Confidentiality / HIPAA 2.0 Contact Hours

Quiz Button

Course Objectives:

1. Define confidentiality and related key terms.
2. Discuss concepts concerning confidentiality.
3. Analyze what is considered “confidential information”.
4. Describe consequences associated with a breach in confidentiality.
5. Examine the responsibilities of a healthcare worker regarding private and confidential information.
6. Explore the meaning of “informed consent”.
7. Recognize how confidentiality relates to HIV/AIDS patients.

Overview

Patient confidentiality and privacy are very important aspects of jobs in the healthcare industry. Each and every day patients place their trust in the hands of health care providers. Patient confidentiality generally refers to a patient’s trust that health information will only be shared with those who need to know, and in order to provide appropriate care.

Maintaining confidentiality will ensure that laws and policies will not be broken. Healthcare providers need to be mindful of the problems when confidentiality issues are violated. Smart charting and being aware of company policy and procedures will go a long way in protecting you legally as you do your best to give high quality care to your patients. Confidentiality issues are also a standard of practice related to ethical and

professional healthcare.

For patient care to be appropriately authorized, the health care staff may need full access to a patient's medical record. However, patients have the right to withhold important information if they fear it will not be kept private and confidential. By ensuring patient privacy and confidentiality, your facility will help patients feel a sense of trust and help assure them they will receive appropriate care. Protecting patient privacy and confidentiality is vital to your organization's mission. It helps increase patient's satisfaction and sense of dignity. It helps ensure that patients get the most effective care. It is also the law.

Patient privacy and confidentiality generally refers to a patient's right to:

- Decide what personal health information can be shared with others
- Decide how that information can be shared, and with whom it may be shared
- Have physical privacy (for example, curtains pulled during an examination or even when at rest)

Defining Key Terms

Confidentiality- requires that information shared by a patient in the course of treatment not be shared with others. Confidentiality is a term that entrusts a person with the private information of another. This includes information gained verbally or from written records. All information is considered confidential when it pertains to medical care and client records.

A Breach of Confidentiality- is a security violation. No one outside the health care team caring for the patient is to be told information about that patient. Information can only be shared with someone outside the healthcare team when the patient has signed a "release of information" form.

Indiscretion- is an action in which you inadvertently share confidential information. There is no malicious intent associated with an indiscretion.

Informed Consent- is a process of communication between a patient and physician that results in the patient's authorization or agreement to undergo a specific medical intervention. This permission is given by filling out a legal consent form, which becomes part of the resident or client's permanent record. For consent to be truly informed the patient must be told:

- Who the information will be sent to
- Who requested the information
- How the information will be used
- How long the consent is valid

Private- is defined as not available for the public's viewing or knowledge.

Privileged information- a term that refers to all information shared between an attorney and his client. This information is confidential and is not admissible in court.

Scope of Practice- the duties and responsibilities of an assigned job as designated by education or law.

Concepts Concerning Confidentiality

The following are a list of concepts that are used concerning confidentiality:

- **"Do No Harm"-** In regard to gathering, recording and sharing verbal or written information, "do no harm" means that sensitive data should be disclosed at no risk to the patient and that there will not be a breach in confidential issues. In regard to privacy, "do no harm" means that absolutely no health professional will

intentionally let a patient feel embarrassed while being treated and/or examined physically.

- **Be honest-** Whether you're dealing with the patient or the resident's family members always remain honesty. Do not be afraid to admit if you made a mistake and tell them how you will be rectifying said mistake.
- **Use information proactively-** The main purpose of sharing information is to provide the most accuracy when diagnosing a patient, prescribing the best recommended treatment, and providing the best care.
- **Irreversible-** Information that is already shared cannot be unshared, erased, or deleted. Before you make a statement about a patient, think about what you say before you say it. Once it is said it cannot be taken back- this is irreversible.
- **Threat of self-destruction-** A claim of confidential or private matters cannot be honored if concealment poses a threat to the patient. For example, if a patient tells you he or she wants to harm or kill his or herself or someone else, under no circumstance can you keep that confidential. You have to share this information with a supervisor to prevent a possible suicide or other crime.

What is Considered Confidential?

Information and actions that are confidential and private include, but are not limited to the following:

- Age
- Sex
- Race
- Religion
- Marital status
- Occupation
- Health information
- Social security number
- Insurance information
- Health conditions and problems

- Lab tests and X-rays
- Blood work
- MRI and CT scan
- Any diagnostic procedure done on the patient
- Any physical contact that involves examination
- Personal care
- Toileting and dressing

HIPPA

The Health Insurance Portability and Accountability Act (HIPPA) of 1996 was enacted by the United States Congress and signed by President Bill Clinton in 1996.

Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. The Administration Simplification provisions also address the security and privacy of health data. The standards are meant to improve the efficiency and effectiveness of the nation’s health care system by encouraging the widespread use of electronic data interchange in the U.S. health care system.

In January 2013, there were adjustments made to HIPPA, known as the Final Omnibus Rule. This provides expanded protection and control over personal health information with regard to business associates of healthcare facilities and insurance companies that must accept and collect patients’ health information. It has been found that the majority of breaches and issues around reporting breaches center around these business entities. The definition of the term “significant harm” to an individual was updated so that there will be more auditing for those covered so that there will be more opportunity to report breaches of confidentiality that had not been reported previously. Before this new rule, there would be to be more proof with regard to the fact that the alleged breach intended harm. Now they must prove instead that no harm

occurred or it must be reported. Finally, now Personal Health Information (PHI) is protected not indefinitely, but until fifty years after a patient has died. There are also more serious penalties put into effect for those that would breach PHI privacy policies.

Violations of HIPAA

A breakdown of the HIPAA violations that resulted in the illegal exposure of personal information.

A breakdown of the HIPAA violations that resulted in the illegal exposure of personal information.

According to the US Department of Health and Human Services Office for Civil Rights, between April 2003 and January 2013 they received 91,000 complaints of HIPAA violations, in which 22,000 led to enforcement actions of varying kinds (from settlements to fines) and 521 led to referrals to the US Dept of Justice (criminal actions). Examples of significant breaches of protected information and other HIPAA violations include:

- the largest loss of data that affected 4.9 million people by Tricare Management of Virginia in 2011
- the largest fines of $4.3 million levied against Cignet Health of Maryland in 2010 for ignoring patients' requests to obtain copies of their own records and repeated ignoring of federal officials' inquiries
- the first criminal indictment was lodged in 2011 against a Virginia physician who shared information with a patient's employer "under the false pretenses that the patient was a serious and imminent threat to the safety of the public, when in fact he knew that the patient was not such a threat."

The differences between civil and criminal penalties are summarized in the following table:

Type of Violation	CIVIL Penalty (min)	CIVIL Penalty (max)
Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA	$100 per violation, with an annual maximum of $25,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation due to reasonable cause and not due to willful neglect	$1,000 per violation, with an annual maximum of $100,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation due to willful neglect but violation is corrected within the required time period	$10,000 per violation, with an annual maximum of $250,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation is due to willful neglect and is not corrected	$50,000 per violation, with an annual maximum of $1,000,000	$50,000 per violation, with an annual maximum of $1.5 million
Type of Violation	**CRIMINAL Penalty**	
Covered entities and specified individuals who “knowingly” obtain or disclose individually identifiable health information	A fine of up to $50,000 Imprisonment up to 1 year	

Offenses committed under false pretenses	A fine of up to $100,000 Imprisonment up to 5 years
Offenses committed with the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain or malicious harm	A fine of up to $250,000 Imprisonment up to 10 years

Breach of Confidentiality

There are two types of outcomes related to a breach of confidentiality: positive and negative.

Examples of *positive* outcomes regarding a breach in confidentiality include:

- If you suspect abuse or neglect and it needs to be investigated and is thus ended.
- If you suspect possible future abuse and neglect and report it to avoid or prevent it.
- An attempt at suicide or other violent crime is divulged which needs to be prevented.
- If appropriate interventions need to be initiated for a patient to get help in appropriately related areas.

Examples of *negative* outcomes regarding a breach in confidentiality include:

- A facility or agency may reprimand a healthcare worker with disciplinary action for breaching confidentiality related to patient care issues.
- The resident or client may suffer embarrassment and emotional distress.

- Irreversible damage may be done to the patient-provider relationship.
- The patient filing charges against the healthcare worker, staff, and facility. When a patient sues a facility/staff for breach of confidentiality they usually win.

Guidelines for Protecting Private and Confidential Information

- Discuss resident and client information ONLY to appropriate individuals and in a private place that is away from and out of earshot of other residents, families and visitors.
- Shift reports should not be delivered at the nurses' station where confidential information can be overheard.
- Never discuss anything about patients in: an elevator, a hallway, a cafeteria, or any other public place within or outside of the facility.
- Discuss resident information only with appropriate and necessary staff. Never release information to media, newspapers or social media. Never release information to the police without approval from your supervisor, manager or administration. If approached, refer them to an appropriate supervisor, manager, or administration.
- Never make or keep a copy of patient information.
- Shift report sheets should not leave the facility.
- Any item with a resident's name or identifying medical information should be shredded and placed in specially indicated trash bins. Never place even shredded documents in the same trash that is used for the public.

Responsibilities Regarding Private and Confidential Information

- Ask your supervisor to explain any issues regarding confidentiality that you are not clear on or do not understand.
- Never discuss information that you do not understand or

are not sure about.
- Make sure you are sharing the right information with the right people. The patient or the patient's proxy (surrogate) has the ultimate right to make the decision as to who is allowed to have access to the patient's medical information.
- Patient care is private and your behavior needs to guard that confidence.
- Keep the lines of communication open between your superior and yourself.
- Do not discuss information about a patient in areas where others can overhear.

Issues in Protecting Patient Privacy and Confidentiality

New technology and the growing use of computers help improve health care but can also cause wrong information to be added to data and can make it easier to illegally share information. Healthcare facilities must make sure patient information is protected when using electronic technology such as: fax machines, e-mail, computer networks, electronic records, telephones and voice mail systems. The newest HIPPA update in 2013, the Final Omnibus Rule, covers these issues at length.

Who Monitors Patient Privacy?

Government agencies that monitor patient privacy include:

- **The Joint Commission on Accreditation of Healthcare Organizations (JCAHO) –** This national organization accredits healthcare facilities that meet JCAHO standards. Patient confidentiality and privacy is an important part of these standards. If JCAHO surveyors evaluate your organization, they will expect you to know your organization's mission, your organization's policies for protecting confidentiality, what efforts your department is making to improve patient privacy and confidentiality, and how your job relates to all of

these.

- **The National Committee for Quality Assurance (NCQA) –** This national organization evaluates managed care plans and accredits managed care organizations. NCQA and JCAHO have developed special recommendations to help managed care organizations protect patient privacy and confidentiality. Areas that these recommendations address include: staff education, patient consent, and systems to ensure confidentiality.
- **The Health Care Financing Administration (HCFA) –** HCFA is a part of the U.S. Department of Health and Human Services and administers Medicare, Medicaid, and Child Health Insurance Programs. HCFA's responsibilities include: ensuring that Medicare, Medicaid and the Child Health Insurance Programs are properly run by state agencies. HCFA also plays a part in evaluating health care facilities and services including guidelines related to patient privacy and confidentiality. Healthcare facilities and providers must meet strict guidelines to be certified by HCFA.

Meeting Legal Requirements

- The best way to ensure meeting legal requirements and your facility's standards is to understand and follow your facility's policies and procedures. All staff should be familiar with: who has access to patient information, security measures for handling patient health information, and the proper procedures for destroying patient health information.
- Developing an environment of trust is another key to meeting legal requirements. Trust develops when patients see a facility's commitment to protecting privacy and confidentiality. Staff should never leave medical records open or unattended in public areas where unauthorized people could gain access.

- Receive informed consent from patients whenever health information needs to be released.
- Research your facility's "need to know" policy. Only healthcare staff that needs to have access to patient information should be allowed access.
- Know the difference between "need to know" information which is needed for patient care and "want to know" which is not needed for patient care.
- If you even suspect certain information might be confidential, treat it as such. Always better to be safe than sorry.
- Show courtesy and respect to yourself and to the person in your care.
- Respect every patient's right to privacy at all times.

Signing an Informed Consent

- Every adult is considered competent to make all of his or her decisions unless proven otherwise by a court of law.
- If the patient is proven incompetent, the patient's proxy (surrogate) or court appointed guardian makes decisions on his or her behalf.
- When the patient is a minor, a parent or legal guardian must give consent for most procedures and in most instances. Exceptions are discussed below. But in most cases, the law states that a minor cannot make any decision dealing with their health. The parent or legal guardian will have to make the decision for the minor.
- Healthcare staff must use language that patient can understand, or get an appropriate person to speak to the patient in a language or way the patient can understand; it may be necessary to bring in a qualified interpreter.
- It must be clear that the patient understands the information given to him. Questions must be discussed and answered using verbal or nonverbal cues.
- Remember that consent must be voluntary- the patient

must give consent without feeling pressured. No patient should feel obligated to give consent if they don't want to. Consent that is not voluntary is not legally binding.

- Patients must be given the opportunity to review their medical records before giving informed consent if the patient so desires.

  Some information must be released with or without consent. In general, healthcare staff must report abuse, criminal activity, or threats from patients to their supervisor.

Confidentiality and HIV/AIDS

Every state requires reporting of HIV positive status and AIDS cases to the state's health department. While the data is used for infection control purposes, the requirement is still controversial because in some states, facilities are required report a patient's name, address or other identifying information to the designated department and this strikes some as a violation of the spirit of confidentiality.

It's very important to protect HIV/AIDS information from all other sources. Anyone who improperly releases a patient's HIV/AIDS status can face serious legal action, as well as severe reprimand by the Board of Nursing. Laws vary from state to state.

Minors and Confidentiality

In most instances, the law does state that a minor is not able to make decisions involving their healthcare. This falls to the discretion of the parent or legal guardian. But in many states, minors can give consent for certain medical care. This includes care for pregnancy, sexually transmitted diseases, and drug dependency. Some minors, such as those who are married or in the armed forces, can make all of decisions regarding medical care on their own. Laws vary from state to

state.

Mental Health and Substance Abuse

Special laws and policies apply to the release of patient information regarding mental health or substance abuse. Staff should be aware of laws and policies affecting the release of this type of information to the patient and to others.

References

McGowan, C. (2012). Patients' Confidentiality. *Critical Care Nurse*, *32*(5), 61-64.

Nurses Legal Handbook
Fourth Edition, Springhouse Publishing
2010, Springhouse Corporation

Resident's rights and confidentiality
Sixth edition
Mosby Publishers; 2010

New Rule Protects Patient Privacy, Secures Health Information (2013), from

http://www.hhs.gov/news/press/2013pres/01/20130117b.html

HIV Disclosure Policies and Procedures (2012), from

http://aids.gov/hiv-aids-basics/just-diagnosed-with-hiv-aids/your-legal-rights/legal-disclosure/

State Laboratory Reporting Laws: Viral Load and CD4 Requirements (2013), from

http://www.cdc.gov/hiv/policies/law/states/reporting.html

www.ahca.gov
www.jcaho.org

Quiz Button