

LEARNING MODULE:

HIPAA & COMPLIANCE

For Clinical Students & Instructors

Greater Green Bay Healthcare Alliance

ggbha.org

Reviewed & Updated 6/14/2018



This learning module must be reviewed by students and faculty annually (once per year).

2

Important!!!

REMINDER:

When reading the modules, please know you are accountable for understanding the information presented. If you have any questions, you will need to talk to your instructor/school/facility representative(s) to find out the answer(s) before going any further.

Objectives

3

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

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

What is HIPAA?

4

- A. In 1996, the federal government passed the Health Insurance Portability and Accountability Act “HIPAA”
- B. The law requires healthcare providers to adopt standards or policies in the areas of privacy, security and electronic transfer of data or billing.
- C. The law defines **“protected health information” (PHI)** and sets standards for healthcare providers to protect that information.

Does HIPAA and Compliance apply to students?

5

- 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.

What happens to those that don't comply?

6

- The law defines stiff penalties (fines and even imprisonment) for violating any privacy provisions. These penalties apply to any member of the “workforce team”, **including students**.
- Wisconsin State laws also protect the privacy of patient information.

Protected Health Information (PHI)

7

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

Examples of PHI

8

Protected Health Information (PHI):

- A. Medical Record Number
- B. Billing Information
- C. Medical Information

Personal Information:

- A. Name
- B. Address
- C. Date of Birth (DOB)
- D. Phone Number
- E. Insurance and Social Security Numbers
- F. Medical History

Forms of PHI

9

Protected Health Information can be seen in different forms.

Be aware of these examples:

- A. Spoken information
- B. Paper, documents, charts
- C. Computer screens
- D. White boards (surgery schedules, patient boards)
- E. Photos, videos
- F. Medical container labels (prescription bottles, IV labels, packages, specimen labels, etc.)
- G. Student post-clinical conference discussions



Be aware of ePHI

10

- 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:

- A. Desktop computers
- B. Laptop computers
- C. Smart phones
- D. Computer flash drives
- E. And others

The HIPAA Security Rule

11

- The HIPAA security rule has additional requirements regarding how ePHI is accessed, stored, displayed, and transferred electronically.
- 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

12

- A. As part of the workforce team in a healthcare system, you may or may not be provided with computer access.
- B. All healthcare systems have special safeguards in place to protect PHI.
- C. HIPAA and healthcare systems require unique identifiers (passwords) to access computer applications or systems that contain patient, client or resident information.

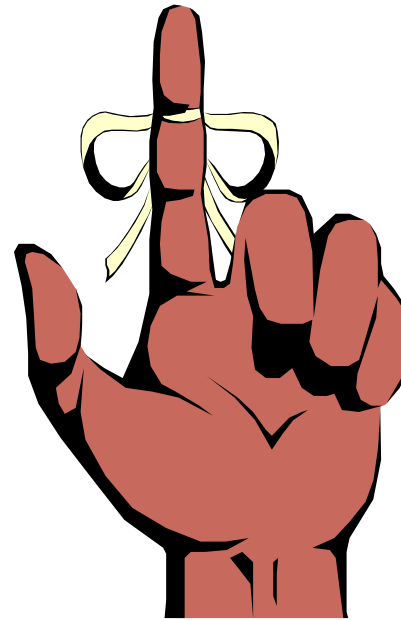
Always remember:

13

YOU MUST SAFEGUARD THE PRIVACY AND SECURITY OF PHI.

This rule must be followed at school, clinical sites, all workplace settings, and during your free time.

**YOU MUST SAFEGUARD THE
PRIVACY AND SECURITY OF PHI
AT ALL TIMES.**



Patient Privacy Rights

14

Under HIPAA, patients have the **right to:**

- A. Access their health information.
- B. Request an amendment to their PHI if they feel the information is incomplete or inaccurate.
- C. Request a place to receive PHI.
- D. Request restrictions on what PHI can be disclosed.
- E. Request an accounting of what PHI has been disclosed.

Caution: Technology/Social Media

15

- A. In addition, confidential information should not be transferred to or from, or stored within, **any form** of personal technology (e.g. personal computers, cell phones, etc.) .
- B. Confidential information should **never** be shared in any form of social media outlet such as Facebook, YouTube, Snapchat, Twitter, Instagram, etc.
- C. Video and audio recordings and taking images (pictures) via cell phones or any other electronic device is **not permitted**.
- D. Text messaging is **not permitted**.



Examples: Social Media

16

- A. Do not comment regarding clinical site patients on Facebook, Twitter, Instagram, Snapchat, etc. - even if **not** mentioning a patient's name.
- B. Do not text or take pictures in work areas.
- C. Do not save any PHI on a jump (USB) drive.



For Students and Instructors with Computer Access

17

- A. 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.
- B. Protect your password and keep it secure.
- C. Do not share it with others on the workforce team.
- D. Do not write it or store it in a place accessible by others.
- E. Use a “strong” password (avoid pet names, sports team names or phone numbers, etc.).

Access to Your Own Patient Information

18

- You may not access your own record while in your student role.
- To access your medical information, you must follow the organization's process for access to patient's information.



YOUR ROLE IN CONFIDENTIALITY, PRIVACY, AND SECURITY OF PHI



Physical Privacy and Security

20

- A. Dispose of printed PHI in secure recycling/shredding bins – **never** remove PHI from unit/facility. There should be no patient identifying information on anything that leaves the facility.

- B. Labels (bottles, IV bags, other) containing PHI should be discarded in privacy bins or “blackened out” prior to discarding.

- C. The sharing of patient/resident PHI should be done in a private and secure manner (not in the hallway, break room, cafeteria, elevator, etc.) on a need to know basis.

Physical Privacy and Security

21

Never share PHI with family, friends or acquaintances.

Examples:

- A. *Do not share that you saw your neighbor at the hospital today.*
- B. *Do not share that you cared for a friend or neighbor.*
- C. ***HIPAA rules exist inside and outside the facility at all times.***

Physical Privacy and Security

22

- A. Workstations (computers) should be logged off when not in use.
- B. Turn screens away from public view. Use privacy screens.
- C. Do not send emails containing ePHI unless the information is encrypted or safeguarded in some other manner.
- D. Students must use their **school** email accounts for any clinical related communications.

Tips for Students/Instructors

23

- A. Report suspicious behavior by others to security or information services departments.
- B. Never leave medical records/films in an open area, including census printouts or other documents.
- C. Do not share information learned about anyone when at a clinical site with others (friends, family, acquaintances, etc.).
- D. Do not discuss or access cases or PHI of patients you are not directly involved with.
- E. Do not use any patient identifiers such as; name, date of birth, and/or medical record number **on assignments**. This includes **unique physical** identifying information.

Tips for Students/Instructors

24

- For example, if a friend says, “I heard Mary Smith is in the hospital. Did you see her there?” You should respond something like, “I cannot share information about patients.”
- The easiest way to remember how to implement this law is the saying;

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

Compliance

25

- Corporate integrity or “corporate compliance” means an organization is abiding by high moral principles and standards set out by that organization.
- The HIPAA Privacy and Security rules are an example of an area of compliance for healthcare systems and facilities.

Compliance Plans

26

Healthcare systems include the following in their compliance plans:

- **General standards of workforce conduct are established.**
- **Rules and regulations that healthcare systems must follow.**

Compliance Plans

27

The rules that healthcare systems must follow are:

- A. Health Insurance Portability and Accountability Act (HIPAA)
- B. False Claims Act (FCA)
- C. Anti-Kickback Statute (AKS)
- D. Physician Self-Referral Prohibition (also called the Stark Law)
- E. Emergency Medical Treatment and Active Labor Act (EMTALA)
- F. Fraud and abuse in billing

False Claims Act (FCA)

28

- 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

29



- 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

30

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

Emergency Medical Treatment and Active Labor Act (EMTALA)

31

- This EMTALA law pertains only to those facilities who have a designated Emergency Department.
- 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).

Fraud and Abuse in Billing

32

- This refers to knowingly billing for services **not** 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.

Reporting Compliance Issues

33

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.



A final reminder...

34

- 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.

Source: www.hhs.gov/hipaa