HIPAA/HITECH

HIPAA PRIVACY AND SECURITY

Today more than ever before people are concerned about how their private health information can be used, shared or released without their knowledge and:

How it is kept secure in an electronic world

What is HIPAA??

- Health Insurance Portability and Accountability Act
- To assure health insurance portability
- To reduce health care fraud and abuse
- To enforce standards for the use and disclosure of protected health information (PHI)
- To guarantee the security and privacy of health information

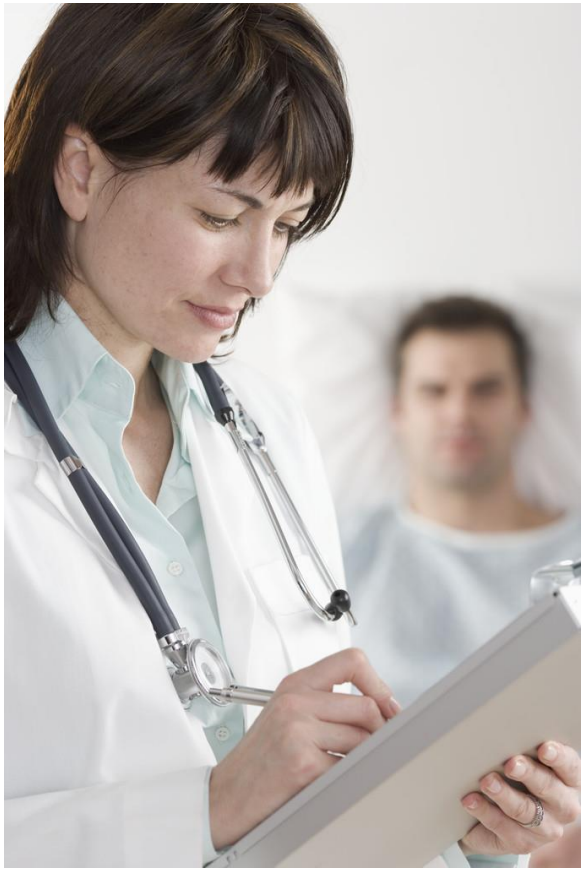
There are 3 standards

PRIVACY

SECURITY

ELECTRONIC

THE PRIVACY STANDARDS



The goal of the Privacy Standards is to protect and limit access to PHI (Protected Health Information). PHI is **individually identifiable** information that relates to health status, provision of healthcare, or payment for healthcare.

What Makes Info Individually Identifiable

- When health/billing information is linked to a person
- Common identifiers that would link info to an individual include names, social security numbers, addresses, and birth dates.
- Before disclosing any information (for purposes other than treatment, billing, or healthcare operations) without a written consent from a patient you MUST make sure it is de-identifiable by removing any identifiers.

Examples of PHI

- Resident's name and diet order
- Resident's SS# and diagnosis
- Resident's name associated with their address (if in a healthcare facility)
- A list of DOB's with associated medical tests ordered
- Medical record number with a diagnosis
- PHI can be verbal, written, electronic

When Can We Use/Disclose PHI

- PHI can be used/disclosed for the purposes of treatment, billing, and healthcare operations.
- Any other use or disclosure (sharing info) requires consent from the individual/patient.

Examples: We are allowed to send health information to hospital with patient because it is for treatment.

We would require patient consent to share health information with an attorney that requests their records because it is not for treatment, billing purposes, or healthcare operations of the facility.

How do we dispose of PHI?

- In resident care areas (nurses stations/clinic etc) place PHI in locked bins which will be picked up and shredded.
- In private offices maintain a box and when needed take in person to medical records to be placed in large bins for shredding.
- **NEVER put documents that contain PHI on them in the garbage!**

Breach

- A breach is an **impermissible** use or disclosure of unsecured PHI under the Privacy Rule that compromises the security or privacy of the protected health information.
- All written/printed PHI needs to be discarded in a shred bin for proper disposal.

Privacy is the right of an individual to control his/her personal information and to not have it divulged or released or used without permission.

- **The three security safeguards are**
- 1. **Administrative** safeguards that limit access by establishing and enforcing policies and procedures
- 2. **Physical** safeguards that limit access by use of a physical barrier such as locks on doors where PHI is stored or moving a computer screen so it cannot be seen
- 3. **Technical** safeguards that limit access to information stored electronically by the use of passwords, virus protection or by placing limitations on software

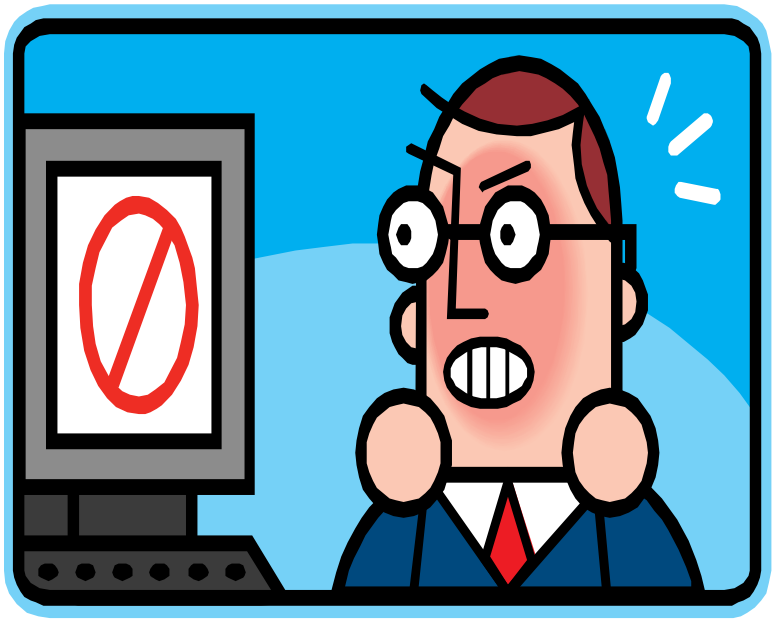
- The facility must limit access to who can access/obtain PHI inside and outside of the facility
- Masonic Pathways must make sure that resident PHI will not be accidentally or maliciously altered or destroyed and kept secure and confidential but still readily available to staff that need to use it.

Definitions to know:

- **Minimum necessary rule-**you will have what you need to do your job- if it is information that you do not need to do your job then you should not be looking at it
- **ePHI-**Electronic Protected Health Information-computer, fax, e-mail or any electronic device

Security/Computer System Access

- All staff that require access to a computer will have a password, staff will change the password at a minimum of every 90 days and never share their passwords with anyone else.
- Use encrypted devices



Records Requests

- All requests for patient records MUST go through the Medical Records Department in order to ensure that proper consent is obtained when necessary and an accounting of the disclosure is maintained.

What is HITECH

- Health Information Technology for Economic and Clinical Health
- Made changes to HIPAA privacy and security requirements, increased monitoring and enforcement:

-Added Breach Notification Rule: Any disclosure (sharing) of PHI that violates the privacy rule must be reported to the individual whose information was breached, the Department of Health and Human Services (HHS), and in certain cases the media.

More terms to know

- Security breach or security incident-refers to unauthorized access to an organization's electronic database-from criminal invasion to natural disasters
- Privacy officer – Vicki Ritz X 3855
- Security Officer - Phil Troyer X 3816

- All staff must actively protect and safeguard PHI. **All staff must notify their immediate supervisor, the Privacy Officer/Security Officer or any member of the management upon learning of any breaches of PHI or other violations of this policy.**

Identity Theft Protection

- The security officer also administers the Masonic Pathways Identity Theft Prevention Program
- Staff are trained to recognize any "Red Flags" on admission and act upon them as necessary to protect fraudulent activity
- All service providers at Masonic are also required to comply with the Identity Theft Prevention Program

Examples of Violations

- Talking about PHI in public areas like hallways
- Accessing PHI you do not need to do your job/looking at a patient's record that you are not assigned to.
- Talking/sharing PHI with unauthorized individuals and/or anywhere outside of work including on social media (avoid even using first names only)
- Disclosing that a patient is at Pathways without receiving their written consent (unless disclosing to person in building that specifically asked for patient by name)

Violations

- Individuals not following established policies and procedures who act in a way or omit a practice that results in a violation can result in disciplinary action, including immediate discharge.

Safeguards to Practice Everyday

- Do not share passwords
- Use fax cover sheets/program frequently used numbers into fax to decrease sending PHI to unauthorized individuals
- Limit use of PHI in e-mails or use encryption
- Limit Discussion of PHI to private areas
- Do not release PHI/patient information if you are unsure if the disclosure is allowed
- Consult Medical Records/Privacy Officer/Security Officer

Practice Daily

- Ask if you are using/sharing the minimum amount of PHI necessary to accomplish the goal
- Limit attendees at meetings where PHI is discussed to those that require the information to do their jobs
- Follow policy/procedure. If you don't know ask or look it up.
- Log out from computer (minimize screen if close by)
- Turn resident meal tickets face down in dining room to prevent public viewing.

Confidentiality Statement

- At the end of the post test please read and ensure you understand the confidentiality statement prior to signing your name.