45 Social Media Safe Practices

TEACHING PLAN

To use this lesson for self-study, the learner should read the material, do the activity, and take the test. For group study, the leader may give each learner a copy of the learning guide and follow this teaching plan to conduct the lesson.

LEARNING OBJECTIVES

Participants will be able to:

- Explain the purpose of the Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Identify the HIPAA compliance rule of thumb
- Describe the privacy and confidentiality policies and procedures required by law
- Obey agency procedures aimed at protecting patient information
- Recognize and alleviate the information security risks posed by new technologies

ACTIVITY

Discuss with your fellow home health aides the HIPAA-compliant ways that you are able to communicate about a patient's PHI. In what situations are you tempted to discuss a patient's PHI with others, but you know the discussion may not be HIPAA compliant? What separates compliant communications from noncompliant ones? Secure and review your agency's HIPAA policies and procedures. It is very important for all HHAs to possess an understanding of those policies and procedures, which will provide clarity when it comes to tricky communication situations and will help to ensure HIPAA compliance throughout the agency.

THE LESSON

Review the material in the lesson with participants. Allow for discussion.

SOCIAL MEDIA SAFE PRACTICES

Social Media

Social media, or websites and applications that enable users to create and share content or to participate in social networking, is all around us. Most of us use some sort of social media in our private lives, and while millennials do tend to use it the most, we've all caught the social media bug. Mobile smartphones, tablets, more accessible internet and wifi, and more and more jobs that require connectivity have thrust social media upon us. Facebook, Twitter, Instagram, LinkedIn, Google+, Disqus, Snapchat, Tumblr, YouTube, Vine, WhatsApp, Meetup, Pinterest, even plain texting—the list goes on. The idea of all these applications, or apps, is to enable the average person the ability to share written or image-based information with one person or thousands with the click of a button or a swipe.

HIPAA compliance is critical and must be a prominent component within any agency's policies and procedures. All staff members, especially home health aides, who interact frequently with patients, need to familiarize themselves with the types of data considered to be protected health information (PHI) and what information requires authorization.

The rule of thumb for HIPAA compliance is the right information to the right person for the right reasons, even on (if at all) social media. HHAs who are cognizant of this rule and who vigilantly aim to adhere to it should avoid running into any HIPAA problems.

Social media gives everyone a microphone, which can be incredibly important. Social media has helped protests, has helped people in need raise money, has helped people find each other safe and sound after disaster, has helped find lost puppies, etc. Social media can be incredibly helpful. Social media can also be disastrous.

Social media gives the average person the freedom to share, and this is not always a good thing. Sharing information with an audience is a great responsibility. What do you share? You might share whatever is on your mind, whatever you might think to be of interest, maybe something for a laugh. Sharing has become so easy, it's nearly mindless. However, when you work in healthcare, you can never share mindlessly about work.

In home health, it's particularly important to be careful. You're in your personal car, often working by yourself. Not only do you feel the need to connect, but you might feel the authority to use your personal mobile device freely. You might experience things as a home health aide that astound you, anger you, sadden you, or make you laugh. It's natural to want to share stories with others; however, it's critical you don't reach for your phone. You might think you understand HIPAA and know how to post without giving details, but the risk is too great to the patient and to you. Always realize that you never truly know who will

see what you put online, and that whatever you share online can be shared by anyone, over and over again. Even if you have put your settings on any of these social media apps to be private, realize that you have still shared with someone, and it only takes sharing with one person to violate HIPAA. That person you've shared with now has information that he or she might share with others.

Social Media Provides Information You Might Not Realize

HIPAA is one of the most important pieces of federal healthcare legislation. Passed in 1996 and mandating compliance by April 2003, HIPAA requires that all healthcare workers uphold the privacy, confidentiality, and security of their patients' healthcare information. To be very clear, HIPAA can be violated through any social media app. It's also important to keep in mind that you can't take back anything you post online. Not only is there likely an actual written record of your statement or picture, but once anyone sees it, you can't make that person unsee it. Just like once you say something to someone, you can't make them un-hear it. HIPAA was created in part because of this principle—it's so critical to protect someone's privacy because once it's violated, it's ruined. There is no taking it back. Ever.

Many providers think they know HIPAA well. And while you might understand the importance of patient privacy and the main tenets of the policy, are you willing to risk your career for it?

You also might not know social media as well as you think. Is your place of employment listed on your Facebook page? Do you know that your Facebook friend is also a patient at your agency? When you took that picture, did you really get rid of identifying factors? When you post about your rough day, with a patient in his 80s who can't hear well, are you sure that your Twitter follower isn't friends with your patient, and knows the agency you work for is the same one he gets care from? You've just left too much identifying information on the table and have committed a violation of HIPAA.

A study of medical blogs written by healthcare professionals found that individual patients were described in 42% of the 271 samples studied. Of these samples, 17% were found to include enough information for patients to identify themselves or their providers, and three included recognizable photographs of the patients. If you accidentally reveal a patient's identity via social media, you and your agency could be in violation of HIPAA and would suffer severe consequences (Chretien KC, Kind T. Circulation. 2013 Apr 2; 127[13]:1413–21).

HIPAA and You

HIPAA has many rules your agency must follow. Some of those rules apply to you in your role as a home health aide. There may be penalties if you break the HIPAA rules. You could even be fined. HIPAA regulations cover many areas, but privacy of information is one of the most important for you to know about. Privacy of information means that anything you say or write about a patient must not be overheard or read by anyone unless that person has a right and a need to hear or see the information. He or she can have that right only if the patient has agreed that the person may have the information.

In a nutshell, HIPAA compliance is all about the privacy, confidentiality, and security of PHI:

- *Privacy* refers to who should and should not have access to health information. Patients have the right to privacy, meaning that information about them should be available only to people who need it to provide care.
- Confidentiality refers to preventing someone from hearing or seeing a person's private health records and information unless he or she has the proper authorization. All health information is confidential. Anyone who possesses PHI is responsible for protecting it.
- Security is the means used to provide privacy and confidentiality. The purpose of security is to ensure that only those people having authorizations may access personal health information.

HIPAA rules must be obeyed by the following public and private organizations, which are referred to as covered entities by HIPAA:

- Health plans and health insurance companies (e.g., health maintenance organizations and preferred provider organizations)
- Healthcare clearinghouses (e.g., billing services)
- Healthcare providers (e.g., doctors, dentists, chiropractors, therapists, hospitals, nursing facilities, clinics, pharmacies, hospices, and home health agencies)

KEY TERMS TO AID YOUR UNDERSTANDING

CMPs: Civil money penalties.
Confidentiality: Preventing someone from hearing or seeing a person's private health records and information unless they have the proper authorization.
Covered entity: The public and private organizations that must obey HIPAA rules.
HHS: Department of Health and Human Services.
HIPAA: Health Insurance Portability and Accountability Act of 1996.
OCR: Office for Civil Rights.
Patient consent: In signing one consent form with a provider, a patient gives permission to that provider to disclose the patient's PHI for purposes of providing care.
PHI: Protected health information.
Privacy: Information about patients should be available only to individuals who need it in order to provide care.
Security: The means used to provide patients with privacy and confidentiality when it comes to their PHI.
Specific authorization: A patient's signature is required on a specific authorization form for every instance that a covered entity seeks to use or disclose a patient's PHI for purposes not related to providing the patient with care.
Social media: Websites and applications that enable users to create and share content or to participate in social networking.

Protecting Patient Privacy

The privacy protections of HIPAA apply to all PHI, which includes:

- Information created or received by a covered entity or an employer that relates to a patient's past, present, or future health condition, health treatment, or payment for healthcare services
- Information that can identify an individual (e.g., name, address, telephone number, email address, date of birth, Social Security number, diagnosis, medical record number, employer, position, or other identifying data)
- The patient record

PHI can be in any format (e.g., paper, electronic, or oral). If a provider needs to disclose a patient's PHI for purposes of providing healthcare, the provider needs to obtain that patient's consent. Reasons for disclosing PHI include routine healthcare-related uses of the information, such as when a doctor consults with another

doctor to provide better care for an individual. If a covered entity wants to disclose a person's PHI for purposes other than providing care, the covered entity needs that person's specific authorization.

The difference between consent and specific authorization is that to give consent, a patient must sign a form. He or she needs to sign the consent only one time for each provider. The consent will apply whenever that provider discloses the patient's PHI for purposes of providing healthcare.

Specific authorization is required when a covered entity wants to use or disclose a patient's PHI for purposes not related to providing healthcare. The patient must sign an authorization form for each specific instance in that case.

The HIPAA privacy rule generally permits covered entities to disclose PHI without a patient's specific authorization in the following situations, depending on state or local law:

- Emergencies
- Public health needs (e.g., infectious disease registries)
- Mandatory reporting of child or elder abuse and neglect
- Judicial and administrative proceedings
- Substantial communication barriers

If there is no state or local law specifically requiring disclosure of information in the instances listed, covered entities are required to use professional judgment in deciding whether to disclose information and exactly how much to disclose.

A covered entity must allow a person to view and photocopy his or her own PHI if that person submits a request. An organization may charge the person for copies of records. In a few special circumstances, such as when a covered entity has compiled information for use in a civil, criminal, or administrative proceeding, that entity does not have to give a person access to his or her PHI.

A covered entity may deny a patient access to the PHI if it has reason to believe that access would create a risk of danger to that patient's health. If a patient believes that his or her PHI contains information that is incorrect, he or she may ask the covered entity to make changes. The covered entity may deny the request if it believes that the current information is accurate and complete or if it did not create the information.

Covered entities are also required to do the following:

- Notify patients about their privacy rights. This can be done by producing a clear, written explanation of how the provider may use and also disclose the patient's health information.

- Adopt written privacy procedures that clearly define who has access to protected information, how the entity will use the information, and when the entity might disclose the information to others.
- Train employees so that they are fully aware of the privacy procedures.
- Implement safeguards to prevent intentional or accidental misuse of PHI.
- Appoint an individual to make sure that employees follow the privacy procedures.
- Give an account of instances in which the entity has disclosed PHI for purposes other than treatment, payment, or healthcare operations.

HHA Confidentiality

Some patients may fear that exposure of their PHI could result in job discrimination, personal embarrassment, or the loss or denial of health insurance. Confidentiality of information, whether in written, electronic, or verbal form, is a priority. Confidentiality should extend to all health information, and you should handle all patient records as though they are confidential at all times. Do not leave them open where unauthorized people can see them.

All HHAs should learn the safeguards that their agency requires for the use, disclosure, and storage of PHI. Know your agency's privacy policies and procedures. Keep in mind that individuals have the right to know and decide who may have access to their health information and under what circumstances they may have it. Most agencies provide annual training on HIPAA rules and agency policies with mandatory attendance.

In addition, HHAs should remember the following:

- Discuss patient information only in private locations where others cannot overhear the conversation.
- A cover sheet marked "confidential" should accompany all faxed information.
- If emailing information about a patient is permitted within your agency, remove any detailed identifying information (e.g., do not refer to the patient by his or her full name; consider using the patient's initials or internal patient number).
- Only authorized personnel should enter confidential medical information into a computer-based patient record.
- Use only objective, precise language when documenting in the patient record and avoid casual remarks and abbreviations that might be misunderstood. Do not express opinions. Stick to factual information.
- Always take the utmost care to protect the privacy and confidentiality of all health information by being aware of who is around you and not allowing unauthorized people to hear or see any PHI (e.g., while at the home of patient X, do not leave patient Y's file out in the open where patient X or his family can see any of patient Y's information). In fact, never take any part of a patient record into the

home of another patient. Keep records in your car, in a covered container so nothing is visible. While in a patient's home, do not call your next patient. The first patient may well be able to figure out who you are talking from what you say, which then could provoke him to ask how Mr. Y is doing—and you cannot give patient X that information.

- Think about how you would want your PHI treated, and give your patients that much protection and more.
- While tempting, avoid posting text, pictures, or videos that have anything to do with your patients or work on any social media app. Never take photos or videos of your patient except to specifically document a finding, such as a wound or bruising. Identify the photo with only the patient internal ID number and date. Do not include the face or other identifying features. It is most advisable that you use only agency-owned equipment for patient photographs. It should be password protected and encrypted in accordance with HIPAA's technical standards. Always check your agency policy regarding taking patient photos before you use your own phone or equipment.

The Ramifications of HIPAA Violations

The OCR, an agency within the HHS, is responsible for enforcing the HIPAA privacy and security rules. One of the ways that OCR carries out this responsibility is to investigate complaints filed with it. OCR may also conduct compliance reviews to determine whether covered entities are in compliance.

OCR may take actions only on complaints that meet the following conditions:

- The alleged action must have taken place after the dates the rules took effect
- The complaint must be filed against an entity that is required by law to comply with the privacy and security rules (i.e., a covered entity)
- A complaint must allege an activity that, if proven true, would violate the privacy or security rule
- Complaints must be filed within 180 days of when the person submitting the complaint knew or should have known about the alleged violation

If OCR accepts a complaint for investigation, OCR will notify the person who filed the complaint and the covered entity named in it. Then the complainant and the covered entity are asked to present information about the incident or problem described in the complaint. OCR may request specific information from each to get an understanding of the facts. Covered entities are required by law to cooperate with complaint investigations. If a complaint describes an action that could be a violation of the criminal provision of HIPAA, OCR may refer the complaint to the Department of Justice for investigation.

OCR reviews the information, or evidence, that it gathers in each case. In some cases, it may determine that the covered entity did not violate the requirements of the privacy or security rule. If the evidence indicates

that the covered entity was not in compliance, OCR will attempt to resolve the case with the covered entity by obtaining voluntary compliance, corrective action, and/or a resolution agreement.

Most investigations are concluded to the satisfaction of OCR through these types of resolutions. OCR notifies the person who filed the complaint and the covered entity in writing of the resolution result.

If the covered entity does not take action to resolve the matter in a way that is satisfactory, OCR may decide to impose CMP on the covered entity. If CMPs are imposed, the covered entity may request a hearing in which an HHS administrative law judge decides whether the penalties are supported by the evidence in the case. Complainants do not receive a portion of CMPs collected from covered entities; the penalties are deposited in the U.S. Treasury.

Outside of HIPAA

It's also important to remember that posting your personal life might not be as personal as you think. Complaining about patients and coworkers can hurt your work life (and worse) if someone sees what you've posted and knows it's about them. Disparaging comments aimed at a coworker online can be considered cyberbullying, and pictures taken of you inappropriately using work equipment might come back to you.

Of course, it's not safe to type or take pictures while you drive. If you do, not only could you harm yourself or someone else, but you could also be violating your agency's workplace safety policy. In most states use of any keyboard while driving is a violation, subject to fine.

The Aide's Role

To say home health aides play an important role in maintaining the privacy, confidentiality, and security of their patients' PHI would be an understatement. Home health aides work very closely with patient records, information that can easily identify a patient, and patients' past and present health conditions, treatments, and payments for services rendered. Home health aides must be extremely attentive in their handling of such sensitive information for their patients' benefit but also for that of their agency. HIPAA compliance is taken very seriously. Providers can quickly find themselves in hot water due to HIPAA violations. Remember the rule of thumb: The right information to the right person for the right reasons. If home health aides abide by this rule, take care to be ever mindful of their environment and whether patients' PHI is at risk of unauthorized disclosure, and treat documentation, electronic sources, and mobile devices containing PHI like they would treat their own valuable and sensitive personal information, any and all HIPAA problems should be avoided. And most importantly, patients will receive the vigilance they deserve when it comes to their information.

Outcomes and the HHA

When home health aides understand HIPAA; retain the privacy, confidentiality, and security of their patients' PHI; and work with their agency to maintain HIPAA compliance, all outcomes are positive. A thorough understanding of the purpose of HIPAA, in conjunction with a complete grasp of their agency's HIPAA policies and procedures, will guide HHAs in virtually all situations where the wrong decision could put a patient's information at risk. Likewise, HHAs will preserve patients' confidence in the care they receive and in the quality of services provided by the agency when it is clear that HIPAA compliance is a top priority and that PHI is always handled carefully.

Your Agency's Policies

- Learn and follow your agency's policies on security and confidentiality of patient information.
- Provide information only when you are certain that the patient does not object.
- If the patient is present, ask if it is all right to discuss the information and give the patient an opportunity to say no. If the patient is not present, you will likely need to ask your supervisor whether or not you should discuss the information. The information you would disclose should be directly related to the person's need to know, and it should be a person involved in the patient's healthcare.

Case Study

Mr. Wise was recently admitted to home health following a large skin graft on his back, secondary to removal of a melanoma. There were actually two donor sites, one on his right thigh and the other his left buttock. Much skin was required to cover this large area. He is retired and lives with his brother in a third-floor walkup. He is homebound currently. It is a taxing effort for him to navigate three flights of stairs due to the placement of the donor sites.

Jane is a home health aide who has been providing assistance with personal care during the recovery. She has never seen such a large skin graft, and the bandaging itself is unlike any she had seen before: The bandage is sewn into place over the graft. There is some oozing and odor coming from the donor sites. Jane pulls out her phone and takes some photos of Mr. Wise and his wounds to show her supervisor.

After work, Jane meets her friends Betty and Sue to have an early dinner. They are home health aides, too, but work for a different agency. Jane is so excited about this new experience, she begins talking with her friends about the intriguing case she was on. She is careful not to say the patient's actual name, but she does

graphically describe the grafts, the unique dressings, and the odor and oozing. She quietly shares her photographs of the patient and his wounds.

The small restaurant is filled with patrons. You never know who might be sitting next to you!

THINK ABOUT IT

1. Clearly, Jane has committed several breaches of HIPAA laws. Even though she gives a hint of the need for privacy, write down at least three ways that she is out of compliance.
2. What would you have done differently?
3. Should she use her personal phone to take wound photographs?
4. Did she have permission to take photos? How do you know?