HIPAA/HITECH Keys to Success

Education for Students

West Florida HOSPITAL

Student Responsibility

- Your student affiliation with West Florida Hospital may involve the exchange of protected health information.
- As a student, you have a legal and ethical responsibility to safeguard the privacy of all patients and to protect the confidentiality of patient health information.
- Failure to comply with West Florida Hospital privacy and information security policies may result in removal from on-site participation.

Confirm your Commitment

- In the course of your assignment at West Florida Hospital, understand that you may come into the possession of protected health information and/or confidential (company) information.
- Access and use this information only when it is necessary to perform your student-related duties in accordance with the hospital's Privacy and Security Policies.
- Understand that you may be asked to sign and comply with the hospital's Confidentiality and Security Agreement in order to obtain authorization for access to Confidential Information.

Review of Federal Law

What is HIPAA? A federal law - **H**ealth **I**nsurance **P**ortability and **A**ccountability **A**ct

What is HITECH? A federal law - **H**ealth **I**nformation **T**echnology for **E**conomic and **C**linical **H**ealth Act

As a covered entity, compliance with HIPAA and HITECH is mandatory and there are penalties for failing to comply with these federal laws.

Compliance includes mandatory training for all members of our workforce, including students.

WFH Demonstrates Compliance

West Florida Hospital has a comprehensive Patient Privacy & Information Security Program which includes:

- An appointed FPO (Facility Privacy Official) Debbie Wroten
- An appointed FISO (Facility Information Security Officer) Jeff Amerson
- Comprehensive patient privacy & information security policies
- Job-specific patient privacy and information security training
- A published Notice of Privacy Practices distributed to each patient
- Designated shredding containers for disposal of protected health information.
- Patient issued passcodes for sharing information with patient family members and friends.
- Role-based access to information systems including unique assigned user log-ins and individual passwords
- Safeguards to protect health information from any intentional or unintentional use or disclosure that is in violation of privacy policies, the HIPAA Privacy Rule, or HITECH
- Routinely monitor s for compliance with privacy/information security policies and procedures, to include rounding, audits of information systems, and documenting areas of noncompliance and creating a corrective action and follow-up plan
- Investigation and timely reporting of all privacy and/or information security complaints, concerns, breaches

Use/Disclosure of PHI to Students

- HIPAA allows an individual who is a part of a formalized training program or part of a formal agreement with the facility, where they are learning under supervision to practice or improve their skills to receive protected health information (PHI). It does not allow for an individual who is a friend, or acquaintance to receive PHI.

PHI, Minimum Necessary, and Need-to-Know Principles

- **PHI** - Any oral, written or electronic individually-identifiable health information collected or stored by a facility. Individually-identifiable health information includes demographic information and any information that relates to past, present or future physical or mental condition of an individual.

- **Minimum Necessary/Need-to Know** - Only those workforce members (including students) with a legitimate "need to know" may access, use or disclose PHI. This includes, but is not limited to all activities related to treatment, payment and health care operations. Each workforce member may only access the minimum information necessary to perform his or her designated role regardless of the extent of access provided to him or her.

Patient Privacy Rights under HIPAA

- Right to Access (Inspect & Copy)
- Right to Amend
- Right to an Accounting of Disclosures
- Right to Opt Out of Facility Directory
- Right to Request Privacy Restriction
- Right to Request Confidential Communications
- Right to Receive the Notice of Privacy Practices

Patient Requests/Complaints

- During your assignment to West Florida Hospital, you may receive a request from a patient to invoke a privacy right. It is your obligation to inform your West Florida Hospital preceptor so he/she can contact the FPO.
- Never agree to a patient's request.
- Privacy Complaints should also be forwarded to the FPO.

Disclosing PHI to Family Members/Friends

- Patients are assigned a unique four-digit passcode upon admission.
- Distribution of the passcode is the responsibility of patient
- Family members or friends requesting protected health information must provide the passcode.
- Passcode is the last 4-digits of patient account number.
- The passcode may be changed during treatment, based on written and approved request.

Patient Right to Access

- A patient may request access to or a copy of his or her protected health information (medical record or designated record set).
- Request for access must be made in writing.
- All written requests for access must be sent to HIM (Medical Records) for processing
- Must be able to provide access and/or hard copy of record within 30 days of a request
- If patient is in-house, FPO will manage access process.
- Patient may also be referred to the new Patient Portal to access records.

Patient Right to Amend

- A patient may request to amend of his or her protected health information.
- Request for amendment must be made in writing.
- All written requests for amendment must be forwarded to the Director of HIM for processing.
- Note: For the purpose of this policy, "amend" is defined as the patient's right to add to (or append) information with which he/she disagrees

Patient Right to Opt out of Directory

- The hospital maintains a directory of all hospitalized patients.
- A patient may request to opt out of the directory at anytime during hospitalization. Most requests occur during the registration process, but can occur after admission.
- Request to "opt out" of the directory must be submitted in writing.
- Forward any request for opting out of the directory to Patient Access/Registration and FPO for processing.
- There is a process in place for Meditech to reflect when a patient has requested to "opt out" of the directory.
- Opting out does not apply to outpatients.

Patient Right to Opt out of Directory

- All Meditech modules will reflect a little “c” in front of the patient’s name, which indicates that a confidential flag has been issued for this patient:

cPCCSTUDENT,EDWARD H00000057756 ADM IN 01/14/03 H.810-A

- If a patient has the confidential flag, you may not acknowledge the patient is in the facility or give information about the patient to friends, family or others who may inquire, including phone callers or flower delivery personnel.
- You can release information to family and friends, as long as they provide the passcode as defined in the hospital policy.

Confidential Communications

- Patient may request use of alternate address or phone number for future contact
- The patient's request should be in writing.
- Requests for Confidential Communications must be forwarded to the FPO & Patient Access Department.
- If accepted, the hospital should communicate only to the alternate address or phone number provided.

Right to Privacy Restrictions

- Patients have the right to request a privacy restriction of their PHI.
- All requests for restrictions must be presented in writing.
- The written request for restriction must be routed to the FPO.
- **NEVER** agree to a restriction that a patient may request or question why the patient is requesting the restriction.
- The facility is not required to act immediately. The FPO will investigate the facility's ability to meet the request.

Patient Privacy Complaints

- Patients have the right to file a privacy complaint if they feel their privacy rights have been violated.
- Complaints should be made in writing, but occasionally, the patient may complain directly to a caregiver.
- If so, please gather the following information from the complainant: Name, phone number & address, names of any workforce members who were involved and short summary of the privacy concern.
- **ALL** privacy complaints must be routed to the FPO.
- A Patient may also file a complaint with the Secretary of the U.S. Department of Health and Human Services.

Accounting of Disclosures (AOD)

- Right to an accounting of disclosures of protected health information
- An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested, except for certain disclosures.

What types of disclosures must be accounted for?

Following are common disclosures of protected health information the hospital is required to track:

- State mandated reporting (such as suspected abuse or neglect victims, disease reporting such as STDs, brain injuries, dog bites, etc.)
- Cadaveric organ, eye, or tissue donation purposes
- Disclosures required by law (Gun shot wounds, victims of a crime, reporting a crime in emergencies, court order or court-ordered warrant)
- Decedents: Funeral Home Directors, Coroners and medical examiners
- Health Oversight Activities (i.e., The Joint Commission)
- Faxing patient information to the wrong location or to the wrong clinician
- Disclosure of patient information outside of a "need to know"

Common Privacy/Security Violations

- Discussions of patient information in public places such as elevators, hallways and cafeterias
- Printed or electronic information left in public view
- Patient charts left on counters
- Removing patient information from the facility
- Protected health information placed in regular trash
- Records that are accessed without need to know in order to perform job duties
- Unauthorized individuals hearing patient sensitive information such as diagnosis or treatment
- Disclosing your password or logging onto a computer and allowing someone else to use it.

Privacy/Security Violations & Sanctions

The following categories represent the types of patient privacy/information security violations:

Negligent *– Accidental disclosure or due to lack of education/training*

Purposeful *–An intentional violation of the terms of the Information Security Agreement or Company/Facility Privacy & Security policies; May also include any violation associated with potential for patient harm, such as a breach.*

Violating patient privacy or information security policies is a serious matter. Purposeful disclosures or violations may result in West Florida Hospital requesting that you be removed from on-site participation.

What is a breach?

- Unauthorized acquisition, access, use, or disclosure of unsecured, unencrypted protected health information which compromises the security or privacy of such information and **poses a significant risk of financial, reputational, or other harm to the individual**. To determine if a breach has occurred, a risk assessment must be performed to determine if the security or privacy of the PHI has been compromised.
- In the case of a confirmed breach, the hospital must notify the patient or their personal representative without unreasonable delay and in no case later than 60 days of discovering the breach.
- In the case where a single breach event affected more than 500 patients, the hospital must provide notice to prominent media outlets and the Secretary of the Department of Health and Human Services (HHS).

Common Breaches Reported in the Hospital

- Misdirected faxes containing sensitive information
- Incorrect PHI provided to requestor than includes sensitive information
- PHI given without authorization
- Inappropriate disclosure to employer
- Identity theft
- Stealing and disclosing PHI
- Sensitive information lost or found
- Inappropriate access of record
- Confidential Communication Violations
- Adoption disclosure

Reasonable Safeguards

- Lower your voice when discussing patient information.
- Do not discuss patient information in public areas, including cafeteria, elevator, waiting room.
- Do not view your own medical record (contact HIM and complete an authorization).
- Dispose of protected health information in designated bins for shredding.
- Verify fax numbers before transmitting protected health information.
- Share information with others only when required for PAYMENT, TREATMENT, or HEALTHCARE OPERATIONS.

Printing, Faxing, Disposing of PHI

- When printing PHI, verify the printer name and location prior to printing.
- When faxing PHI, verify the fax number and always use a cover sheet.
- Dispose of all PHI in designated shredding containers. Do not throw PHI in the trash.
- Do not remove PHI from the hospital.

To Test Your Knowledge

- Do you know who the WFH FPO is?
- Does the patient have the right to access or obtain a copy their medical record?
- Can a patient amend their record?
- Do you know who to refer patient privacy questions or complaints to?
- What is a breach?
- What is an Accounting of Disclosures?
- Where do you dispose of patient information?
- Can you take protected health information home with you?
- How can you protect patient privacy?