Guadalupe Regional Medical Center

Health Insurance Portability & Accountability Act (HIPAA)

By Debby Hernandez, Compliance/HIPAA Officer

HIPAA Privacy & Security Training

Module 1

This module will address primary responsibilities in maintaining the privacy and security of sensitive information and protected health information (PHI) at GRMC

During this training you will learn:

- HIPAA Privacy & Security Rules
- Patient identifiers under HIPAA
- How to recognize situations in which confidential and protected health information can be mishandled
- Ways to protect PHI
- That employees will be held responsible if they mishandle confidential or protected health information

Forms of Sensitive Information

Sensitive information exists in various forms….

printed

spoken

electronic

It is the responsibility of every employee to **protect the privacy and security of sensitive information** in ALL FORMS.

Examples of Sensitive Information

- Social Security Numbers
- Credit Card Numbers
- Driver's License Numbers
- Personal Information
- Individually Identifiable Health Information

The improper disclosure of sensitive information present the risk of identity theft, invasion of privacy, and can cause harm and embarrassment to staff and patients at GRMC.

What is the Health Insurance Portability & Accountability Act

The Health Insurance Portability & Accountability Act, more commonly known as HIPAA, is a federal law designed to protect a subset of Sensitive Information known as protected health information (PHI).

The law was:

- Established in 1996
- Implemented April 14, 2003
- Last amended January 25, 2013

This module focuses on two primary areas under HIPAA:

- HIPAA Privacy Rule
- HIPAA Security Rule

Section I – Part A
HIPAA Privacy Rule

Overview

HIPAA Privacy Rule

Basically, the HIPAA Privacy Rule states that covered entities have a duty to protect PHI. A "covered entity" is:

- A health plan
- A health care clearinghouse
- A health care provider who transmits any health information in electronic form in connection with a covered transaction.

* This definition is not identical for the State of Texas. Under new regulations, Texas captures many more organizations and entities under a broader definition.

Protected Health Information (PHI) defined

Protected Health Information or PHI is generally defined as:

- Any information that can be used to identify a patient – whether living or deceased and which relates to the patient's past, present, or future physical or mental health condition, including health care services provided and payment for those services.

Employees may access PHI
only when necessary to perform their job-related duties

Any of the following are considered identifiers under HIPAA

- Patient names
- Geographic subdivisions (smaller than state)
- Telephone numbers
- Fax numbers
- Social Security numbers
- Vehicle identifiers
- E-mail addresses
- Web URLs and IP addresses
- Dates (except year)
- Names of Relatives
- Full face photographs/images
- Healthcare record numbers
- Account numbers
- Biometric identifiers (fingerprints)
- Device identifiers
- Health plan beneficiary number (example: MCR number)
- Certificate/license numbers
- Any other unique number or characteristic that can be linked to an individual

HIPAA Violation

In general, HIPAA violations are enforced by the Department of Health and Human Services. However, regulations now permit states to bring **civil actions** AND **monetary awards** to be shared with harmed individuals.

A healthcare facility and an employee were sued by a patient who alleged the facility sent documents containing her protected health information to a shared office fax machine in her place of business without her consent, causing her great embarrassment. Although the PHI was related to the employee's disability claims, it was sent to the wrong fax machine located in a common area of her office

Confirm authorization instructions and verify telephone numbers before faxing.

Employee Access

Having so much information on a computer system allows for better continuity of care but also opens up the opportunity for **inappropriate access**

Employees must follow the hospital's policies and procedures regarding Confidentiality / HIPAA guidelines and always use good judgment when accessing patient information

Access Must Be Authorized

An employee may only access or disclose a patient's PHI when this access is **part of the employee's job duties.**

If an employee accesses or discloses PHI without a **patient's written authorization** or without a **job related reason** for doing so, the employee violates hospital policy and HIPAA.

Unauthorized Access

It is **never acceptable** for an employee to look at PHI "just out of curiosity", even if no harm is intended.

It is **never acceptable** for an employee to access his/her own health information. This is against hospital policy.

It **makes no difference** if the information relates to a VIP or a close friend or family. All information is entitled the **same protection and must be kept private**.

These rules apply to all employees and health care professionals.

Be aware that accessing PHI of someone involved in a divorce, separation, break-up, or custody dispute may be an indication of intent to use information for personal advantage, unless the access is job related. Such behavior will be considered by GRMC when determining disciplinary action.

HIPAA Violation

A former UCLA Health System employee became the first person in the United States to receive **jail time in a federal prison for a misdemeanor HIPAA offense.** The employee used his access to the University's electronic medical records to view medical records of his supervisors, co-workers, and high profile patients. While none of the information was "used" or sold, the access was illegal because the employee **lacked a valid reason for looking at the records.**

The ex-employee pled guilty to four misdemeanor counts of violating HIPAA.

His sentence was four months in prison and a $2,000 fine.

Breaches

A breach occurs when PHI or sensitive information is:

- Lost or stolen (i.e., losing a mobile phone or laptop computer which contained PHI)
- Improperly disposed of (i.e., documents containing PHI were not shredded)
- Accessed by people or programs that are not authorized to have access (i.e., someone hacking our computer system)
- Communicated or sent to others who have no official need to receive it (i.e., faxing PHI to the wrong individual)

What if there is a breach?

Part of your responsibility as a hospital employee is to report privacy or security concerns involving PHI to the Compliance/HIPAA Officer.

Debby Hernandez serves as the Compliance/HIPAA Officer and may be reached at (830) 401-7100. The Compliance/HIPAA Officer is ultimately responsible for investigating HIPAA complaints.

Employees, volunteers, or contractors of GRMC may not threaten or take any retaliatory action against an individual for filing a HIPAA complaint.

The Hospital is required to take *reasonable* steps to lessen effects of any breach, which may include notifying the individual whose information was breached and reporting the breach to the Secretary of Health & Human Services.

Penalties for breaches

Breaches of the HIPAA Privacy and Security Rules may result in serious consequences. In addition to possible disciplinary actions imposed by GRMC, breaches may also result in civil and criminal penalties.

Guadalupe Regional Medical Center may also be required to notify potentially affected individuals of breaches involving their PHI.

Breach Notification Requirements

Improper disclosures or breaches of protected health information may require notification to authorities. Depending on the nature of the breach, notifications may have to be made to:

- The Department of Health and Human Services,
- All individuals whose information was breached, and
- The media

Quick Review

- Sensitive information exists in many forms: printed, spoken, and electronic.
- Sensitive information includes Social Security numbers, credit card numbers, driver's license numbers, personnel information, and PHI.
- Two primary HIPAA regulations are the Privacy Rule and the Security Rule
- An employee must have a patient's written authorization or a job-related reason for accessing or disclosing patient information.
- Breaches of privacy and security information may result in civil and criminal penalties, as well as hospital disciplinary procedures. Employees must report breaches to the HIPAA Officer.

Section I – Part B
HIPAA Privacy Rule

Program Components

HIPAA Program Components

HIPAA address several areas under the Privacy Rule. I will highlight a few of the areas, including:

- Individual Patient Rights
- Minimum Necessary Rule
- Special Circumstances as indicated in the Guadalupe Regional's Notices of Privacy Practices

Patient Rights

HIPAA not only provides requirements for healthcare organizations (covered entities) with regards to protecting PHI, but it also created several patient rights under the Privacy Rule.

Under this rule, patients have the right:

- To receive GRMC's Notice of Privacy Practices
- To Inspect and Copy their medical records
- To Amend their records if they feel information is incorrect or incomplete
- To an Accounting of Disclosures
- To Request Restrictions
- To Request Confidential Communications
- To Be Notified Of A Breach In Their Health Information
- To File a Complaint in the event the rights have been denied or PHI is not protected

“Minimum Necessary” Rule

Under the HIPAA Privacy Rule, when the use or disclosure of PHI is permitted, only the **minimum necessary information** may be disclosed. However, this does not restrict the ability of physicians, nurses, and other healthcare providers to share information needed to treat patients, process payments, or carryout healthcare operations.

Disclosures of PHI

HIPAA regulations permit use or disclosure of PHI for:

- Providing medical **treatment**
- Processing healthcare **payments**
- Conducting healthcare **operations**

Employees **may not** otherwise access or disclose PHI unless:

- The patient has given written permission
- It is within the scope of the employee's job duties
- Permitted by law

Special Circumstances

Guadalupe Regional identifies special circumstances that require the patient's permission and/or written authorization in order for information to be shared.

The following is a listing of some common situations where patients will be asked for permission and/or written authorization to release information.

- Release of patient information on the hospital's directory
- Release of patients religious affiliation to members of the clergy
- Release of information to individuals involved in your care
- Release of PHI for marketing and fundraising use
- Release of a patient's psychotherapy notes
- Sale of PHI

Special Circumstances (Continued)

Authorization for these special circumstances may be canceled at any time in writing. If a patient cancels the authorization, GRMC will no longer use or share information about you for the reasons listed or covered by your written authorization.

Marketing & Fundraising

Without an authorization, GRMC may not use information about the medical treatment of an individual for **targeted** fundraising or marketing.

The Notice of Privacy Practices and other general fundraising and marketing communications must advise patients of the right to **"opt out"** of being contacted for fundraising and marketing purposes.

Business Associates

An outside company or individual is a HIPAA Business Associate of the Hospital if they provide services involving PHI that is maintained by the Hospital.

Under HIPAA, a Business Associate must:

- Enter into a Business Associate Agreement with the hospital
- Use appropriate safeguards to prevent the use or disclosure of PHI other than as permitted by the contract
- Notify the hospital in the event of a breach
- Ensure that their employees and subcontractors received HIPAA training
- Protect PHI to the same degree as the hospital

Quick Review

- Under the HIPAA rule, patients have designated rights.
- The Hospital may use or share only the minimum necessary information to perform its duties.
- HIPAA permits disclosure of PHI for treatment, payment, and healthcare operations.
- The Hospital must obtain an individual's specific authorization for certain circumstances, including but not limited to marketing or fundraising.

Section II
HIPAA Security Rule

Overview

HIPAA Security Rule

The HIPAA Security Rule concentrates on safeguarding protected health information (PHI) by focusing on the confidentiality, integrity, and availability of PHI.

- **Confidentiality** means that the data or information is not made available or disclosed to unauthorized persons or processes.
- **Integrity** means that the data or information has not been altered or destroyed in an unauthorized manner.
- **Availability** means that the data or information is accessible and usable upon demand only by an authorized person.

Security Standards/Safeguards

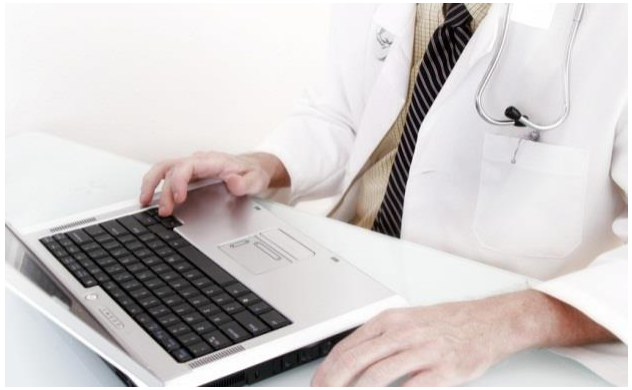
The Hospital is required to have **administrative**, **technical**, and **physical** safeguards to protect the privacy of PHI.

Safeguards must:

- **Protect PHI** from accidental or intentional unauthorized use/disclosure in computer systems (including social networking sites such as Facebook, Twitter and others).
- **Limit accidental disclosures** (such as discussions in waiting rooms and hallways); and
- **Include practices** such as document shredding, locking doors and file storage areas, and use of passwords and codes for access.

HIPAA Violation

A physician at Westerly Hospital in Rhode Island was fired for posting information on Facebook about a patient she treated. Although the posting did not reveal the patient's name, there was enough information that others could easily identify him or her. The information also indicated the patient had problems with alcohol and marijuana abuse.



Hospital employees should never disclose work related sensitive information through social media such as Facebook and Twitter.

Malicious Software

Viruses, worms, spyware, and spam are examples of malicious software, sometimes known as “malware.” To minimize the spread of malicious software, employees should:

- Use the hospital’s anti-virus and anti-spyware software.
- Use safe internet browsing habits
- Minimize personal use of the internet

Safe Email Use

- An employee whose work involves the transmission of sensitive information or PHI **must encrypt** the data **UNLESS** the data is transmitted within the hospital network. Employees sending transmissions containing PHI (outside of the hospital network) should consult with the Compliance/HIPAA Officer for approval and/or to ensure proper safeguards are in place.

- Do not open email attachments if the message looks suspicious. "When in doubt, throw it out"

- Do not respond to "spam" – delete the email.

Password Control

- Use strong passwords where possible (at least 6 characters, containing a combination of alpha-numeric).
- Change your passwords frequently to prevent hackers from using automated tools to guess your password (at minimum bi-annually).
- It is a violation of hospital policy to share your password with anyone. Electronic audit records track information based on activity associated with User IDs.

The Compliance/HIPAA Officer uses audit reports based on User IDs. If you share your password to an individual and that individual accesses information inappropriately, it will be **YOUR ID** associated with the access.

Mobile Devices

If you use mobile computing devices such as laptop PCs, PDAs such as iPads, iPhones, Blackberrys, smart phones, or regular cell phones to store and send information, do not send PHI.

Employees are required to utilize the following security controls when storing and transmitting sensitive information.

- Strong power on passwords (numeric, pattern, etc)
- Automatic log-off
- Screen lock at regular intervals while the device is inactive.

Laptop PCs which are used as part of your job related activities **must have encryption is place.**

Never leave mobile devices unattended in an unsecured area.
Immediately report the loss or theft of any mobile device.

HIPAA Violation

Martin Memorial Center in Florida took disciplinary action against several employees for taking pictures of a shark attack victim with their cellular phones. Penalties for employees who took the photos ranged from written warnings and demotions to suspension.

Portable Storage Devices

Whenever possible, avoid using external storage devices to store Sensitive Information and PHI. If you must store Sensitive Information or PHI, ensure you have at minimum a password and auto lock on your storage device. Additional securities such as **ENCRYPTION** are also available on most phones.

- Use portable storage devices only for **transporting** information, and not to permanently store information.
- Once information has been used, **erase** it from the device.
- Ensure safe keeping of portable devices.
- Immediately report loss of any storage device to the Director of Information Technology at extension 7523.

Remote Access

All computers and mobile devices used to connect to the hospital's network or systems from home or other off-site location should meet the same **minimum safety standards** that apply to your work PC. Anyone requesting Remote Access must receive approval by his/her Administrator and the Compliance/HIPAA Officer.

To ensure safeguards are in place, employees should:

- Make use of the hospital's Virtual Private Network (VPN) at home or off-site and transmit PHI **only** to locations within the hospital's network, otherwise the data must be **ENCRYPTED**.
- Run Windows Update or the update features of the particular operating software.
- Keep anti-virus software up to date.

Communications in Public Areas

Be aware of your surrounding when discussing Sensitive Information, including PHI. Do not discuss sensitive information or PHI in public areas.

Use caution when conducting conversations in:

- **Semi-private rooms**
- **Waiting Areas**
- **Corridors**
- **Elevators**

Appropriate Disposal of Data

Observe the following procedures for the appropriate disposal of sensitive information, including PHI.

- Paper should be properly shredded or placed in a secured bin for shredding later.
- Magnetic media such as disks, tapes, or hard drive must be physically destroyed or "wiped" using approved software or procedures.
- CD ROM disk must be rendered unreadable by shredding, defacing the recording surface, or breaking.
- For more information on appropriate disposal of data, contact the Director of Information Technology.

Sensitive information and PHI should never be placed with the regular trash.

Physical Security

Equipment such as PCs, servers, mainframes, fax machines, and copiers must be physically protected.

- Computer screens, copiers, and fax machines must be placed so that they cannot be accessed or viewed by unauthorized personnel.
- Computer systems with access to patient information must be **LOGGED OFF** or **SUSPENDED** when left unattended.
- Servers and mainframes must be in a secure area where physical access is controlled

Disciplinary Actions

Employees who violate the Guadalupe Regional Medical Center's HIPAA and confidentiality policies or guidelines will be subject to **disciplinary action** as well as possible **criminal or civil penalties.**

Employee Responsibilities

- Comply with hospital policies and guidelines.
- Access information only as necessary for your authorized job responsibilities.
- Keep your passwords confidential.
- Immediately report HIPAA Privacy and Security concerns.
- Avoid storing sensitive information on mobile devices and portable media, and if you must, make sure the device is encrypted.
- Always keep portable devices physically secure to prevent theft and unauthorized access.
- Follow procedures for proper disposal of PHI.
- Do not hold discussion of PHI in public areas.