Health Insurance Portability & Accountability Act (HIPAA) Privacy Training

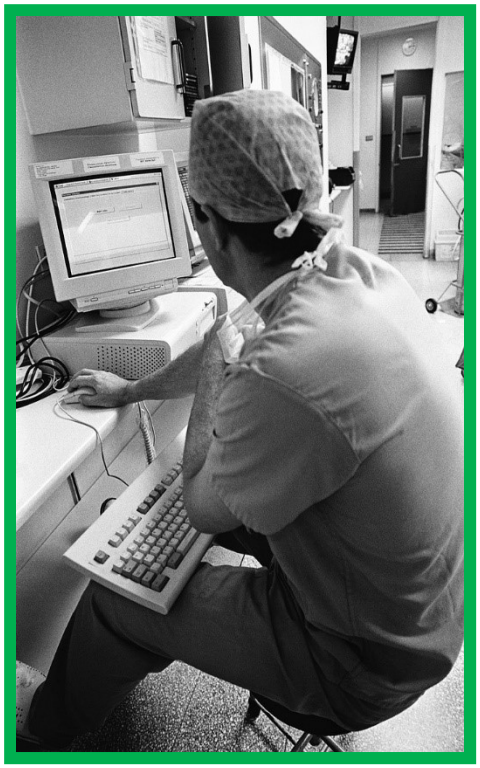
Purpose of Training

- Explain the legal basis for the information security and privacy policies and practices.
- Reinforce the importance of privacy and the expectation that patient information be reasonably maintained and safeguarded at all times.

Purpose of Training

- Discuss the impact of failure to safeguard patient information can pose risk of financial, reputational, medical or other harm to the patient, affect trust in the quality of care given, and result in various regulatory violations.
- Emphasize training through application to actual work-relevant scenarios which have occurred at facilities across the country.

Culture of Privacy



- Benefits of health information technology can only be fully realized if patients and providers are confident that medical information is private and secure at all times.
- Healthcare workforce are expected to abide by all applicable privacy and information security laws.
- Concept of protecting patient information is deeply ingrained in how day-to-day duties and responsibilities are carried out.
- Adhere to department's reasonable physical, technical and procedural controls to safeguard patient information.
- Exhibit practices that are rooted in the minimum necessary principle; access, use and disclose only what is needed to perform your responsibilities.

Legal Basis for Policies

- 2003 – the Health Insurance Portability and Accountability Act's Privacy Rule (**HIPAA** Privacy) established federal protections and standards for using and disclosing patient information. It also created new individual rights to privacy.
- 2005 – HIPAA's Security Rule established federal protections and standards for the administrative, technical and physical safeguarding of patient information.
- 2009 – The HIPAA Privacy and Security Rules were amended by the HITECH Act to expand privacy rights, strengthen enforcement, and enhance existing safeguards.
- On occasion, Hawaii state privacy laws will provide patients greater protection, as is the case for certain sensitive health information and for certain treatment records belonging to minors.
- Hawaii laws may require us to disclose specific information to report disease or injury, child abuse, birth, or death, or for public health surveillance, investigation, or intervention.

Consequences

- Failure to safeguard patient information can result in a HIPAA privacy/security violation. HIPAA violations can lead to large fines and even jail time for the most serious offenses. Based on intent and institution responsiveness to a violation, penalties can be as much as $1.5 million.
- The federal government is required to conduct periodic audits, investigate all complaints, and impose penalties when there are findings.
- As students, you can be held personally accountable for willful, civil HIPAA violations. This means the Hawaii Attorney General can bring civil suits against individual employees & students.
- Non-compliance with privacy policies can result in progressive discipline, up to and including suspension or termination. Students may lose access privileges and face cancellation of their participation in educational opportunities. Violations may also be reported to law enforcement officials.

Breach Notification

- Facilities are required to notify patients affected by a breach that poses a significant risk of financial, reputational, or other harm to the patient.
- Hospitals must report all breaches of unsecured PHI to the federal government who, in turn, must publicly post the breach reports on its website.
- All workforce, medical staff and business associates are required to immediately report any suspected or actual breach. This ensures proper corrective actions and timely notification steps can be taken.
- Failure to promptly report a breach may result in disciplinary action or loss of priviledges.

PHI & Specially Protected Health Information

- PHI means **Protected Health Information**. It is the information we must appropriately use, disclose and safeguard.
- PHI is often interchanged with the term "Patient Information" or “Personal Health Information” and can be in any form or format (spoken, written or electronic).
- PHI is any health information that is individually identifiable by name, address, e-Mail address, social security number, location in our facility, employer, name of relatives, birth date, date of birth, dates associated with care, fingerprints, full face photo, and any other unique identifying number, characteristic or code like the Medical Record Number.
- PHI is therefore the information contained in the patient’s medical record **as well as any information found in the patient’s billing records and appointment schedule**.
- e-PHI refers specifically to PHI in an electronic form. Examples include PHI in an e-mail, EPIC or stored on CDs, flash drives, or electronic devices like a laptop or smart phone.
- Certain PHI is considered “Specially Protected Health Information" and includes PHI related to alcohol or drug abuse treatment information, and psychotherapy notes.

De-identified Information

De-identified Information is any information that does not contain **<u>any</u>** of the following Individually Identifiable Health Information :

- Name
- Address
- Fax number
- E-mail address
- Employer
- Member /Account Numbers
- Names of relatives
- Telephone number
- Medical record number
- Vehicle identifiers
- Device identifiers
- Internet Protocol (IP) address
- Certificate/License Numbers
- Full Face Photographic image
- Social Security Number
- Biometric identifiers (Fingerprints/Voiceprints)
- Web Universal Resource Locators (URLs)
- Dates except year (e.g., birth date, date of service, date of death)
- Any other characteristics that might be unique in certain populations

Information that has been de-identified is NOT subject to the HIPAA Privacy and Security Rules.

Minimum Necessary

- Limit access to use or disclosures and requests for information to the minimum necessary to perform the task for the intended purpose.
- Applied to all spoken, written, or electronic uses, disclosures, and requests for PHI, EXCEPT when patient treatment is involved.
- Need-to-Know Rule

Scenario: Minimum Necessary

Scenario: On your way back from a break, you see someone in a waiting room who looks like your mother's friend. After work, you tell your mother who you saw and where you saw this person. Is this okay?

NO. This is a violation of the patient's privacy rule. A patient's name and location in the facility is considered PHI. Never share information about patients you saw or provided care for anyone who does not need the information.

You & Family Members as Patients

- When you are hospitalized or receiving care at any facility, you have the same rights to privacy as any patient.
- Your employer/fellow students may only access your PHI to perform their treatment, payment processing, and healthcare operations responsibilities.
- You may **not** access your personal medical record for purposes that are not work-related.
- You may **not** access your family member records unless you have direct medical, billing or other operational responsibility and the access is required for you to perform your job.

Scenarios: Access & Min Necessary

Scenario 3: A patient you cared for in the ICU was transferred to another unit. Can you call the unit and talk to the nurse who is now caring for her?

NO. This activity is questionable. As much as this may reflect your compassion and concern for patients whom you have taken care of in the past, it falls under personal curiosity and may be subject to progressive discipline as there is not a clear treatment or business reason for the access.

Scenario: Facility Directory

Scenario 1: Someone approaches you in the hallway and asks for a specific patient's room number. You recall the patient and her location. What do you do?

Answer: Do not give out any information unless you know or can verify the patient has not requested any hospital directory restrictions. Instead, direct or escort the visitor to the nurse's station, information desk, or nearest telephone to call the hospital operator.

Scenario: Facility Directory

- Scenario 2: A persistent visitor is asking about a **No Info** patient. How do you respond?

- Answer: "I'm sorry, we are unable to give you any information. "
- *Follow-up question:* "But the patient called me and told me that he is here at this hospital. How can you say you have no information?"
- *Response:* "I have no information to give you about that person. Perhaps you can contact the patient's family for information." *If visitor is insistent, refer the* visitor to a supervisor.

Computers and Portable Devices

- Facility-provided workstations or portable computing devices are for business use only. Other uses are prohibited.
- Never place PHI on portable computer devices or portable media (disk, flash drives, CDs, DVD, phones,etc.) for storage or transfer unless the data is encrypted to prevent unauthorized access.
- Only facility-owned devices are permitted to be connected to the facility network.
- Patient photographs are not permitted unless explicitly authorized by the patient. Taking photographs without permission or without completing the proper release forms is prohibited.

Use of Social Media

- Must not discuss patients on any kind of social media. Even when patient is not identified by name, there is a chance that person could be identified from the information.
- Do not disclose or discuss patients or work-related issues online.
- Do not post photos of patients or PHI

Disposal of PHI

- Paper containing PHI must be shredded. Never place PHI in public rubbish cans, even in the exam rooms.
- Containers temporarily storing "To Be Shredded" documents must be reasonably secured. Never leave documents to be shredded in publicly accessible areas or outside of/next to shred bins.
- Any labels, tags or materials containing PHI that are affixed to medical supplies must be destroyed before the product is disposed.
- Files on computer disks or flash drives or hard drives must be COMPLETELY overwritten. Selecting "delete" or pressing the delete key is not sufficient and files deleted in this manner can still be recovered.