



LEARNING MODULE #2

HIPAA AND COMPLIANCE

For Clinical Students and Instructors

FVHCA Member Clinical Sites

Reviewed 2-25-10

Objectives

At the completion of this learning module, students and/or instructors will be able to:

- Define HIPAA;
- Identify methods to maintain the privacy and confidentiality of personal protected health information;
- Identify how HIPAA impacts your role; and
- Indicate compliance and regulatory issues that may impact your role.

- All students and instructors who participate in clinical activities are deemed “workforce members” at the various healthcare systems.
- All policies and procedures are applicable to “workforce members”, just as they would be for employees.
- This includes policies and procedures related to HIPAA, Confidentiality and other Compliance or Regulatory requirements.

What is HIPAA?

- In 1996, the federal government passed a law named “HIPAA” (Health Insurance Portability and Accountability Act).
- The original and primary intent of the law was to provide continuous insurance coverage for employees who changed jobs.
- When writing the law, the authors became aware of how much personal health information was shared between health care providers and insurance companies.
- Because of this, additional sections were added to the law, requiring healthcare providers to adopt standards in the areas of privacy, security and electronic transfer of data or billing.

What is HIPAA?

- The law defines “protected health information” (PHI) and sets standards for health care providers to protect that information.
- All healthcare systems have policies in place to ensure that PHI is available, private and secure in order to promote quality care and treatment.

What happens to those that don't comply?



- If not, the law also defines stiff penalties (fines and even imprisonment) for violating any privacy provisions. These penalties apply to any member of the “workforce team”.
- Some Wisconsin State laws also protect the privacy of patient information.

Patient Privacy Rights

Under HIPAA, patients have certain rights:

- Right to access their health information.
- Right to request an amendment to their PHI if they feel the information is incomplete or inaccurate.
- Right to request a place to receive PHI.
- Right to request restrictions on what PHI can be disclosed.
- Right to request an accounting of what PHI has been disclosed.

What is Confidential?

- Any information that we collect, create, store, etc., that relates to an individual's health and **identifies** that patient, client or resident is *confidential*.
- This is called **Protected Health Information** (PHI). PHI includes any information we create.
- PHI includes any personal information we ask the patient, client or resident to provide.

Examples of PHI

Protected Health Information (PHI):

- Medical Record Number
- Billing Information
- Medical Information

Personal Information:

- Name
- Address
- Date of Birth (DOB)
- Phone Number
- Insurance and Social Security Numbers
- Medical History

Forms of PHI

- **Protected Health Information can be seen in different forms.**
- Be aware of these examples:
 - Spoken information
 - Paper, documents, charts
 - Computer screens
 - White boards (surgery schedules, patient boards)
 - Photos, videos
 - Medical container labels (prescription bottles, IV labels, packages, specimen labels, etc.)



Be aware of ePHI

- The “e” in “ePHI” stands for electronic.
- “ePHI” is any information that is accessed or stored electronically using computers or other equipment.
- These electronic devices or computers include:
 - Desktop computers
 - Laptop computers
 - PDA (personal digital assistants)
 - Smart phones or Blackberries®
 - Computer discs or flash drives
 - And others

The HIPAA Security Rule

- The HIPAA security rule was also developed and now paired with the privacy rule.
- The HIPAA security rule has additional requirements regarding how ePHI is accessed, stored, displayed, and transferred electronically.
- The security rule requires healthcare providers to make sure health information is available when needed and we ensure the integrity of the information.
- Integrity – this means we must make sure the information is not altered or changed by anyone who does not have the authority to do so.



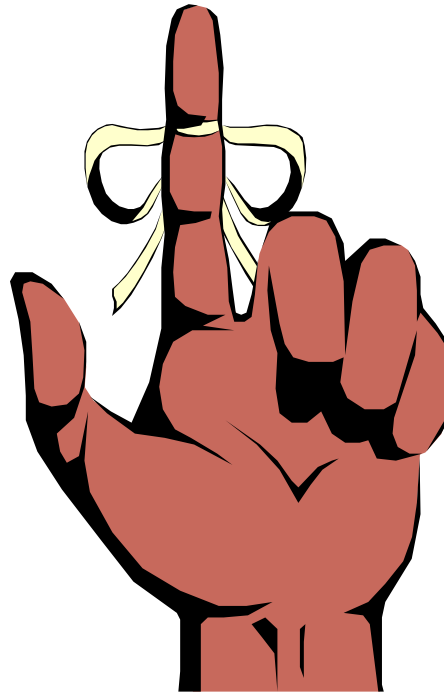
The HIPAA Security Rule



- The security rule also has requirements regarding how information is accessed.
- All healthcare systems have special safeguards in place to protect ePHI.
- As part of the workforce team in a healthcare system, you may or may not be provided with computer access.
- HIPAA and Healthcare Systems require unique identifiers to access computer applications or systems that contain patient, client or resident information.

Always remember:

**YOU MUST SAFEGUARD THE
PRIVACY AND SECURITY OF PHI.**



For Students and Instructors with Computer Access

- If you are provided computer access with an assigned user ID and password, you must protect the privacy and security of patients' PHI at all times.
- Also, protect your password and keep it secure.
- Do not share it with others on the workforce team.
- Do not write it or store it in a place accessible by others.
- And use a “strong” password (avoid pet names, sports team names or phone numbers, etc.).

Access to PHI

- Each healthcare system has specific policies governing how information is accessed and who may access it.
- Please be aware of system policies surrounding the minimum necessary information you may be allowed to access.
- This information may be found in the healthcare system site links.



YOUR ROLE IN CONFIDENTIALITY, PRIVACY, AND SECURITY OF PHI



Physical Privacy and Security

- ❑ Do not leave PHI in an area that is public or where unauthorized individuals may come in contact with it.
- ❑ Dispose of printed PHI in secure recycling/shredding bins.
- ❑ Labels (bottles, IV bags, other) containing PHI should be discarded in privacy bins or “blackened out” prior to discarding.
- ❑ The sharing of patient/resident PHI should be done in a private and secure manner (not in the hallway, break room, cafeteria, elevator, etc.)

Physical Privacy and Security

- Workstations (computers) should be logged off when not in use.
- Turn screens away from public view, use privacy screens.
- Use screen savers when user has stepped away from computer.
- E-mails may not contain ePHI unless the information is encrypted or safeguarded in some other manner.

Physical Privacy and Security

- Report suspicious behavior by others to security or information services departments.
- Each healthcare system has procedures for disposing of documents or media (CDs, flash drives, PDAs, etc.) containing patient PHI. Please follow these when indicated.

Tips for Students/Instructors

- ❑ Be cautious of where you hold conversations, especially about patients and their families.
- ❑ Never leave medical records/films in an open area, including census print outs, or other documents.
- ❑ Don't share passwords with others.
- ❑ Don't share information about friends or family (in the facility) with others.
- ❑ Do not discuss cases or PHI of patients you are not directly involved with.

Tips for Students/Instructors

- For example, if a friend says, “I heard that Mary Smith is in the hospital. Did you see her there?” You should respond something like, “I have no information about that.”
- The easiest way to remember how to implement this law is the saying;

“What you see here, or *hear* here, must stay here.”

Compliance

- Each healthcare system or facility abides by specific policies, procedures and regulatory standards.
- When we trust that facilities are doing this, it is referred to as *corporate integrity*.
- Corporate integrity or “corporate compliance” means that an organization is abiding by high moral principles and standards set out by that organization.

Compliance

- The HIPAA Privacy and Security rules are an example of an area of compliance for healthcare systems and facilities.
- Each healthcare system may have different codes of conduct or compliance manuals.
- You may find this information in the facility link on the FVHCA website.

Compliance Plans

- Healthcare systems include the following in their compliance plans:
 - General standards of workforce conduct are established.
 - Background checks on all workforce team members including students and instructors must be completed.
 - Rules and regulations that healthcare systems must follow.

Compliance Plans

The rules that healthcare systems must follow are:

- ❑ Health Insurance Portability and Accountability Act (HIPAA)
- ❑ False Claims Act (FCA)
- ❑ Anti-Kickback Statute (AKS)
- ❑ Physician Self-Referral Prohibition (also called the Stark Law)
- ❑ Emergency Medical Treatment and Active Labor Act (EMTALA)
- ❑ Fraud and Abuse in Billing

False Claims Act (FCA)

- Any organization that makes a false claim to the government (Medicare/Medicaid) for payment is in violation of the FCA.
 - ▣ *Example; sending a bill for a service that was not done.*
- If an organization is found guilty of doing this, they may be prohibited from participating in any Medicare/Medicaid or other federally funded healthcare program.

Anti-Kickback Statute



- The federal law forbids anyone to offer, pay, ask for, or receive something of value in return for referring Medicare or Medicaid patients.
- There are fines up to \$25,000 associated with this violation.

The Physician Self-Referral Law

- This law is only related to physicians.
- The government forbids physicians from referring patients to an entity where a physician has a financial relationship with that entity.
- There are, however, many complicated exceptions to this law.

Emergency Medical Treatment and Active Labor Act (EMTALA)

- **NOTE:** This EMTALA law pertains only to those facilities who have a designated Emergency Department.
- EMTALA was created during a time when hospitals often refused to treat uninsured patients who arrived by ambulance.
- The hospital must perform a medical screening exam to determine if an emergency condition exists for anyone who comes to the emergency department (regardless of their ability to pay).

EMTALA

If there is an emergency medical condition:

- The hospital must stabilize the medical condition

OR

- Transfer that person to another facility,
if the hospital cannot treat the person.



Fraud and Abuse in Billing

- This refers to knowingly billing for services provided, submitting inaccurate or misleading claims or actual services provided or making false statements to obtain payment.
- Fraud is an intentional act. In other words, the person knows they are doing something wrong.
- The government (Federal Office of the Inspector General – OIG) investigates and targets different health care areas to assure this is not happening.

Reporting Compliance Issues

- If you see things that may not be lawful, ethical or do not protect the privacy and security of the patient, client or resident, please notify your instructor, the supervisor, or department manager at the facility.



Following discovery of a breach in privacy:

- An investigation will take place based on a facility's policy.
- The Secretary of the Department of Health and Human Services, the news media, and law enforcement officials may be notified.

A final reminder...



- Remember, as a member of the healthcare workforce team, you have an obligation to keep protected health information confidential, private, and secure.
- For additional information regarding privacy policies and compliance plans, please refer to the healthcare site's policies and procedures.



Completing your Orientation

Congratulations, you are almost done!



- After completing both learning modules:

“Infection Control, Bloodborne Pathogens and Safety” (#1)

“HIPAA & Compliance” (#2)

To receive credit and verify completion of orientation:

1. Print off the [Confidentiality Agreement/ General On-line Orientation form.](#)
2. Read and Sign.
3. Turn forms in to school coordinator or faculty. (Note: These forms will be retained in your student record).