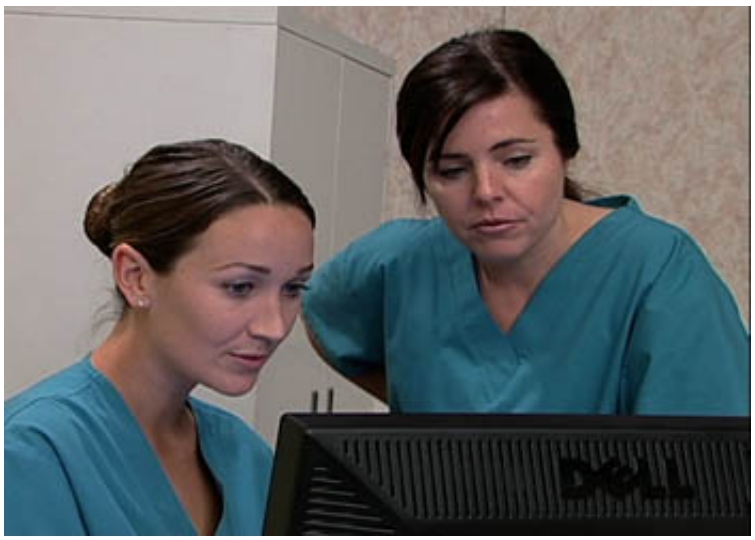
Confidentiality (Mandatory Update / Non-CE)

Course Overview

COURSE INTRODUCTION

Confidentiality is the foundation for trust in the patient-caregiver relationship. Efforts to maintain and protect confidential information once focused solely on paper medical records. But as communication technology has made it possible to easily store and transmit enormous amounts of medical information through computerized databases, fax machines, and the internet, there is an increased danger that confidential information may be revealed to inappropriate individuals.



To complete this course, you must do the following:

- Read the Overview and Learning Objectives
- Study the Terminology
- Study the Content
- Complete the Post Test with a passing score of 80% or more

OVERVIEW

This course describes the Health Insurance Portability and Accountability Act (HIPAA) and the guidelines that have been implemented to ensure patient confidentiality. The material is organized around the following categories:

- Introduction
- HIPAA Today
- Administrative Simplification
- Privacy Standards
- Confidentiality in Practice
- Confidentiality Scenarios
- Conclusion

PURPOSE/OVERALL GOAL

The purpose of this program is to provide healthcare workers an understanding of how to maintain patient confidentiality in the era of electronic record keeping.

LEARNING OBJECTIVES

After completing this course, the learner should be able to:

- Describe the Health Insurance Portability and Accountability Act (HIPAA).
- Describe various confidentiality considerations in daily practice.
- Identify ways to keep electronically stored information private.
- Follow guidelines for maintaining confidentiality in written and verbal communications.
- Describe the administrative simplification guidelines and codes.
- Identify actions and responses that constitute breach of privacy and describe the consequences for these breaches.
- Identify privacy rules in special settings and describe exceptions to the privacy laws.

NOTE: *Some sections of this course include video demonstrations. Adobe Flash Player is required to view the videos. Click here to download the free Adobe Flash Player if you do not already have it installed.*

v03.01.17

Original Release: 2008
Reviewed for Accuracy: 7/2016

Terminology

AIDS: Acquired Immunodeficiency Syndrome.

Breach: Failure to uphold agreed upon responsibility.

Chemical dependency setting: An institution set up to help those addicted to substances such as drugs and alcohol.

HIPAA: The Health Insurance Portability and Accountability Act, passed by Congress in 1996 to address a variety of insurance-related issues including new questions of privacy raised by the storage and transfer of information electronically.

HIV: The virus that causes Acquired Immune Deficiency Syndrome (AIDS).

Privacy Officer: The person in your institution designated to know and understand your state's laws as well as federal laws regarding privacy and confidentiality, and your facility's policies.

Reporting laws: Those laws, varying from state to state, that define when information must be passed to police or other authorities, often including threats to others and observed indications of crimes, such as gunshot wounds.

Introduction

Confidentiality is the foundation for trust in the patient caregiver relationship. Efforts to maintain and protect confidential information once focused solely on paper medical records. But as communication technology has made it possible to easily store and transmit enormous amounts of medical information through computerized databases, fax machines, and the internet, there is an increased danger that confidential information may be revealed to inappropriate individuals.

HIPAA Today

It's likely that the Health Insurance Portability and Accountability Act (HIPAA) has already caused changes in your own practice, especially in relation to patient confidentiality. It is important to understand the underlying HIPAA laws that brought these changes about, and the rationale for the laws.

With the number of Americans changing jobs today, many employees suddenly find themselves covered by new and different health care plans. Congress wanted to address the issue of portability of health coverage, allowing employees to carry their existing plans with them to new jobs. But given the great variety of plans, it simply was not practical to require immediate portability, so Congress decided on a course of incremental reform.

As a first step toward health care portability, Congress passed the HIPAA act of 1996, which has been further modified in subsequent years. A primary focus of this reform is protecting the privacy and security of a patient's health information. Some portions of HIPAA mainly affect personnel in information systems, medical records and administration. But other requirements affect virtually everyone working in healthcare.

HIPAA requires that you protect patient confidentiality in all its forms–oral, written and electronic–and that you protect the security of patient data–particularly as more and more patient data is transmitted electronically.

Administrative Simplification

To lay the groundwork for portability, Title II of HIPAA called for Administrative Simplification rules that specify standardized codes and formats for the interchange of medical data, and protect the confidentiality of that data. The Administrative Simplification regulations are the provisions that have had the most impact on those providing patient care because they require providers to keep a patient's protected health information confidential in all its forms–oral, written and electronic.

The Administrative Simplification provisions consist of five sets of rules:

- The Transactions and Code Sets Rule
- The Unique Identifiers Rule
- The Security Rule
- The Enforcement Rule
- The Privacy Rule

We'll look briefly at the first four rules, then look in more detail at the Privacy Rule.

Computers and other electronic systems have proved to be a tremendous benefit in medicine. Along with these benefits, however, there has been a proliferation of a wide variety of different standards and formats and codings–for a variety of purposes: recording and transmitting treatment decisions among providers, billing insurance

providers, payment remittance, and many others.

Transactions and Code Sets

To help simplify all this, the Transactions and Code Sets Rule of HIPAA defined certain code sets as the standards for all electronic data interchange. For example the standard coding for diagnoses is now based on the International Classification of Diseases, 10th edition (ICD-10). And for physician services the codes are based on the Current Procedural Terminology (CPT).

Unique Identifiers Rule: National Provider Identifier (NPI)

To maintain security as well as standardization of information as it is passed to other locations, HIPAA also mandated the creation of unique identifier codes for healthcare providers, health plans, and employers. This is known as the National Provider Identifier (NPI).

The NPI replaces older identifiers used by government programs for billing purposes, such as the unique physician identification number, but it does not replace identifiers used for other purposes, such as the DEA number, a tax ID number, or a provider's state license number.

Security Rule: Administrative Safeguards, Physical Safeguards and Technical Safeguards

The Security Rule focuses specifically on protecting protected health information in an electronic form. The Security Rule takes a three-pronged approach to protecting this information.

First Administrative Safeguards protect information through specific administrative policies and procedures, such as determining who will have access to protected information and at what level.

Second, Physical Safeguards protect physical access to protected information, such as through the use of specific hardware or software, or simply through protective positioning of computer screens.

Third, Technical Safeguards are used to protect information through the use of encryption, authentication programs and other electronic means.

Enforcement Rule

The Enforcement Rule established the civil penalties for violations of the Administrative Simplification rules. HIPAA regulations provide serious civil and criminal penalties for violations. At the extreme, anyone caught selling private health care information can be fined up to $250,000 and sentenced to up to 10 years in prison. Civil penalties can run as high as $25,000. Even unintentional disclosure can involve penalties, so it is crucial that all healthcare workers learn their HIPAA responsibilities and make them part of their daily practice.

Most of the decisions relating to the administrative simplification task have fallen to administrators, medical records managers and information processing personnel. But, whatever your place in the healthcare system, you should be aware of these coding standards and any implications they have for your job.

Privacy Standards

It is the privacy and security components of HIPAA that probably have had the greatest impact on your day-to-day job.

Understanding the Privacy Rules starts with understanding what is considered protected health information. Protected health information (PHI) is any information about a person's health, in any form–written, spoken or electronic–that includes the patient's name or other individual identifiers, such as a birth date or medical record number.

Doctors, nurses and other healthcare providers can share patient information, medical tests, reports and other medical data with one another without needing specific patient authorization as long as it is for treatment purposes, or to complete material for a third-party payor.

There are also some permitted uses and disclosures of protected health information that do not require permission from the patient. These kinds of disclosures are often viewed as "beneficial" to the public. For example: reporting vital statistics, reporting communicable diseases, reporting adverse reactions to drugs or medical devices to the FDA, and reporting information related to organ donation.

Written Notice

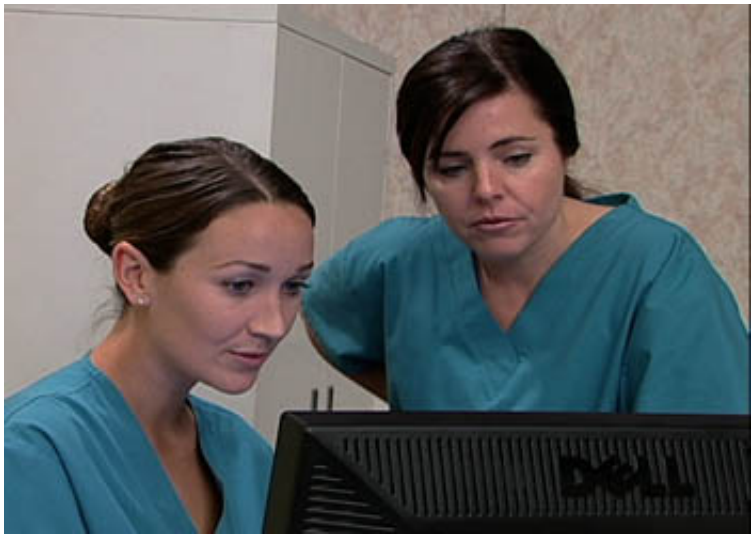
The general privacy rule is that patients have to be notified of the institution's privacy policies, and you must make a good faith effort to obtain a written acknowledgement of this. The HIPAA notice explains to patients that their health information may be transmitted to third parties for routine use in treatment, payment or other healthcare operations.

The notice also explains patients' rights to see their own medical and billing records, make changes to anything they feel is inaccurate, and in certain circumstances, learn who has seen their records. Patients must now be asked to acknowledge that they have seen this privacy notice. However if they refuse to sign it, you may still provide treatment.

HIPAA allows exceptions to the requirement for a privacy notice and written acknowledgement, in situations when it might prevent or delay timely care–for example, with emergency care. While some disclosures are permitted under HIPAA, they require that the patient be given an opportunity to object before the disclosure can be made.

Confidentiality in Practice

To enhance confidentiality, your facility should have reduced the identifiable patient information that is visible. For example, door tags and whiteboards have less information or none about identity, and no diagnosis, procedure or treatment information that is visible to the public and can be linked to the patient. In some facilities, whiteboards and scheduling tools have been moved to an area out of sight of the general public.



Patient safety and patient care are still paramount, however, and some information, such as fall risk is still clearly posted–as are important food orders such as "Nothing By Mouth," or "Diabetic Food Only." Also, charts containing patient names or other identifiers are now stored out of view where they cannot be read by passers-by.

If necessary for patient care, a chart can be kept at bedside or in other areas, but reasonable precautions must be taken to make sure passers-by cannot access it. Some of these precautions include limiting access to these areas, allowing only escorted access, or having any visible information on the chart covered in some way or turned toward the wall.

The use of white board logs and lightboards for X-rays and other scans also require new safeguards. Either they are positioned out of public view, or they have safeguards or covers to prevent any accidental disclosures.

Computer Security

Confidentiality is equally important on computers and electronic equipment. For example, you need to blank the screen or sign off whenever you leave a terminal. Terminals should be oriented so the public cannot read what is on the screen over your shoulder.

As they become available, you will see much more use of flat screen monitors. The data on a flat screen is much harder to read at an angle, which provides greater data security. A flat screen by itself does not, however, offer complete security. Some facilities may use a form of cover over the screen, or limited access privacy screen, to conceal it.

Never share a password, or allow another healthcare worker to access information under your sign-in. Even if the person is in a hurry and seems to need the information for legitimate reasons, it is a serious violation of data security. And it leaves no record that that person accessed the information.

Another change in the workplace has been made necessary by the increasing use of fax machines for sending patient information. One way fax security is maintained is by locating fax machines in a secure area, and making sure all faxes have a cover sheet, noting that confidential information is contained in the transmission.

You should also telephone to let the recipient know that the patient's information is coming in a fax. If the receiving fax machine is publicly accessible, someone should be asked to stand by the machine and collect the information as soon as it arrives. Faxes with patient information should never be left unattended where they might easily be picked up, even by accident, by someone expecting a different fax. Either destroy any faxes or printouts immediately or place them in the patient's medical chart, as appropriate.

E-mail security must also be maintained if you are sending patient information. Use password protection at both ends and encryption if it is going over the internet. Be sure to double-check the name of the recipient so it does not go to the wrong place. It is all too easy to click on the wrong name on a mailing list, or mistype a name.

Information Storage

In your facility, it is likely that filing cabinets, medical charts, or other information are now kept in secure locations where they cannot be accessed by the public. All healthcare workers must take reasonable precautions to protect X-rays and other scan displays from public view. As mentioned earlier, in many facilities the X-ray viewers are no longer in public areas. Further, there must be a system in place to record the name of every healthcare worker, and anyone else who views or discloses a patient's record. HIPAA requires that patients be given this information if they ask for it.

Sign-In and Public Address

In waiting rooms, the use of sign-in sheets and publicly calling out patient names are both allowable as long as no other information is disclosed. Public announcements of patients' names are considered to be "incidental uses or disclosures" that are not violations of the privacy rule, provided that the facility has reasonable safeguards that prevent revealing any further information.

It may sometimes be necessary to announce a patient's name over the facility's public address system. In this situation, the patient should be referred to a reception desk or some other more private place where they can receive further information in a more confidential manner. The use of devices such as pagers, can also be used as a way to call patients, or family members, in a way that maintains confidentiality.

Messages and Reminders

Messages and reminders, both on the telephone and in the mail also require care. Bear in mind that any messages or appointment reminders left on an answering machine may be overheard by others. Limit the amount of information disclosed to the name of the facility or physician and the time of the appointment. If it is necessary to discuss a treatment or preparations for a procedure, leave a call-back number so the patient can return the call in private.

If a patient requests confidential communications, the facility should accommodate the request as long as it is reasonable. Some patients may request receiving all communication in a sealed envelope, or receiving it at a post office box or a work address.

Pharmacists may use their professional judgment in releasing a prescription to a person other than the patient. The fact that a person asks for a specific prescription for a specific individual can usually be taken as a reasonable indication that that person is involved in the patient's care and has the patient's permission.

Rules Covering Conversation

Confidentiality regulations allow healthcare providers to share patient information for treatment purposes, as long as reasonable care is taken to prevent others, who have no need to access this information, from overhearing. Voice levels can be lowered, you can move to a private place and take any other reasonable measures you need so you are not overheard discussing patient information. If discussion is necessary, you should avoid public places such as elevators, lunchrooms or corridors as much as possible.

Patient safety is still paramount. Healthcare workers may share necessary information with family and others as long as the patient does not object. For example, discharge planners can share information about a patient's impaired mobility to someone driving the patient home. And discharge planners can share information about medication dosages with a family member or roommate whom they can reasonably infer will be involved in the patient's care. But you should still guard against any casual release of protected patient information.

HIPAA does not override state laws, which may demand even stricter privacy. For example, many states grant minors specific rights to privacy, particularly in relation to questions of sexual activity or pregnancy.

Confidentiality Scenarios

To help you think through and prepare for situations where confidentiality is an issue, this program will present a number of scenarios, in a variety of nursing situations, and ask you to decide if the correct decision about confidentiality is being made in each case.

Scenario 1: Two healthcare workers talking at a

table in a cafeteria.

HCW 1: Drug addiction, eh?

HCW 2: Yup. She's in here this time for gall bladder surgery, but my friend got a look at her chart. I heard she was hooked on painkillers for two years.

HCW 1: And this is somebody I would know?

HCW 2: Her husband is a bigshot in city government. That's all I'm going to say.

They get up and pass a man sitting at the next table, watching them leave. He pulls out a cell phone and makes a call.

Sometimes the natural urge to talk about confidential information is hard to resist. But telling just one person may result in a rumor being spread over an entire institution and beyond. This scenario illustrated a serious violation of confidentiality.

Scenario 2: *A telephone rings at a nursing station. The nurse answers it.*

NURSE: Nurses' station.Yes, he is.You're his mother?

She looks at the chart. Comes back on the line.

NURSE: Let's see. Pneumonia. He should be discharged by the end of the week. Was the pneumonia caused by the HIV? I don't know for sure, but it probably was.

Even if the patient had authorized releasing information to his family, how did the nurse know she was talking to his mother? Many states and the federal government have even stronger privacy laws in special cases–such as for patients who have HIV or AIDS. This was a serious violation.

In this case the nurse should have established a code system for those authorized to know, or simply and politely explained that that information is private.

Scenario 3: *A young woman in the doorway of a patient room, says good-bye to her father and walks over to the nursing station.*

DAUGHTER: I'd like to see my father's chart, please.

NURSE: Sure, here it is.

The nurse hands over the chart.

In many states, access to the chart is prohibited by law, without the patient's written authorization. Depending on state law, some institutions may even require that the physician be present when the patient or family views the medical record. You should learn your state laws, and your institution's policies about access to the chart.

Scenario 4

As a home health nurse walks to her car parked in front of her patient's home, a neighbor approaches to speak to her.

NEIGHBOR

How are things going in there? Are they getting along any better?

HOME HEALTH WORKER

I tell you, those people fight like cats and dogs. No wonder they're getting a divorce.

Remember that confidentiality applies to all healthcare workers, and in all settings, even in a person's home or a public area. And it applies to both information about the person's health, and to personal information you may have learned while providing care. Unauthorized disclosure of personal information can easily get back to your patient and may destroy the trust inherent in the caregiver-patient relationship. Learn to limit yourself to general comments, or to turning a conversation to another subject.

Scenario 5: *As a nurse exits an exam room with a teen-age girl, the girl's parents confront them.*

MOTHER: Nurse, can we talk to you?

NURSE: Yes, what can I help you with?

FATHER: This is just about the limit.

MOTHER: Could you please tell us if our daughter is pregnant?

FATHER: We have a right to know!

NURSE: Yes, I'm sorry to have to tell you. It appears that your daughter is about two months' pregnant.

In many states this is a serious violation. Normally the parents of minors are automatically given information about their child's condition. But in many states, cases involving pregnancy, sexual abuse, rape, or other special circumstances are treated differently under the law and disclosure even to parents may be a serious breach of confidentiality. You should learn the laws in your state.

Scenario 6: *In a emergency department room, a nurse assesses a woman with a black eye, bruises and other marks consistent with abuse.*

NURSE *(suspicious):* So you say you got the black eye and all these bruises in a fall?

BATTERED WOMAN: Yes! Like I said, I just fell. Now would you people just mind your own business and get me patched up!

NURSE: OK.Wait right here. I'll be back in just a second. OK?

Nurse exits exam area and finds her supervisor.

NURSE *(to supervisor):* I'm glad I caught you. That woman who just came in–she says she fell, but her

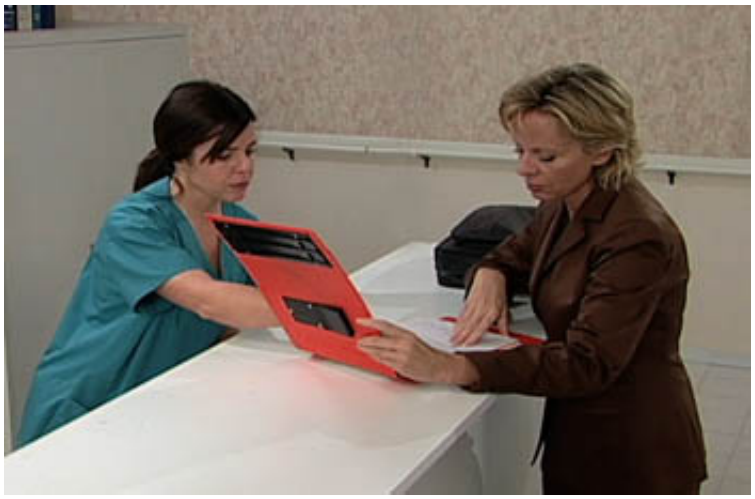
injuries look like a battering. I don't think there's any way they could be from a fall. I think we have to report this.

The nurse and supervisor re-enter the exam room.

This is not a violation. There are important exceptions to a caregiver's obligation to keep information confidential. These exceptions are set forth in your state's reporting laws. When you encounter any patient who appears to have been physically abused, you have a duty to report your suspicions. Normally the police or county social service agency must be notified by you or your supervisor. Laws vary from state to state and caregivers have a legal obligation to know the state laws regarding reporting child, domestic and elder abuse.

Conclusion

HIPAA regulations have required a number of changes in your work habits and in the accustomed culture of healthcare throughout the country. Remember that these HIPAA privacy requirements not only are federal law but also are an important part of maintaining patient confidentiality, which is a crucial part of the trust necessary between a patient and a caregiver.



When protected health information must be communicated, make sure it is for treatment or billing or other uses that are within the law and within the policies and procedures of your institution. Healthcare providers are caring and giving people. Part of that caring attitude is doing your utmost to respect the privacy of everyone under your care.