USING HIPAA IN THE REAL WORLD: A REVIEW FOR NURSES

INTRODUCTION

The Health Insurance Portability and Accountability Act (HIPAA) was introduced by the federal government in 1996. The original impetus for HIPAA was not what people think of today when they think of HIPAA. The HIPAA regulations were designed to: (1) ensure that patients could transfer health care coverage (the portability in HIPAA) when they changed jobs, and; (2) decrease the cost of medical records by replacing hard copy, paper records with streamlined electronic medical records that used standardized terminology and identifiers, and; (3) standardize terminology to avoid confusion and make medical records and financial transactions more uniform. HIPAA was designed in response to the growth and increasingly complicated nature of health care and the health care system. The health care system was becoming larger and more complex, it was clear that this trend was going to continue, and it was also clear that the cost and complexity of information transmission and storage was going to be enormous if the system continued to use hard copy. There were also concerns for the misuse of, and unauthorized access to electronic records so part of HIPAA outlined the responsibilities health care providers had to secure patient information that was stored and transmitted electronically.

However, these aspects of HIPAA - portability of health care coverage, cost saving, standardization of terminology, and administrative simplification - have become secondary to health care professionals who are directly involved in patient care because HIPAA has grown and been expanded. In 2001 the federal government amended HIPAA by adding the Privacy Rule and in 2003 the Security Rule was added to HIPAA, and although they may not be aware of the fact, it is the Privacy Rule and the Security Rule that nurses are referring to when they speak of HIPAA. It is those parts of HIPAA (they will be discussed in detail later in this module) that directly affect the way nurses practice and the way that health care facilities conduct business. Nurses have constant access to patients’ personal information, and health care facilities and health care providers and insurers must store and transmit patients’ personal information. In both instances, HIPAA provides guidelines for how nurses must protect the privacy of patients’ information and how health care facilities and other concerned parties must keep that information secure.

Nurses do not need to be experts in HIPAA rules and regulations. However, nurses must understand and be compliant with the HIPAA Privacy Rule and the HIPAA Security Rule. It is requirement of their job, it protects the patients, and there can be significant fines and penalties for violations of HIPAA regulations. Fortunately, although many nurses are unclear about what HIPAA allows and restricts, working within HIPAA guidelines is not difficult.

(Note: The sections of text in this module that are enclosed in quotation marks have been copied from the US Department Health and Human service website. This website has extensive information on HIPAA. The website address is provided at the end of the module. Underlining or highlighting in these sections of text was done by the author of this module).
OBJECTIVES

After completing this module, the learner will be able to

1. Identify the two components of HIPAA that directly affect nursing practice.
2. Correctly identify the term protected health information.
3. Identify the basic goal of the HIPAA Privacy Rule.
4. Identify basic rules for sharing protected health information.
5. Identify requirements for sharing protected health information.
6. Correctly identify the term covered entity.
7. Correctly identify the term notice of privacy practices.
8. Correctly identify the term incidental disclosure.
9. Identify the process for correctly sharing/transmitting protected health information.
10. Identify nursing responsibilities for maintaining information transmission and computer workstation security.

THE HIPAA PRIVACY RULE AND NURSES

The rules and regulations of HIPAA are lengthy and complex, but HIPAA is primarily concerned with the following issues.

- Notifying patients about their privacy rights and how their information can be used.
- Adopting and implementing privacy procedures.
- Training employees so that they understand the privacy procedures.
- Designating an individual to be responsible for seeing that the privacy procedures are adopted and followed.
- Securing patient records containing individually identifiable health information.

Although all parts of HIPAA affect nursing practice, the HIPAA Privacy Rule is the section of HIPAA that most directly impacts nurses in their day-to-day practice. The Privacy Rule has many aspects but the essential definition of the Privacy Rule is that a patient’s protected health information is private and confidential and must be protected.

Learning Break: HIPAA defines protected health information as health information, associated with other forms of information that could be used to identify a patient because it contains one or more identifiers such as: (1) name; (2) Social Security number; (3) telephone number, address, photographs, etc. This does not refer to information sources such as a driver’s license, but to information such as a medical record, laboratory test results, financial records associated with medical/psychiatric care, etc. that can be identified with one of the sources listed above.

Health information is any information about a patient’s current, past, or future medical or psychiatric health or health care, so in essence the HIPAA Privacy Rule requires nurses to ensure that a patient’s protected health information - any information about
medical or psychiatric health, treatment, etc. that can be identified with a specific patient - is protected.

The concept is simple: a patient’s medical and psychiatric information is personal and confidential and it must be protected. Applying this concept in the real world in real time is more complicated and can be confusing. There are many situations in health care in which nurses want to know when protected health information can be shared, how it can be shared, and with whom it can be shared. Given the complexity of clinical situations in which these questions can arise, it is not surprising that nurses may be unsure of how to apply the HIPAA Privacy Rule. However, with forethought and common sense, it is easy to be compliant with HIPAA. You can start by simply remember these points.

- Protected health information is identifiable patient information that also contains:
  (1) any information that concerns the health status of an individual; (2) any information about medical/psychiatric care that has been, is being, or will be delivered, and; (3) any information about the financial aspect of, or payment for that medical coverage. Protected health information can be electronic, verbal, or in written form.
- Protected health information can only be shared with, or transmitted to someone who has a legitimate and reasonable interest in providing treatment to a patient, ensuring patient safety, or facilitating payment for medical care. Protected health information may also be shared with or transmitted to a spouse, family members, friends, if it is reasonable to assume that the patient would not object and it is in the patient’s best interests.
- Protected health information must be shared or transmitted in ways that are safe, secure, and confidential (Some aspects of this will be outlined here, but others will be covered in the section of this module that discusses the HIPAA Security Rule).
- The patient is the final arbiter of what information is shared and/or transmitted.

The HIPPA Privacy Rule begins with patient education: the patient must be informed of her/his privacy rights regarding protected health information. Whenever a patient is to receive care, the covered entities (this will be explained later) must provide the patient with a notice or publicly display a notice that explains: (1) how the provider will use and disclose the protected health information; (2) the patient’s rights regarding use and disclosure of protected health information and information about how a patient can complain if these rights are violated; (3) the legal obligations of the covered entity regarding protected health information; (4) a statement that the covered entity is required by law to maintain the privacy of protected health information, and; (4) contact information for patients if they have questions above the privacy polices of the covered entity. (Note: A more detailed explanation of this topic can be found in the HIPAA regulations, Section 45 CFR 164.520, Notice of Privacy Practices for Protected Health Information)

Learning Break: HIPAA regulations apply to all covered entities. A covered entity is defined as: (1) a healthcare provider such as a clinic, hospital, physician’s office; (2) a healthcare plan, healthcare insurer, or: (3) a healthcare clearinghouse that processes
information for a healthcare plan. These are all considered to be covered entities, and because they transmit medical/psychiatric information about patients, claims, referrals, authorizations, or eligibility requests, they must comply with the HIPAA Privacy Rule.

The notice of privacy practice is typically given to patients when they first visit a covered entity. The HIPAA regulations state that “a covered health care provider with a direct treatment relationship with individuals make a good faith effort to obtain written acknowledgments from those individuals that they have received the provider’s notice . .” A sample of the notice of privacy practice that is given to patients is illustrated below. The sample is not complete, but it does cover the main points of a typical notice of privacy practice.

This notice describes how medical information about you may be used and disclose and how you can get access to this information. Please review it carefully.

Our Privacy Pledge
We want you to understand that we respect your privacy. Other than the necessary uses and disclosures we described above, we will not sell your health information or provide any of your health information to any outside marketing company.

Uses and Disclosures
Below you will find examples of how we may have to use or disclose your health care information:
1. Your doctor or a staff member may have to disclose your health information (up to and including all of your clinical records) to another health care provider or a hospital if it is necessary to refer you to them for diagnosis, assessment, or treatment of your health condition.
2. It may be necessary for our insurance and/or billing staff to disclose your examination and treatment records and your billing records to another party, such as an insurance carrier, your employer, a family member, other relative or close personal friend, who is involved in our care or to facilitate the payment related to your care.
3. It may be necessary for the doctor and members of the staff to use your health information, examination, and treatment records and your billing records for quality control purposes or for other administrative purposes to efficiently and effectively run our practice.
4. Your doctor and members of the practice staff may need to use your information (ex. name, address, phone number, and your clinical records) to contact you to provide appointment reminders, information about treatment alternatives, or other health related information that may be of interest to you. 164.520(b)(1)(iii)(A). If you are not at home to receive an appointment reminder, a message will be left on your answering machine.

Permitted uses and disclosures without your consent or authorization
Under federal law, we are also permitted or required to use or disclose your health information without your consent or authorization in these following circumstances:

1. If we are providing services to you based on the orders of another health care provider.
2. If we provide health care services to you in an emergency or disaster relief situation.
3. If we are required by law to treat you and we are unable to obtain your consent after attempting to do so.
4. If we are provide health care services to you as a result of a Workers’ Compensation injury.
5. If you are/ were a member of the armed forces, we are required by military command authorities to release your health information.
6. If we provide health care services to you as an inmate.
7. If there are substantial barriers to communicating with you, but in our professional judgment we believe that you intend for us to provide care.

Other than the circumstances described in the above examples, any other use or disclosure of your health information will only be made with your written consent.

Your right to revoke your authorization
You may revoke (take away) your privacy release authorization from us at any time; however, your revocation must be in writing. You can call for information about revoking your authorization during normal business hours, or send your request to the address listed below. There are two circumstances under which we will not be able to honor your revocation request.

1. If we have already released your health information before we received your request to revoke your authorization. 164.508(b)(5)(i).
2. If you were required to give your authorization as a condition of obtaining insurance, the insurance company may have a right to your health information if they decide to contest any of your claims. If you wish to revoke your authorization, please write to us.

Our Duties
We are required by law to maintain the privacy of your health information. We are also required to provide you with this notice of our legal duties and our privacy practices with respect to your health information.

We must abide by the terms of this notice while it is in effect. However, we reserve the right to change the terms of our privacy notices. If we make a change in our privacy terms the change will apply for all of our health information in our files.

The notice of privacy practices must be given to each patient (or prominently displayed), but the HIPAA regulations recognize that there can and will be exceptions. For example, the HIPAA Privacy Rule states that: “Hospitals and other covered health
care providers with a direct treatment relationship with individuals are not required to provide their notices to patients at the time they are providing emergency treatment. In these situations, the HIPAA Privacy Rule requires only that providers give patients a notice when it is practical to do so after the emergency situation has ended,” and in the case of children the HIPAA Privacy Rule states that: “In cases where the individual has a personal representative, as is generally the case when a parent brings a child in for treatment, the provider satisfies the notice distribution requirements by providing the notice to the personal representative (e.g., the child’s parent), and making a good faith effort to obtain the personal representative’s acknowledgment of the notice.”

**Working with the HIPAA Privacy Rule in the Real World**

The issues that arise with the HIPAA Privacy Rule and nursing practice do not often involve nurses identifying protected health information: issues arise most often when nurses are not sure of when and to whom they can disclose and/or transmit information. The HIPAA regulations are admittedly lengthy and understanding how to comply with the Privacy Rule can seem daunting at first, but it is actually simple if you follow this three-step process.

1. Identify what it and what is not, protected health information.

2. Determine if the person or entity who is requesting the information have a legitimate need for the information.

3. If need be, make a reasonable effort to identify the person or entity that is requesting the information.

The second and third steps are often the sticking points and the source of confusion. But you will be complaint with HIPAA if you understand that: (1) protected health information can only be shared with or transmitted to someone who has a legitimate and reasonable interest in providing treatment to a patient, ensuring patient safety, or facilitating payment for medical care. Protected health information may also be shared with or transmitted to a spouse, family members, friends, if it is reasonable to assume that the patient would not object and it is in the patient’s best interests, and; (2) HIPAA requires you to make a reasonable effort to identify the person or the covered entity to whoever you will be transmitting/sharing protected health information.

So if you are not sure if you can share protected health information with the person or covered entity that is requesting the information, ask yourself two questions: (1) does the person or entity requesting the information or the person to whom the information will be given have a legitimate need for that information, and; (2) have you made a reasonable effort to identify that person or entity? The following examples illustrate these points.

**Example:** You are caring for a patient who had a surgical procedure that morning. Someone calls, identifies herself as a surgical resident who had assisted in the operation, and asks for an update on the patient’s condition. You do not know the physician. Should you provide the caller with information about the patient’s condition? **Answer:** Yes. The
surgeon certainly has a legitimate need to know, and it is very unlikely that the person calling is not who she says she is, but prudence will require the nurse to ask a few simple questions, e.g., who was the surgeon who performed the operation, how long did the procedure, etc. in order to have a reasonable assumption that you are talking to one of the assisting surgeons.

**Example:** You are working in a busy, crowded emergency room. You must discuss test results and a plan for medication administration with a patient, but this simply cannot be done out of earshot of other patients. Would discussing this information - and having other patients hear it - be a HIPAA violation? **Answer:** No. When a clinical situation is such that protected health information that is shared or transmitted can be overheard or accessed by someone who does not have a legitimate need for the information, and there is no reasonable way to avoid this, this situation is called an *incidental disclosure* and “The HIPAA Privacy Rule does not require that all risk of incidental use or disclosure be eliminated to satisfy its standards. Rather, the Rule requires only that covered entities implement reasonable safeguards to limit incidental uses or disclosures.” The HIPAA regulations recognize the realities of health care.

**Example:** A nurse receives a telephone call from someone who identifies himself as a patient’s son. The caller lives in another country, he has not and cannot come to see the patient, and would like to know about the patient’s condition. Should the nurse release this information? **Answer:** Yes. The son certainly has a legitimate need to know, and if the nurse can make a reasonable effort to identify him, the nurse can provide the caller with an update. The simplest solution would be to ask the patient to help you identify his son. If the patient cannot help, the nurse could offer to call another family member she does know and provide the update to that person; that family member can then call the son. There are many easy and simple ways to resolve this situation. “The HIPAA Privacy Rule at 45 CFR 164.510(b) specifically permits covered entities to share information that is directly relevant to the involvement of a spouse, family members, friends, or other persons identified by a patient, in the patient’s care or payment for health care.”

**Example:** You are caring for a patient who has tuberculosis. You overhear a physician discussing the patient’s case with someone from the local health department, and you know that the patient has not been told that the public health department will be informed of his condition. Has the physician committed a HIPAA violation? **Answer:** No. The HIPAA Privacy Rule does not require patient consent or require the patient to be informed when information about a reportable disease is shared. ” All States have laws that require providers to report cases of specific diseases to public health officials. The HIPAA Privacy Rule permits disclosures that are required by law. Furthermore, disclosures to public health authorities that are authorized by law to collect or receive information for public health purposes are also permissible under the Privacy Rule.”

**Example:** You are working in a clinic and someone comes in to pick up a prescription. That person says he is a relative, an uncle, of a patient who was seen in the clinic the day before. Test results that were recently returned indicate that the patient has an infection, and the physician has prescribed an antibiotic. Should you give the prescription to this
person? **Answer:** Yes. “HIPAA allows health care providers to use professional judgment and experience to decide if it is in the patient’s best interest to allow another person to pick up a prescription, medical supplies, X-rays, or other similar forms of information for the patient. For example, the fact that a relative or friend arrives at a pharmacy and asks to pick up a specific prescription for a patient effectively verifies that he or she is involved in the patient’s care. HIPAA allows the pharmacist to give the filled prescription to the relative or friend.” As always, the operative words in these situations, according to HIPAA, are professional judgment and experience and the patient’s best interest. You would also make a reasonable attempt to verify who this person is and his relationship to the patient.

**Example:** Two nurses are in an elevator on their way to the cafeteria, and they are discussing a patient’s condition. There are other nurses and several members of the public in the elevator. They do not identify the patient by name, but they do talk about several very specific details of the case. Is this HIPAA violation? **Answer:** Yes. This would not be considered a protected, incidental disclosure as there is no need to discuss the patient’s condition in that place and at that time and although they did not mention the patient’s name, they did mention details of her case that could identify her.

**Example:** A nurse working in an ICU is caring for a patient who has taken an overdose of prescription medication. The patient’s condition is stable. You receive a telephone call from someone who says he is calling from the local Poison Control Center. He tells you his name and says that the Poison Control Center was consulted on this case by the emergency room physician, and he would like to get an update on the patient’s condition. You have never discussed a case with the Poison Control Center and you do not know the caller. Should you give him this information? **Answer:** Yes. The Poison Control Center obviously has a legitimate need to know. However, given the circumstances the nurse should make a reasonable effort to identify the caller. The nurse can: (1) check the telephone number the caller is using: almost every Poison Control Center has the same 1-800-222-1222 number; (2) check the chart to see if contact with the Poison Control Center was documented by the ER physician; (3) ask your co-workers if they recognize the caller; (4) get his telephone number and call him back, or; (5) most Poison Control centers have a form that can be faxed that identifies and outlines their relationship with the hospitals they serve.

**Example:** A physician asks you to call a patient at home and tell the patient that her prescription is ready. You make the call, but the patient is not at home, and someone who identifies himself as her husband asks you to give him this information. You have never met the patient’s husband. Is it acceptable to give this person the message? **Answer:** Yes. “A covered entity also may leave a message with a family member or other person who answers the phone when the patient is not home. The Privacy Rule permits covered entities to disclose limited information to family members, friends, or other persons regarding an individual’s care, even when the individual is not present. However, covered entities should use professional judgment to assure that such disclosures are in the best interest of the individual and limit the information disclosed.” A reasonable approach in this situation would be to make sure you have dialed the correct number, ask one or two
easy questions that would confirm that the person who answered is very likely the patient’s husband, and then simply tell him that the patient’s prescription is ready. If he asks what the prescription is and what it is used for, the most sensible action would be to advise the husband to discuss these questions with his wife.

The US Department of Health and Human Services website has a section about HIPAA that covers basic information about the HIPAA Privacy Rule, and it includes an extensive and comprehensive list of Frequently Asked Questions that deal with “real life” examples of using HIPAA and how to work with the HIPAA Privacy rule. These can be accessed when needed, but if you feel pressed for an immediate answer, the guiding principles are: a legitimate need to know, a reasonable attempt to identify the person/entity who is requesting information, and common sense. If you keep these principles in mind it is easy to be compliant with the requirements of the HIPAA Privacy Rule.

THE HIPAA SECURITY RULE AND NURSES

The HIPAA Security Rule is the second part of HIPAA that can affect nursing practice. The HIPAA Privacy Rule provides a general outline of what you must do to safeguard protected health information: the HIPAA Security Rule provides much more specific guidance on how to safeguard this information. “The HIPAA Security Rule establishes national standards to protect individuals’ electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.”

Nurses are not responsible for installation, maintenance, etc. of the administrative, physical and technical safeguards used to ensure the confidentiality and security of protected health information, but they are constantly transmitting and receiving written and electronic information about their patients. In order to be compliant with HIPAA Security Rule requirements, this information must be handled correctly and for nurses this means that the physical safeguards used to protect health information must be understood and used correctly. Doing so is relatively simple and involves: (1) information transmission; (2) computer work station security, and; disposal of protected health information.

Information Transmission

Concerns for safeguarding protected health information during transmission occur when the information is faxed, mailed, discussed verbally, or sent via the telephone or electronically. All of these are permissible: “The Privacy Rule allows covered health care providers to share protected health information for treatment purposes without patient authorization, as long as they use reasonable safeguards when doing so. These treatment communications may occur orally or in writing, by phone, fax, e-mail, or otherwise.”
• Faxing: “When faxing protected health information to a telephone number that is not regularly used, a reasonable safeguard would be to first confirm the fax number with the intended recipient. Similarly, a covered entity may pre-program frequently used numbers directly into the fax machine to avoid misdirecting the information.” If you are faxing protected information, you should make a reasonable attempt to confirm receipt, and you should make a reasonable attempt to make sure that the fax is properly disposed of or stored as soon as it has been transmitted. If you do not have time to dispose of or store the fax, place it somewhere secure until you can.

• Mail: Confirm the correct mailing address and after an appropriate period of time confirm receipt of the material.

• Email: Confirm the correct email address ad if needed, confirm receipt of the email you sent. “The Security Rule does not expressly prohibit the use of email for sending e-PHI. However, the standards for access control (45 CFR § 164.312(a)), integrity (45 CFR § 164.312(c)(1)), and transmission security (45 CFR § 164.312(e)(1)) require covered entities to implement policies and procedures to restrict access to, protect the integrity of, and guard against unauthorized access to e-PHI.” These procedures for restricting access and protecting against unauthorized access can and do involve nurses, and they will be discussed later in the module.

• Telephone: Confirm the telephone number and the identity of the person you are speaking with. If you must use the telephone and privacy is not possible, lower your voice and try to avoid, as much as possible, using information that bystanders could use to identify the person you are calling and the clinical situation you are discussing.

• Texting: Texting can be used to transmit protected health information, but you must check with the HIPAA privacy/compliance officer at your work place for directions about how to do so securely, and you must use approved devices and protocols. Using a text message also requires all of the normal safeguards such as confirming receipt of the message, making sure you are sending the message to the right person, and only texting when you can be sure that unauthorized people cannot read what you are texting.

**Computer Work Station Security**

Enormous amounts of protected health information is accessed, stored, and transmitted electronically. As mentioned previously, the “The Security Rule . . . requires covered entities to implement policies and procedures to restrict access to, protect the integrity of, and guard against unauthorized access to e-PHI.” Installation and maintenance of electronic safeguards and the technical requirements for safeguarding protected health information are the responsibility of the covered entity, but nurses are interfacing with these computer resources all the time and must use them correctly to be compliant with the HIPAA Security Rule. Fortunately, doing so is simple.

• A computer screen should never be made visible to anyone not involved with patient care.
• You should always “hide” a computer screen that has patient information on it if you must interrupt data entry.
• Never share your password with anyone.
• Log off when you are finished with the computer.

Nurses do not need sophisticated information about computer systems or computer security to be compliant with the HIPAA Security Rule. The four common sense points listed above are, essentially, all you need to know to provide computer work station security.

SUGGESTED READING

