HIPAA

Health Insurance Portability and Accountability Act of 1996

Protected Health Information (PHI)

- Covers patient information in any form – written, verbal, or electronic
- PHI Includes
  - Any information that can be used to identify the patient such as: name, address, social security number, medical record number, telephone number, patient account number
  - Anything about the patient's medical conditions and treatment – past, present, or possible
  - Billing and Payment records

**Breaches can occur even if you de-identify

Why is Privacy Important?

- It is a patient's right
- It builds trust between the patient and their caregivers
- It contributes to customer satisfaction
- It allows us to provide quality care

Before You Access Patient Information, Ask Yourself:

1. Is the patient information I am about to access necessary for me to complete my job?
2. Am I accessing only the minimum necessary to complete my job, no more and no less?
3. If I am accessing, using, or disclosing this information, should I have a signed authorization from the patient?

When is it Okay to Share PHI?

- Share only the minimum amount of PHI necessary to fulfill the job responsibility
- Share PHI only with those with a clinical or business need to know
- Share only the amount of PHI requested. The entire medical record may not be needed.

Examples of Minimum Necessary

- A billing clerk may need to know what laboratory test was done, but not the result
- An admissions clerk does not need to have access to the full medical record in order to carry out his/her job
- A patient transporter typically does not need to access the full medical record to do his/her job

Snooping and Casual Disregard… Our Greatest Risk

- Accessing the medical records of family members, friends, ex-spouses, neighbors, celebrities, etc.
- Failure to verify the authority of the individual receiving the PHI
- Improper use of technology such as camera phones, texting, and social networking sites
- Employees exceeding their scope of job duty

Incidental Uses & Disclosures

- An incidental use or disclosure is not a violation of HIPAA provided the facility has applied reasonable safeguards and implemented the minimum necessary standard.
- Examples of incidental uses and disclosures:
  - Discussions during teaching rounds
  - Calling out a patient's name in the waiting room
  - Sign in sheets in hospitals and clinics containing the minimum information necessary

Protecting Patient Privacy

DO:

- Close curtains and speak softly when discussing treatments in semi-private rooms
- Log off of the computer when not attended
- Dispose of patient information in accordance with hospital policy and procedure
- Clear patient information off of your desk and place in a secure location when not in use
- Verify fax numbers and addresses before sending PHI

Protecting Patient Privacy

DO NOT:

- Discuss a patient in public areas such as elevators, hallways, cafeteria, or outside the facility or office
- Share your computer username, ID, or password
- Look at information about a patient unless you need it to do your job
- Take information about patients (including nursing report notes) home
- Discuss patient information in front of visitors without explicit, documented authorization of the patient
- Post any patient related information in church bulletins, newsletters, Facebook, or any other social networking websites
- Bring friends or family into areas of the facility or clinic where they can see or hear patients receiving care or where they might have access to PHI

Sharing PHI with Family & Friends

- The patient must be given the opportunity to agree, restrict, or object to providing PHI to family members, friends, or others identified by the patient as involved in the patient's care or payment for health care
- Document the patient's decision
- Use professional judgment to determine if disclosing PHI would be in the patient's best interest if the patient is unable to agree or object

Areas of Concern: Friends/Family/Self

- When you are seeking information on your family, friends, or yourself, you are not acting as an employee and you must access PHI using the procedures required for non-employees. This means you need a written authorization for release of information which can be obtained in Medical Records
- You are *not* permitted to access your own medical records

Areas of Concern: Employees as Patients

- Information available to the facility as a healthcare provider is not generally available to it in the role of an employer. For example, if an employee comes into the ED – his/her supervisor or co-workers should not be accessing his/her ED information
- This can be a challenging area: call the Facility Privacy Officer if questions arise

Examples of Potential HIPAA Violations

- Text messaging medical information about a patient to anyone!
- An employee passing on information to her son about his spouse or their children
- Allowing a former employee, friends, family, or co-workers into off-limits areas where PHI is located – this includes children
- Taking pictures of patients with a cell phone camera

Examples of Potential HIPAA Violations

- Releasing information to a caller who is not properly identified as being authorized to receive information
- Mailing/faxing PHI to the wrong person
- Looking at the PHI of a co-worker, supervisor, family, friend, or self for non-work reasons
- Posting information about a patient or specific information about a day at your workplace on a social networking site such as Facebook

No Excuses

- Good intentions such as "I needed to let his mother know he was in the hospital" or "She is my best friend and she wouldn't mind me looking" do not count.
- Just plain nosiness is NO excuse.

What can happen if I violate UPHS Policy or break the law?

- State and federal authorities may hold workforce members individually responsible for their actions
- Charged fines from $100 to as much as $1,500,000
- Criminal prosecution and jail time may occur depending on the type of violation
- Civil suits by state Attorney General against the facility
- Violation of UPHS policy will result in disciplinary action up to and including termination

Reporting Suspected Violations

- Suspected HIPAA violations should be reported to:
  - Your Supervisor
  - The UPHS – Portage Privacy Officer: Beth Agen - (906) 483-1518
  - The HSC Privacy Officer and Director of Ethics & Compliance: Tina Qualls – (615) 920-7412
  - LifePoint Compliance Line: 1-877-508-LIFE (5433)

    **you will remain anonymous using this route

Non-Retaliation

- UPHS policy and state and federal laws provide protection from retribution or retaliation against any person for reporting actual or suspected violations.

COMPLIANCE IS NOT AN OPTION – IT IS MANDATORY

- Compliance with HIPAA is part of our culture
- Compliance with HIPAA is part of your job responsibilities
- Noncompliance may result in disciplinary action up to and including termination
- Noncompliance may also result in civil and/or criminal penalties

UPHS Protect Patient Privacy by:

- Assigning a facility Privacy Officer: Beth Agen - (906) 483-1518
- Having written policies and procedures to help employees understand the privacy rules
- Putting in place ways to protect health information from being misused
- Having a way for patients and others to file complaints
- Providing discipline for employees who don't follow the privacy practices

Facility Directory Disclosures

- The patient must be given the opportunity to opt-out from the directory
- Unless the patient opts-out, the following PHI may be included in the facility directory and given to those individuals who inquire about the patient by name:
  - Name
  - Location
  - Condition of the patient in general terms (e.g. good, critical, serious)
  - Only members of the clergy may have access to the religious affiliation of the patient, if provided
- If the patient has opted-out of the patient directory, no information may be discussed. Simply say, “I have no information on that person.”

Patient Rights

- Under the HIPAA Privacy Regulations, patients have the right to:
  - Receive the Notice of Privacy Practices
  - Inspect and request a copy of their PHI
  - Know to whom their information is being disclosed to in certain situations
  - Request restrictions on use and disclosure of their PHI
  - Request an amendment to their PHI
  - Request confidential communications of their PHI

Case Study

- While working on the fourth floor, Suzy from ES noticed that her neighbor Patty Patient was walking down the hall in a hospital gown and pushing an IV pole. When Suzy went home later that day, she tells her husband that she saw their neighbor on the cancer unit.

- *Is this a HIPAA Violation? Why?*

Case Study Response:

- Yes, this is a HIPAA Violation. Patty Patient must be given the opportunity to agree, restrict, or object to providing PHI to family members, friends, or others identified by the patient as involved in the patient's care or payment for health care.

Case Study

- Patty Patient is waiting in the outpatient clinic. Nurse Jones enters the waiting room and calls out, “Patty Patient.”
- While still in the waiting room, Nurse Jones asks Patty, “Have you been taking your Prozac for your depression?”

- *Is this a HIPAA Violation? Why?*

Case Study Response

- While it is not a HIPAA violation to call out the patient's name in the waiting room, it is a HIPAA violation to ask about her medication and health information. PHI must only be discussed in private areas where others cannot overhear. If in a semi-private room, curtains should be closed and discussion kept at a soft level to avoid others overhearing.

Case Study

- Nurse Jane sees an employee looking through the medical records to find out medical information about another employee who is a patient in the facility, but the employee is not one of the caregivers for the patient.

- *What should Nurse Jane do?*

Case Study Response

- Nurse Jane should report the incident immediately to one of the following:
  - Her Supervisor
  - The UPHS – Portage Privacy Officer: Beth Agen - (906) 483-1518
  - The HSC Privacy Officer and Director of Ethics & Compliance: Tina Qualls – (615) 920-7412
  - LifePoint Compliance Line: 1-877-508-LIFE (5433)

    **she will remain anonymous using this route
- Remember, Nurse Jane is protected by UPHS policy and state and federal laws from retribution or retaliation for reporting the suspected violation.

To Recap:

- UPHS – Portage is committed to patient privacy
- All complaints regarding patient privacy will be taken seriously
- The facility will investigate all privacy complaints
- Employees who violate the HIPAA privacy policies and procedures will be subject to disciplinary actions which could include verbal or written warnings, suspension from duties, or termination
- Retaliation against any person for reporting actual or suspected violations will not be tolerated

Final Thoughts

- Confidentiality and protecting PHI is everyone's job
- Privacy Matters! Do not discuss protected healthcare information in public or with those who do not need to know
- Do not get casual about privacy and confidentiality

- Remember… It could be YOUR health information that someone is talking about.