HIPAA RULES AND REGULATIONS

INTRODUCTION

Everyone who works in or around health care has heard about the HIPAA, the Health Insurance Portability and Accountability Act. And certainly, everyone who is in the health care field has received printed material about HIPAA, has attended lectures about HIPAA, or attended mandatory education sessions that are designed to help staff understand how HIPAA affects the way they do their job.

However, even though the federal legislation that enacted HIPAA was passed in 1996, many health care professionals are still unsure about exactly what HIPAA is, what it requires, and how HIPAA rules and regulations affect their practice on a day-to-day basis.

When you are working as a Certified Nursing Assistant (CNA), you will definitely be responsible for understanding and using some parts of HIPAA. HIPAA may initially seem complicated, but the practical applications of HIPAA are not really all that difficult, and once you understand the three major concerns of HIPAA – privacy, security, and administrative simplification – then HIPAA and the role it plays in your working day becomes clear.

OBJECTIVES

When the student has finished this module, he/she will be able to:

1. Identify the basic goal of HIPAA.
2. Identify the three parts of HIPAA.
3. Identify what the privacy section of HIPAA is concerned with.
4. Identify your responsibility as it relates to the privacy section of HIPAA.
5. Identify what the security section of HIPAA is concerned with.
6. Identify your responsibility as it relates to the security section of HIPAA.
7. Identify two resources you can use to answer questions about HIPAA.
8. Identify a definition of protected health information.
9. Identify two rules for protecting patient privacy at computer work stations.
10. Identify to whom and when you can disclose patient information.

THE HISTORY AND FORMATION OF HIPAA

The HIPAA legislation was enacted in 1996. Many people do not know that the original HIPAA legislation had two parts. The first part was concerned with making sure that health care coverage was available to workers and their families when an employee changed or lost his/her job.

The other part of the HIPAA legislation, the part that concerns and affects health care professionals, was generated in response to the growing use of electronic records and the increasing size and complexity of the health care system. It was becoming clear that with the change in the way information was generated, transmitted, and stored in hospitals, health care facilities, physician’s offices, etc., that there was big potential for loss of
privacy, and misuse, abuse, and theft of patient information. It was also obvious that it was time for national standards that clearly outlined how confidential medical information should be handled. So, in response to those concerns, the HIPAA legislation was created and put into place. The basic goal of this part of HIPAA is to protect a patient’s privacy.

THE THREE PARTS OF HIPAA

It was mentioned in the introduction that HIPAA is concerned with three basic issues. Although each of these issues – privacy, security, and administrative simplification – will be covered separately, don’t forget that they are interdependent and are designed to work together to protect patient confidentiality.

PRIVACY

Privacy is the easiest part of HIPAA to understand. We have all been taught and socialized that there is information that is considered private. Someone’s personal finances, details about his/her personal life or religious beliefs – this is information that can only be accessed if that person decides to share it or allows it to be shared, and information about someone’s health and/or medical history is no different.

The privacy section of HIPAA is the rules and regulations that specify how and when health care facilities, health care professionals, employers, and health insurance companies (these are collectively called “covered entities” in the HIPAA regulations) can use and disclose protected health information.

Learning Break: Protected health information a) is any information that concerns the health status of an individual, b) any information about medical care that has been delivered, and c) any information about the financial aspect of, or payment for that medical coverage. Some examples of protected health information are obvious: social security number, address, date of birth, diagnosis, medical record number, etc.

The privacy concerns of HIPAA allows covered entities to share protected health information verbally, in writing, or electronically with another covered entity and its employees if this sharing is for the purposes of providing treatment to a patient, ensuring patient safety, or facilitating payment for medical care. The privacy concerns specify that covered entities must keep track of how they use protected health information, document how they use it, and tell individuals how their protected health information is being used. The covered entities are required to have written privacy policies and procedures, and these must be shared with the patient at the patient’s request.

There are also parts of the privacy section of HIPAA that give the patient the right to ask covered entities how his/her protected health information has been used and who has viewed it, and it allows an individual the right to file a compliant with the Department of Health and Human services if he/she feels that a privacy violation has occurred.
Summary

The privacy section of HIPAA can seem complex and confusing, and it does contain a lot of information. However, when working with HIPAA on the job, much of the privacy rules and regulations do come down to common sense. The best way to summarize and remember the privacy aspect of HIPAA is this: As a healthcare professional, you must make sure that a patient’s protected health information is only shared with the appropriate people in an appropriate way. Since the sharing of protected health information can only be done for the purposes of providing treatment to a patient, ensuring patient safety, or facilitating payment for medical care, it is very obvious, when you stop and think about it, who can be told what about whom, and when, where, and how this information can be shared. In addition, a patient’s protected health information should only be shared if he/she has expressed permission that it is okay to do so.

SECURITY

The security part of HIPAA and the privacy section are closely related, but the privacy section outlines in general terms how to handle patients’ protected health information that is written or electronic form. The security section is concerned with electronic protected health information, and it outlines specific security safeguards that must be used by covered entities in order to keep this information safe and make sure it is used appropriately. The privacy section of HIPAA tells you what to do and the security section tells you how to do it.

These security safeguards are:

- Administrative safeguards: Administrative safeguards are the policies and procedures that covered entities must have in order to safeguard protected health information. For example, this part of the security aspect of HIPAA dictates that covered entities must have a HIPAA privacy officer, they must have an emergency plan in case the security of the protected health information is compromised, they must clearly identify which employees are allowed to access protected health information, etc. In order to be “HIPPA compliant,” a covered entity must have written documented plans that address how it handles information security.

- Physical safeguards: Physical safeguards are measures that are used to physically control access to protected health information. Examples: The electronic health information and the computer system that stores and transmits it must be closely monitored, access privileges to the computer clearly outlined and closely monitored, and workstation security must be ensured.

- Technical safeguards: The technical safeguards are, in large part, the responsibility of the computer professionals of each covered entity. HIPAA requires, among many other things, that the computer system of each
covered entity be safe and secure from intrusion, have appropriate back-up systems, have procedures in place for safe information storage, retrieval, and transmission, and any changes in the system be documented. This part of the security aspect of HIPAA is not typically something that concerns someone involved in direct patient. However, health care professionals do need to be aware that electronic information systems can be compromised and can break down. These problems can affect patient privacy, so if you notice something wrong with the system you are working with, notify the appropriate person right away.

Summary

The HIPAA privacy section outlines what needs to be done to safeguard protected health information, and the HIPAA security section tells us how to do it. The most important responsibility you have regarding HIPAA security is to understand the physical safeguards required for using a computer system that stores and transmits protected health information. In order to be compliant with HIPAA rules and regulations, you must understand how to use a computer system and a computer workstation so that protected health information stays safe.

ADMINISTRATIVE SIMPLIFICATION

The administrative simplification section of HIPAA involves a national standard for electronically transmitting information and a series of standard codes that covered entities must use to identify diagnoses, diseases, injuries, and other medical conditions. It also established a uniform system of electronic information exchange about the financial aspects of patient care. Administrative simplification is intended to streamline and standardize the administrative and financial aspects of providing care.

Summary

Certified nursing assistants are direct care providers. The administrative simplification section of HIPAA will not, for the most part, affect how CNAs work. The only possible effect administrative simplification would have for direct care providers would changes in forms, data gathering processes, etc.

USING HIPAA IN THE WORKPLACE

Understanding the different parts of HIPAA is important and it is the first step to using HIPAA. But the obvious question that everyone has is how does HIPAA change the way I work? What sorts of activities does HIPAA allow and what does it prohibit? Am I obeying – or disobeying – HIPAA regulations if I discuss a patient’s condition with his/her family? Do HIPAA regulations mean that a patient cannot call his/her physician’s office to obtain laboratory test results? Am I violating HIPAA regulations if I call a patient by name in front of other people in a busy waiting room? When you think about what HIPAA means, using it can begin to seem very complicated.
Fortunately, actually using HIPAA is not that hard. All covered entities should have a HIPAA information manual you can refer to, and there should also be a staff member who is a HIPAA resource. So if you have a question about HIPAA, you can look up the answer or ask the HIPAA resource staff person.

More importantly, although there are many “do’s and don’ts” of HIPAA, **if you remember the following two statements, you will always understand what you should and should not do with protected health information.**

- Protected health information is information that would reasonably be considered private.
- Protected health information should only be shared with appropriate people in an appropriate way and in an appropriate place.

Remember, HIPAA governs what you write and what you send through a computer, but HIPAA also governs what you say.

**HIPAA IN THE REAL WORLD**

The following scenarios provide examples of using HIPAA in the ‘real world,’” and they are situations that you will most likely encounter.

**Scenario #1:** A patient informs you that he has tuberculosis, but he has not told his physician or anyone else. You decide not to tell anyone because the patient did not give you permission to do so and this is information that would reasonably be considered private. Right or wrong?

**Answer:** Wrong. You are correct that this information is private, that protected health information should only be shared if the patient has given permission, and it should only be shared with the appropriate people. However, there are exceptions to this rule. If the patient has a criminal wound, a gunshot, is a victim of abuse, or has certain communicable diseases, this information can be divulged to public health agencies or appropriate care givers.

**Learning Break:** Should you inform public health agencies or another health care provider if your patient is HIV positive but has not disclosed this fact? No. All health care providers should use universal precautions and these will prevent transmission of HIV, so it is usually not necessary to know a patient’s HIV status. However, tuberculosis is transmitted by infected droplets coughed or exhaled into the air. Wearing a face mask is not part of universal precautions, so if the patient does not divulge the fact that he has tuberculosis, he is putting health care personnel and people in the community at risk without their permission. Use HIPAA, but use your common sense.

**Scenario #2:** You are working at workstation entering information into a patient’s chart. The computer screen is facing away from the hall, but glare from a window reflects on the screen. This makes reading the screen difficult so you turn it around. Then,
someone asks you to assist with moving a patient out of bed, so you leave your note unfinished to go help. Right or wrong?

**Answer:** Wrong. A computer screen should never be made visible to anyone not involved with patient care, and you should always “hide” a computer screen that has patient information on it if you must interrupt data entry. Other important rules for using computers that involve HIPAA: never share your password with anyone, and always log off when you are finished with the computer.

**Scenario #3:** You notice that fax containing laboratory results has been transmitted. You are going to place in a file, but you must answer a call light so you set it down on the desk. When you return, you realize that the same laboratory results are in the electronic record, so you throw the fax in the trash. Right or wrong?

**Answer:** Wrong. If you don’t have time to properly file the fax, place it face down where it won’t be noticed. If the fax isn’t needed, place it in a shredder.

**Scenario #4:** You are in an elevator with a co-worker. One of your patients was just diagnosed with cancer, and you are discussing the patient’s condition – without using her name – so although there are other people are in the elevator, you feel secure. Right or wrong?

**Answer:** Wrong. Never discuss protected health information unless you are sure that only appropriate people can hear the conversation.

**Scenario #5:** Someone stops you in the hall and asks a question about the medical condition of one the patients you are caring for. This is the first time you have cared for this patient, but you have seen this person visiting the patient several times a day in the past week, so you give him a quick summary of the patient’s health. Right or wrong?

**Answer:** Wrong. This person is probably a relative or a friend, but he could be anyone; you don’t know. The patient is the one who decides who can have access to his/her protected health information, so in this situation you would have to check with the patient first. Protected health information can be disclosed to someone if the patient has agreed, if the person receiving the information is involved in some way in the patient’s care, and if the information is needed for that person to be involved in the patient’s care.