement activities)
When required by law (suspected abuse or neglect)

Use means the sharing of PHI within the SHW community and should follow the Minimum Necessary Rule.

Minimum Necessary Rule

The minimum necessary rule is a very simple concept: When performing a task only disclose the minimum amount of PHI necessary.

For example, it is not necessary to release a consumers address, phone number, list of medications, medical record number, and diagnosis, if the requester only needs the diagnosis.

Notice of Privacy Practices

Our Notice of Privacy Practices must be posted in a common area where consumers can see it and must also be handed out at the earliest possible appointment. Each employee should read and understand the agency's Notice of Privacy Practices.

Protecting Consumer Privacy by Employees

SHW has policies and procedures in place to make sure that all staff have appropriate access to electronic PHI to perform their jobs.

SHW is obligated to take measures to prevent inappropriate access.

All staff have the responsibility to be familiar with and follow these policies and procedures to protect PHI.

Need to Know

This requires that employees access and share private consumer information only on a “need to know” basis as part of their job duties.

Employees should only view information related to the job they are doing.

Under no circumstances should employees access a consumer’s clinical record unless they need the information to perform their job duties.

“Snooping” is against agency policy and could result in suspension or termination. SHW monitors the access of consumer clinical records on a regular basis to ensure this policy is being adhered to.

HIPAA Security Rule

The HIPAA Security Rule sets standards to specifically safeguard Electronic PHI (EPHI)

This rule covers the physical protection of the clinical records, as well as the policies and procedures regarding access to those records.

SHW must take all necessary precautions to ensure that confidential consumer information remains secure.

Administrative Safeguards require SHW to:

Adopt a written set of privacy policies and procedures

Have data back up and disaster recovery procedures

Conduct internal audits to identify potential security violations

Have a process for addressing and responding to security breaches

HIPAA Security Rule

Physical Safeguards:

The Security Rule requires that SHW implement policies and procedures to limit physical access to the paper clinical chart. We must also limit physical access to the facility in which they are housed while ensuring that authorized access is allowed.

SHW must also address workstation use including removal of information from high traffic areas and repositioning of monitor screens.

Technical Safeguards:

The Security Rule also requires that SHW implement policies and procedures to limit and control access to the electronic information systems that maintain electronic PHI (ePHI).

We must also ensure that electronic data has not been changed or erased in an unauthorized manner.

Portable Media

Portable media including USB flash or thumb drives, CD's, laptops, smart phones, and iPads, are extremely convenient but also present a tremendous security risk.

Portable devices that contain or may contain ePHI will be encrypted when possible. ePHI should only be placed on portable devices when there is a legitimate business need and when other more secure means of transporting/sending/sharing the information are not an option.

Avoid keeping PHI on portable devices that must leave the office.

If a portable device containing sensitive information is lost or stolen, report it immediately to the Privacy or Security officer.

HIPAA Security Rule

Any system is only as secure as its weakest link. In many cases a security problem can be fixed with a simple change in your own behavior or a gentle reminder to a colleague. However, if you find a problem that you cannot correct contact the Privacy or Security Officer.

There are policies and procedures in place to control physical access to sensitive equipment including computers, printers, faxes, etc.

However, be sure to keep keys and badges in a safe place and notify the Privacy or Security Officer immediately about anything that is lost or stolen.

Consumer Rights

Consumers must be given a notice of privacy practices at the first possible appointment.

Consumers may review the notice prior to signing the consent.

If consent is not obtained due to emergency or communication barriers it must be obtained as soon as feasible.

Consumers have the right to request restrictions on use and disclosure of PHI.

Consumers have the right to access and amend their PHI.

Consumers have the right to file a complaint with the Privacy Officer, the Security Officer, or the Secretary of the United States Department of Health and Human Services.

Consumers have the right to receive a list of PHI disclosed for the 6 years prior.

Best Practices for Ensuring Privacy

Only access consumer information you need to do your job – limit to minimum necessary.

Keep consumer records and other documents containing PHI out of sight.

Remove faxes containing PHI or other confidential information.

Documents with PHI must be placed in a shredding bin or shredded when no longer needed.

Do not talk about consumers in public areas or where you could be overheard.

Protect your computer with alpha-numeric passwords – you should never share or write down your password.

Best Practices for Ensuring Privacy

Do not include PHI in an email unless it is encrypted, or you are using a secure email system (SHIMER).

Log off the computer and any other open files when not in use.

Keep computer screen out of direct sight of others or use a privacy screen as necessary.

If you see any staff violating these best practices give them a helpful reminder – don't just ignore it.

If appropriate, report problems or violations to the Privacy or Security officer.

Sanctions/Enforcement

Fines/ Penalties

Fines for HIPAA violations range from $100 to $50,000 per violation and up to $1.5 million per calendar year.

Sanctions for employees breaching confidentiality range from consultation to termination, depending on the breach.

Breach Notification

If a consumer's health information is breached, SHW must do the following:

Notify the consumer within 60 days of the discovery.

Notify the media and the Secretary of Health and Human Services (HHS) if the breach involves more than 500 consumers.

If the breach involves fewer than 500 consumers, SHW must keep a log and submit it to the Secretary of HHS on an annual basis.

Notify our affiliation - MSHN (PIHP).

Identity Theft

Medical identity theft is the most common type of identity theft in our country. To prevent identity theft, the Federal Government issued the Red Flag Rule. This affects all consumers who make payments to our agency or arrange for payment to be made to our agency through an insurance company. It is a preventative measure to ensure that our consumers' identities are not being stolen.

Preemption of HIPAA Rules

According to HIPAA, health care agencies need to follow HIPAA and/or state laws, whichever is more stringent.

In the case of SHW, we follow HIPAA, 42 CFR Part 2, and the Michigan Mental Health Code to protect our consumer's privacy.

Who to Contact

If you have questions or need to report a HIPAA violation, please contact:

Privacy Officer – Nancy Fogarty - privacyofficer@shiabewell.org

Congratulations!

You have finished the materials for this course.

Remember to complete the test and survey to have this course marked as complete.