CLINICAL SOLUTIONS

Medical Education Training Centers

2 Hour CEU

Course Objectives

The purpose of this program is to provide nurses with information about the Health Insurance Portability and Accountability Act (HIPAA), especially as it relates to protected health information.

After studying the information presented here, you will be able to:

Describe the intent of HIPAA

Describe various professional practices that protect patients' privacy

Discuss practices that protect security of electronic protected health information

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is a federal regulation that requires health care providers and entities to ensure the protection, privacy, and security of patients' medical information. Originally, the act addressed insurance coverage for workers and their families when they

changed or lost their jobs. Since 1996, HIPAA has implemented regulations that govern security, the last and final component, implemented on February 13,2003. This final rule adopts standards for the security of electronic healthy information with the primary goal being the confidentiality, integrity, and availability of health information. Compliance with the security standards is due by April 21, 2005 (Security Standards). HIPAA violations carry both civil and criminal penalties that include fines and imprisonment. The fines can range from $100 for each violation of the law to a limit of $25,000 per year for multiple violations. For knowingly misusing or disclosing patient information, criminal sanctions carry fines of 50,000 to 250,000 and one to ten years imprisonment.

Although everyone in a health care organization is responsible for complying with HIPAA regulations, there is usually one person or department responsible for organizing, implementing, and checking

compliance. Since the regulation does not state who specifically should manage HIPAA responsibilities, the person or department having this role varies based on the decision of the organization. Most often, however, it is a Chief Privacy Officer or other designated health care security professional skilled in understanding the overall regulation requirements who assists and guides the organization towards compliance. Responsibilities of the HIPAA professional are to facilitate compliance with patient privacy and confidentiality regulations by performing periodic surveys and assessments and by examining ways in which the regulation will change current organizational practices. Thus, this designated professional may be responsible for revising policies, procedures, and processes to comply with the regulation, as well as making staff aware of changes and educating them on new procedures. The HIPAA regulation that is concerned with the security of health information focuses on three components: administrative, physical,

and technical safeguards. . Administrative safeguards are actions, policies and procedures, and activities to manage the selection, development, implementation, and maintenance of security measures to protect health information. Many health care facilities will have administrative policies outlining standards and actions employees should take when dealing with patient information and confidentiality. Physical safeguards are measures to protect the organization's electronic information systems, related buildings, and equipment from environmental hazards and unauthorized intrusions. The physical regulation also includes disposing of electronic information. For example; a physician who writes a note regarding patient status incorrectly may decide to rewrite the note. There are specific steps to take when deciding to discard the previous note. The third component of HIPAA security standards is the technical safeguards. The technical components address the policies and procedures for the use of technology, protect electronic

health information, and control access to records. Many institutions have computer software, which is password protected by each user of the technology. A trail may be established and only those individuals with a need to know should be allowed access.

Each of the following issues as they pertain to that provider must be addressed in the notice of privacy practices.

1. Access to medical records. HIPAA protects a patient's right to view the medical record upon request and to obtain a copy. The notice of privacy practices must explain clearly to patients their right to access their own medical record and how to do so, whom to call, and what forms to use in that facility.

2. Amendments to medical records. Patients have the right to request a change in their medical record. Information on what forms to use, what process to follow, how long it will take, and who will manage the process are included in the notice. A health care facility is not obligated to agree to a request for a change, but the

privacy officer is obligated to consider the request and notify the patient of the final decision.

3. Restrictions on the use of protected health information. HIPAA defines the right of patients to restrict the use of their protected health information as long as the restriction does not interfere with activities related to treatment, payment, or operations.

4. Access to an accounting. Patients have a right to know who has been given access to their protected health information. Health care facilities must be able to produce for patients a list of people, companies, or agencies that have received protected health information. If the sharing has taken place in order to implement treatment, collect payment, or otherwise maintain operations, the accounting need not include those transactions.

5. Confidential communications. HIPAA defines the patient's right to request that communications about protected health

information be delivered in such a way that the sender remains anonymous and the information protected. For example, a patient may request that mailed information be placed in envelopes without a return address or in envelopes instead of on postcards.

6. Complaints about violations of privacy. The notice of privacy practices explains to patients how to file complaints about possible violations of privacy. The notice identifies the facility's privacy officer and offers guidance about how to contact the officer and what to expect in response. HIPAA requires facilities to establish a procedure for receiving, assessing, and responding to complaints about violations of client confidentiality. The notice also includes information to guide the patient in contacting the Department of Health and Human Services, the federal agency that oversees HIPAA. The department may investigate and has the power to fine providers who have violated HIPAA.

Security

The goal of the security rules of HIPAA is to establish standard protections for the electronic (computerized) storage and transmission of protected health information. The rules are guided by three main principals: protection of the confidentiality of information, the protection of the integrity (wholeness) of the information, and the continued availability of the information. Compliance with these rules falls in large part to professionals who maintain computer systems for health care organizations.

HIPAA requires health care institutions to identify a security officer who establishes policies and practices that meet minimum standards of information security. Such common practices as password protections on computers that store patient care information are required under HIPAA rules of security. The security officer also oversees creation of procedures that protect electronic information

in the event of disaster, including the continual physical security of hardware as well as software.

The effectiveness of security practices depends on your understanding and cooperation. Your computer sign-on code, for example, is a cornerstone of a secure health information system. Your security officer, in addition to setting up the password system, is responsible for providing education for you and for all employees about safe practices that ensure the confidentiality, integrity, and continued availability of critical health care information. Whenever you begin work at a new facility, you can expect to hear about that facility's practices to ensure a secure health information system.

The "minimum necessary" rule. The "minimum necessary" rule can help you make on-the-spot decisions about whether to share or

discuss a client's protected health information. The rule guides providers to use only the minimum amount of information necessary to get the job done. For example, if you order a wheelchair for a client, you might need to share information about the physical characteristics of the patient, such as height and weight. But the actual diagnosis of the patient is not necessary in order for the correct wheelchair to be delivered. The patient may have become nonambulatory because of brain abscesses resulting from AIDS, for example, but the vendor doesn't have to know the patient's HIV status in order to provide the right wheelchair.

Telephone requests for personal health information. Inpatient nurses are familiar with the privacy issues that arise when telephone inquiries come into the nurses station. How can a nurse or clerk be sure of the identity of a caller who asks about a patient? What is the best way to support the family and loved ones of patients while still

protecting patients' confidentiality? HIPAA suggests that when a caller asks for a patient, the provider can verify whether that person is in the hospital, but only if the caller asks for the patient by name. If a caller asks for specific information about a patient, only minimal information about general status should be communicated. The caller can be directed to speak to the patient or family for any further details. If the caller asks for a list of patients or for a broad category ("Do you have any of the schoolchildren involved in the accident?"), the nurse or clerk should not respond in any detail. An exception to this rule would be a member of the clergy who calls asking, for example, for all people who indicate a certain faith preference at the time of admission. A second exception would be a patient who specifically requests anonymity upon admission. The privacy officer will establish a system of notification in the patient rosters to alert all employees to this special status.

E-mail and faxes. E-mail and faxes are convenient, but information can be sent to the wrong destination without the sender being aware of it. To reduce the vulnerability of accidental error in identifying the recipient, e-mails and faxes that contain protected health information should have a disclaimer explaining the confidential nature of the information included in the transmission. The disclaimer should explain how to reach the sender to notify the sender of any errors. The "minimum necessary" rule is relevant to e-mails and faxes as an added level of security.

The discarding of protected health information. Often in busy health care settings, protected health information appears on documents that do not end up in the medical record. Patient assignment lists, unused labels, notes taken at change of shift—all these documents represent a potential source for violation of privacy. HIPAA does not directly address this type of privacy

violation, but many facilities take steps to guard against it. At some facilities, these documents are discarded in special locations or sent to a shredder. You should ask your employer how to handle the safe disposal of any documents containing protected health information.

Hallway conversations. Talking about patient information in public places is problematic. Although HIPAA does not address this problem specifically, its privacy principles reinforce the professional commitment to use care in such situations to avoid unintentional disclosure of information. Talking in elevators, discussing a case over lunch, discussing a difficult situation with friends over dinner, all of these situations raise the possibility that a client's protected health information will be revealed inappropriately. Certainly, professionals may discuss, and should discuss, difficult situations in a healthy atmosphere of learning and problem solving. Again, the "minimum necessary" rule will help to guide these discussions.

Remembering to delete identifying information when possible, exchanging only enough information to further the discussion, and holding such conversations away from busy public places will improve the ability to protect patient confidentiality.

Computer passwords. Your computer password is key to the security of electronic protected health information. You should never give out your password or write it down. If someone asks you for your password, refer that person to your charge nurse or supervisor for help in obtaining a password. Most computer systems employ a protective device with which access to personal health information can be traced back to the user's password. If you give out your password, you will be vulnerable to the consequences of any violations committed under your password.

The "delete" button. When you delete personal health information from a computer screen, you delete the information only from the screen. The information remains available to "hackers" or professional investigators on the hard drive or within the software. For this reason, most health care providers take special precautions when selling or donating old computers to users outside the health care institution. If you use a PDA or a laptop, you should be aware of this vulnerability and proceed with caution if you remove the PDA or the labtop from the facility. Your security officer can help you learn to encrypt such information, or protect it with passwords, if you frequently use your PDA or laptop outside the workplace.

Computer viruses. Computer viruses can damage or paralyze a system, making access to vital patient information impossible. Viruses can also allow for violations of confidentiality by allowing unauthorized personnel access to confidential information. You can

help protect your hospital's integrity of information by practicing caution with your e-mails. You should not open e-mail attachments from unknown senders. E-mail attachments can contain a virus that spreads quickly throughout a system just by your opening the document on your computer. Unauthorized software can also contain viruses that damage a computer system. You can introduce harmful viruses simply by downloading infected programs from the Internet or from software that you bring from home. The safety officer will be able to help you determine the safety of any software programs you contemplate installing.

When preparing for HIPAA compliance, health care organizations can use "best practices" as their baseline. "Best practice" is a common term used in health care to identify the best standard to follow. A best practice is a way to do something that is most efficient and effective. Identifying the best standards that exist in the

industry and then striving towards achieving them is a good approach. The evaluation of such practices provides a realistic method for justifying security controls and HIPAA compliance. Once practices are established for the organization, the security professional should then ensure that staff is following the documented procedures and should observe those practices during routine assessments and surveys.

HIPAA legislation regarding the portability of health insurance continues to evolve. The U.S. Department of Health and Human Services maintains a Website (www.cms.hhs.gov/hipaa/) with current advice for consumers and news about the status of this aspect of the legislation. You may be interested in learning more about these issues as a consumer yourself or as an advocate for a patient or client. As the Website explains, "If you have questions on getting and continuing health coverage during events such as losing

When you are ready to take the quiz, click here to start the process