HIPAA FOR HOME HEALTH/HOME CARE

Welcome to HIPAA for Home Health!
This course is designed to get you up to speed on HIPAA compliance.

COURSE OVERVIEW AND OBJECTIVES

HIPAA stands for Health Insurance Portability and Accountability Act. It provides data privacy and security provisions for safeguarding medical information. You are responsible for two key regulations: the **Privacy Rule** and the **Security Rule**.

The **Privacy Rule** protect the privacy of all protected health information, or PHI as it's call for short, regardless of how it is stored or transmitted.

The **Security Rule** deals specifically with standard for protecting electronic copies of PHI, called ePHI. The include databases, computer files, email messages, and websites.

Let's review each lesson:

Lesson 1 - Protected Health Information
- Demonstrate an understanding of what Protected Health Information is.
- Identify if given information is PHI or not

Lesson 2 - Security Risks and Safeguards
- Demonstrate an understanding that under HIPAA, healthcare workers must prevent, detect, contain and correct security violations.
- Demonstrate how to ensure the confidentiality, integrity, and availability of electronic PHI
- Demonstrate how to comply with administrative, physical, transportation and technical safeguards

Lesson 3 - HIPAA Privacy Rule
- Demonstrate an understanding of the Privacy Rule
- Differentiate minimum PHI necessary from unnecessary disclosures
- Demonstrate confidential communication skills
- Identify cases where disclosure is allowed

Lesson 4 - HIPAA and Social Media
- Demonstrate an understanding of potential consequences of noncompliance with HIPAA regulations
- Discern what should not be shared on social media

Lesson 5 - Addressing Breaches
- Identify if given scenarios show breaches of privacy or security
- Demonstrate how to report breaches
- Demonstrate an understanding of the penalties

LESSON 1: PROTECTED HEALTH INFORMATION

The Privacy Rule defines Protect Health Information, or PHI as it's called for short, as individually identifiable health information, held or maintained by a covered entity or its business associated acting for the covered entity, that is transmitted or maintained in any form or medium.

This includes identifiable demographic and other information relating to the past, present, or future physical or mental health or condition of an individual, or the provision or payment of health care to an individual that is created or received by a health care provider, health plan, or employer. For purposes of the Privacy Rule, genetic information is considered to be health information.

PHI Categories

PHI can fall under different categories. These can help you identify PHI from non-PHI.

1. Names
2. Geographic Information
3. Dates (e.g. birth date, admission date, discharge date, date of death)
4. Telephone numbers
5. Fax numbers
6. E-mail addresses
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers

LESSON 2: SECURITY RISKS AND SAFEGUARDS

Protected Health Information (PHI) could be at risk if anyone can get access to stored information or if information can be intercepted when sent electronically.

GENERAL SECURITY STANDARDS FOR HOME HEALTH CARE

Under HIPAA you and your agency are required to do the following:

- Ensure the confidentiality, integrity, and availability of electronic PHI
- Protect against threats to the security of PHI
- Protect against any unauthorized use or disclosure of PHI

HIPAA SAFEGUARDS AND SAFETY MEASURES

HIPAA sets security standards in different categories to help you and your agency become compliant with the law.

1. ADMINISTRATIVE SAFEGUARDS

Risk Analysis

This safeguard involved looking at how PHI might be at risk

Risk Management

This safeguard includes taking step to address the risks found in the analysis.

Employee Sanction

There is punishment for staff members who do not follow security rules

Security Awareness and Training

Security Reminders

Be aware of updates on the security program at your facility

Protection from Viruses

Be aware of viruses and report any dangers you encounter. Always run your computer with antivirus software turned on.

Password Management

Create unique passwords. Change them frequently (every 59 days) and safeguard your logins and passwords. Never share them

Reporting Security Incidents

If you suspect that your password has been compromised, change the password immediately. Report suspected or known breaches of confidentiality to the Security Official.

LESSON 2: SECURITY RISKS AND SAFEGUARDS - continued

2. PHYSICAL SAFEGUARDS

Workstation Use

Follow the policies and procedures for what each type of workstation is used for. Do not use workstations improperly.

Workstation Security

Make sure that only authorized users have access to your workstation. Do not allow unauthorized personnel to use your workstation.

Tips:

- Lock hard copies, CDs, USBs and other media containing PHI in file cabinets when not in use
- Return clinical records promptly
- Keep out of sight all papers with patient information
- Shred or destroy media which contains confidential information prior to disposal
- Use fax machines, printers, copiers that are in secure areas
- Remove PHI from copiers, fax machines and printers as soon as possible

Device and Media Controls

Re-use

You must remove electronic PHI from devices or media before you reuse them.

Accountability

Follow procedures about moving hardware and electronic media such as USBs. Your agency will keep a record of where these devices are and who have them. Make sure you don't lose them or lend them to anyone.

Tablets and Phones

- Maintain control of your tablet/phone at all times while in the field
- Notify a supervisor immediately if your tablet/phone is misplaced
- If using in public to document, be aware of your surroundings and who may be able to view information on your tablet
- Never use your phone's speaker when discussing PHI
- Do not make telephone calls regarding patients in public places
- For example: Discussing with a doctor a patient's test results or condition/calling to report to a case manager

LESSON 2: SECURITY RISKS AND SAFEGUARDS - continued

3. TRANSPORTING SAFEGUARDS

You must maintain standards that are required for the safe transport of PHI.

Procedures

- Only individuals authorized by the Privacy Officer will be allowed to transport PHI outside of the agency
- An inventory of the PHI released to the individual will be taken and documented
- PHI is transported in secure carrying cases only
- Vehicles are to be locked at all times while transporting PHI secure cases. PHI secure cases are stored out of sight and/or in the trunk of the vehicle
- You must not leave the PHI unattended at any time when others are present and can access it

Tips:

- Lock travel charts in the trunk of your car when not in use
- Only have the minimum amount of PHI necessary in travel charts
- Don't talk about patients in public places
- Don't talk about patients to anyone not involved in the patient's care
- Do not use the phone in a patient's home to call other patients or discuss patients
- Only share the minimum amount of patient information necessary

4. PHYSICAL SAFEGUARDS

Log-In Monitoring

Log-in attempts and reporting discrepancies are monitored. You are not allowed to access your own ePHI or that of family, friends or coworkers. Inappropriate access to ePHI will result in disciplinary action.

Emails

- Use and manage email appropriately
- Use email resources wisely and clean out old email
- Broadcast emails require prior approval
- Do not open email from unknown senders, especially those with attachments
- Do not transmit patient/resident information via Internet email

Unique Employer Identifier (EIN)

In all electronic health transactions, employers must use their employer identification number (EIN), issued by the IRS, as their unique employer identifier.

Healthcare providers must obtain and use a National Provider Identifier (NPI). The NPI is a 10-digit number issued by the National Provider System that is used for HIPAA standardized transactions.

LESSON 3: HIPAA PRIVACY RULE

AUTHORIZATION

If you need to disclose PHI but it is not allowed by the Privacy Rule, you need to get written permission from the patient.

Written permission needs to:

- Be written in plain language
- Be specific about which information will be used or disclosed
- Specify the people who will be disclosing and receiving the information
- Have an expiration date
- Show the patient's right to revoke the permission in writing

Home health care workers should never look at PHI "just out of curiosity," even if there is no harm intended.

This applies to all people, whether they are "high profile" or a close friend or family member.

ALL information is entitled to the same protection under HIPAA and must be kept private.

MINIMUM NECESSARY

You must always disclose only the minimum amount of PHI necessary for the purpose of disclosure whenever PHI will be used.

For example, you should only disclose your patient's most recent lab results if this will achieve what is needed.

You must never disclose or use the entire medical record of a patient unless the covered entity can clearly show that it is needed to achieve the purpose of the use or disclosure.

CONFIDENTIAL COMMUNICATION

Under HIPAA, you as a covered entity have to agree to some patient requests.

For example, your patient is treated for depression but she wants to keep her treatment private. She doesn't want her insurer to know about her treatment.
Can your patient restrict disclosure to her insurer?
The answer is yes if she:

- Asks that this information be kept private
- Pays for 100% of the treatment herself 'out-of-pocket'

You, in this case, cannot disclose information. You can grant or deny the request if she does not pay 100% of the costs.

.

LESSON 3: HIPAA PRIVACY RULE - continued

DISCLOSURE OF PHI

PHI can be used or disclosed under HIPAA regulations for the purposed of:

- providing medical treatment
- processing healthcare payments
- conducting healthcare business operations
- public health purposes (as required by law)

Aside from these, PHI can only be disclosed if:

- the patient has given written permission
- it is within the scope of an employee's job duties
- proper procedures are followed for using data in research
- it is required or permitted by law

Note: the Final Rule now protects the PHI of a deceased individual for 50 years following their death.

DISCLOSURE OF PHI TO FAMILIES

You can only disclose PHI or notify family members, relatives, close personal friends and any others designated by the patient if he or she has agreed to the disclosure and has been given an opportunity to object the disclosure. If the patient is unable to object to a disclosure and, based on professional judgment and experience, it is in the patient's best interest to allow the disclosure, you may then also disclose.

NECESSARY BREACHES

Patient confidentiality is not absolute.

You may have a duty to breach patient confidentiality when there is a conflict between your patient's authority, which is their right to control their own health information, and non-maleficence, protecting the patient or others from harm.

Here are a few examples of necessary breaches:

- A patient threatens to harm themselves or others.
- The patient is a suspected victim of child abuse or neglect
- The information relates to a crime.
- The patient is a healthcare provider and has a condition that makes him or her a danger to patients.
- The patient is not fit to drive.

.

LESSON 4: HIPAA AND SOCIAL MEDIA

REAL LIFE EXAMPLES

Each year more and more health care workers are violating HIPAA rules on social media. Many commit these breaches because they don't know or understand HIPAA privacy rules and social media.

First, let's look at some examples of what not to do.

1. After a long day at work, a doctor from Rhode Island posted about it on Facebook. Afterwards she was fired from the hospital and reprimanded by the Medical Board. She never mentioned her patient's name but she wrote enough detail about the injuries that other people could guess who it was.
2. A nurse was fined $12,500 and fired after he posted a picture of his patient on Pinterest. He did it because he thought it was "funny" and there was no real harm in it since it was "only a picture".
3. A technician saw a celebrity in the waiting room and decided to tweet their name and their condition. The tech was fined $10,000 and fired.
4. A patient registrar posted his resume on LinkedIn. The resume had enough information regarding patient's conditions that they could be recognized. The registrar was fined $5,000 and fired.

Tips on using Social Media

Here are some easy-to-follow reminders on what you can do to make sure you are HIPAA compliant in social media.

- Don't talk about patients, even in general terms.
- If you wouldn't say it in the elevator, don't put it online.
- Check the tone of your social media presence.
- Don't mix your personal and professional lived on social media.
- Do not repost or share information on a patient even if they post their own information
- Encourage any patient looking for advice on social media to contact their nearest health center.
- Never take a picture of a patient without a release form, this includes taking a photo with your phone.
- Don't post patient photographs or testimonials without permission.

LESSON 5: HIPAA BREACHES

In the last lesson, you proved you're social media savvy. In lesson 5, you will need to show you can identify a HIPAA breach in the real world.

BREACH

A breach occurs when information that, by law, must be protected is lost, stolen or improperly disposed of, hacked into by people or mechanized programs that are not authorized to have access, or communicated or sent to others who have no official need to receive it.

Examples of breaches are:

- Missing hard copy of a piece of information
- Stolen device that contains PHI
- Compromised system or database of information through a "worm"
- Information from a medical record being gossiped about

REPORTING BREACHES

Part of your responsibility as a healthcare worker is to report privacy or security breaches involving PHI to your Privacy Officer immediately.

Individuals who exercise their rights under HIPAA by filing a HIPAA report or complaint may not be threatened by employees or volunteers. This includes notifying of a privacy or security breach.

PENALTIES

Statutory and regulatory penalties for breaches may include:

- Civil Penalties: $50,000 per incident up to $1.5 million per incident for violations that are not corrected, per calendar year
- Criminal Penalties: $50,000 to $250,000 in fines and up to 10 years in prison.

QUIZ

Name: _____ Date: _____ Score: _____

You might not know, but most HIPAA violations are due to health care workers not knowing that information they shared was in fact PHI. Determining PHI from non-PHI is an essential skill as a home health care worker. In this quiz you will need to show that you know what information cannot be shared either physically or electronically.

1. Identify if the following items are PHI or not.

1. Patient's ID	PHI	Not PHI
2. Patient's billing information	PHI	Not PHI
3. Patient's telephone number	PHI	Not PHI
4. Photographs of patients	PHI	Not PHI
5. Patient's email address	PHI	Not PHI
6. Fingerprints	PHI	Not PHI

2. You overhear two nurses talking about their patient's next procedure on their phones. What should you do?

a. Tell them it's against HIPAA's regulations to talk about a patient in a public place
b. Join in the conversation and gossip about the patient.
c. Mind your own business and leave them alone.

3. You hear a nurse talking to a patient's neighbor about the patient's condition. What should you do?

a. Ask the neighbor to mind his own business.
b. Nothing. The neighbor is simply asking if the patient is well.
c. Remind the nurse that she shouldn't be sharing information to anyone not related to the patient's care.

4. You received news that one of your long time patients is sick. You retrieve the patient's address on their record to send a get well card. Is this a violation of HIPAA?

a. No, you might need your patient's personal information for future contact.
b. No, a patient's address is not PHI.
c. Yes, if it's not part of your job, it is a violation.

5. You ask your supervisor about the new patient you're assigned to. The supervisor gives you a copy of the patient's complete medical records. The records include past medical information that is irrelevant to the patient's care. Is this a violation of HIPAA?

a. Yes, never give the complete medical records unless necessary.
b. No, in order to properly care for your patient, you need all the information.
c. No, it's okay because your supervisor gave it to you.

Name: _____ Date: _____ Score: _____

7. Your patient's cousin was recently admitted to the ER. Your patient and her cousin are close friends. Your patient asks you about her condition and you share it with her. Is this a violation of HIPAA?

a. No, family always gets access to medical records.
b. No, when emergency visits are involved, medical records should always be shared.
c. Yes, your patient isn't part of her care team.

8. You had a patient who has been deceased for 10 years. You share information about that patient with a coworker because you think it will help her take care of her mom who has the same condition as your former patient. Is this a violation of HIPAA?

a. No, if medical records can help save a life, you must share them.
b. No, if a patient is deceased, medical records are available to the public.
c. Yes, HIPAA protects medical records for 50 years.

9. Your patient was diagnosed with dementia. His condition has been worsening and you write to the state motor vehicle administration requesting that they evaluate if he is still fit to drive. Is this a violation of HIPAA?

a. Yes, the patient should have been asked if he could still drive or not.
b. No, reporting is the right thing to do since the patient is a threat to himself or others.
c. Yes, you should never share information about patients especially to state administrators.

10. Jessica worked with a famous movie star today and is about to tweet about it. Should she post or delete?

a. Post
b. Delete

11. HHA/CNA Jane worked with her co-worker Jessica and is about to post a photo of her at work with a patient. Should she post or delete?

a. Post
b. Delete

12. Jenny likes an app so much that she wants to share it with her Twitter followers. Should she post or delete?

a. Post
b. Delete

13. HHA/CNA Jane had a patient who is difficult to work with and she feels like venting about it online. Should she post or delete?

a. Post
b. Delete

Name: _____ Date: _____ Score: _____

14. Debbie, an HHA, unknowingly told her sister that one of her patients has Alzheimer's when she was talking about her day. Is this considered a breach?

a. Breach
b. Safe

15. Nurse Carol left a voicemail on Mrs. Harris' phone saying "Hi Mrs. Harris. Your blood transfusion is scheduled tomorrow at 2pm." Why is this a breach?

a. You're not supposed to leave a message on a voicemail. She should have waited to be able to speak with her.
b. She left a voicemail stating the name, condition and treatment of the patient.

16. Rebecca, a CNA, was moved by her patient Mrs. Lewis' situation so she created a fundraising campaign asking people to support her. She lists out Mrs. Lewis' illnesses to acquire sympathy and charity of the people online. Why is this a breach?

a. She should have let Mrs. Lewis' family create the fundraising campaign.
b. Even if it's for a good cause, medical professionals are not allowed to post or share information about a patient outside of the care team.