

Information Security and Privacy Policies and Practices

Nursing Students with Direct Access to Protected Health Information

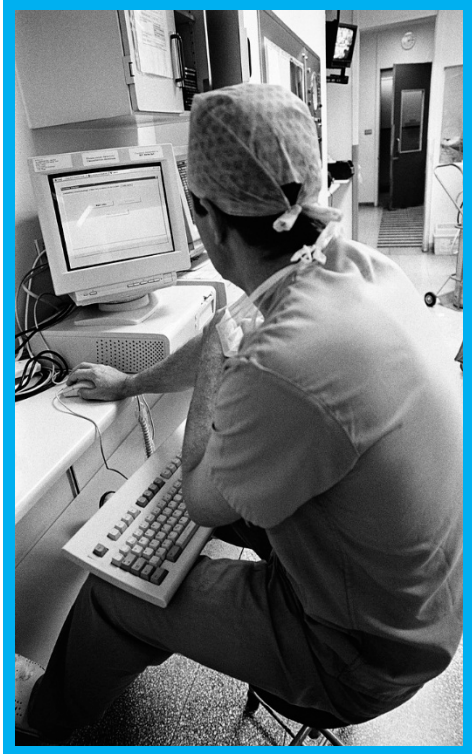
This training program was developed through a collaborative effort of Hawaii Clinical Placement Collaborative (HCPC) members and covers components of the HIPAA regulations for students. Specific procedures may vary from facility to facility.

Purpose of Training



- To explain information security and privacy policies and practices.
- To reinforce the importance of patient privacy
- To communicate expectation that patient information must be reasonably maintained and safeguarded at all times.

Culture of Privacy



- **PATIENT PRIVACY IS TAKEN SERIOUSLY.** The benefits of health information technology can only be fully realized if patients and providers are confident that patient information is private and secure at all times.
- **PRIVACY CONTROLS AND PRACTICES.** Physical, technical and procedural controls that ensure patient information is reasonably secured and private must always be followed. Your department may have specific procedures and operational expectations on the use and disclosure of patient information. You are expected to review and follow these.
- **STRICTLY BUSINESS.** Electronic medical records, patient information, applications and network systems must be used only to do your job or as permitted by policies. Use for personal reasons are strictly prohibited.

Legal Basis for Privacy & Security



- Providers, hospitals and other covered entities must comply with federal and state privacy laws. These laws:
 - Establish individual rights to privacy
 - Set limits on who can access, use and share a person's health information
 - Require reasonable administrative, technical and physical safeguards are in place to protect patient privacy.
 - Mandate patient notification and reporting when breaches occur.

What's Protected?

- **Protected Health Information (PHI)** –Also referred to as "Patient Information" or "Personal Health Information"
- PHI includes spoken, written and electronic information.
- PHI is found in the patient's medical record, billing records, labels on medical equipment/supplies/ medications used by the patient - anywhere the patient's name, MRN or other identifiers are listed in conjunction with his/her health information.



Electronic PHI (e-PHI) is PHI created, processed or stored in any electronic format such as Epic, e-mail, CDs, flash drives, smartphones, and other electronic devices

PHI & Restricted Confidential Information

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.



Restricted Confidential Information is PHI held in the records of a substance abuse treatment program.

Medical ID Theft

- Medical ID Theft is becoming a major issue in the United States.
- Medical ID theft occurs when medical services are obtained by using someone else's insurance, SSN or other information.
- Consequences: Victims risk having wrong information in their record and receiving wrong medical treatment; having health insurance benefits exhausted; and being uninsurable.

Medical ID Theft

- Red Flags Include:
 - ID documents that appear to have been altered;
 - ID photos or descriptions don't match the individual's appearance;
 - Medical histories or other information don't match information in our records
- Notify your supervisor, Risk Management or the Privacy Office anytime patients suggest they are a victim of ID theft or if you suspect a patient is not who they claim to be.

Notice of Privacy Practices



Refer patients with privacy-related complaints or requests to Patient Relations or the Privacy Office.

- Healthcare facilities are required to give patients a “Notice of Privacy Practices” that tells them how we may use and share their PHI, our legal obligations, their rights to PHI, and how they may exercise these rights, including how to file a complaint.
- We must give the notice to the patient no later than their first service encounter and make a good faith effort to obtain written acknowledgment of patient’s receipt of the notice.
- Notice must be made available to any person who asks for it, prominently posted, and made available on the facility’s website.

Patient Privacy Rights

- Patients have the legal right to:
 - Request restrictions on the use and disclosure of their PHI.
 - Request restrictions on the disclosure of their PHI to their health care plan.
 - Request alternative confidential communications from us.
 - Inspect and obtain a copy of their PHI.
 - Request an amendment to their information.
 - Obtain a listing of certain disclosures of their health information.
 - File a complaint with the facility or the government. Refer patient to Patient Relations or the Privacy Office.



Refer patients with privacy-related complaints or requests to Patient Relations or the Privacy Office.

Permitted Uses/Disclosures of PHI

- Except for restricted records, a patient's PHI may be used/disclosed without the patient's authorization for:
 - Treatment,
 - Payment, and
 - Health care operations.
 - Examples of health care operations include training health care professionals, medical review, quality assessment and improvement activities, care management and coordination, and credentialing and peer review.

Restricted Confidential Information

- Federal law provides a higher level of confidentiality for the records of a recognized Substance Abuse Treatment Program
 - Program
 - An identified unit within a general hospital or clinic that holds itself out as providing and does provide substance abuse diagnosis and treatment
 - Does not include a general hospital or clinic that might mention patient's substance abuse in the medical record
 - Require patient consent to release information, even for treatment, payment and health care operations
 - Re-disclosure of records received from a covered program is prohibited

Disclosure of PHI with verbal agreement

- ▶ Certain releases of PHI may occur with the patient's "agreement" as opposed to a written authorization or consent. These releases include:
 - Facility Directory
 - Disclosures to persons involved in the patient's care

Patient or Facility Directory

- As a service to patients, their names and room numbers are routinely included in the hospital or facility directory.
- Information in the directory is considered to be PHI and must be reasonably safeguarded.
- When admitted, patients select one of the following options:
 - Full Info – Patients wishes to be listed in the directory. You may acknowledge the patient is in the facility only when visitors, callers, or the media ask for the patient by name.
 - No Info – Patient does NOT wish to have their information in the patient directory. You may NOT acknowledge the patient is in the facility, even if the patient is asked for by name.

Facility Directory “No Info”

- Under certain situations and at the facility’s discretion, the facility may designate patients that are victims of crime/trauma, psychiatric patients, VIPs and other high profile individuals as “No Info” patients unless the patient has indicated otherwise
- Inmates or other persons in custody of law enforcement officials are automatically designated as **“No Info”**

When Patients Are No Info

- If you are involved with inpatient care, you should know how to identify **No Info** patients. Please check with your department about this.
- Password Process. Your facility or hospital unit may have a password process in place to help facilitate the disclosure of PHI about **No Info** patients to certain authorized individuals. Please check with your department about this.

Scenario: Facility Directory (No Info)

Scenario 1:

- Someone approaches you in the hallway and asks for a specific patient's room number.
- Although you know the patient and her room number, you don't know whether the patient has requested any facility directory restrictions.
- What do you do?

Scenario: Facility Directory (No Info)

Scenario 1 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 (No Info)

Scenario 2:

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

Scenario: Facility Directory (No Info)

Scenario 2 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.*

Disclosure to Persons involved in Patient's Care

- Always get patients' permission before sharing information with others who are or may be involved in their care.
- If patients are not available or unable to indicate their preference, you may:
 - Rely on your past knowledge about the patient's preference and the person's level of involvement in the patient's care
 - Exercise professional judgment based on what is in the best interest of the patient



Disclosure to Persons involved in Patient's Care

- **Remember:** You must limit the information to what the others *need to know* based on their involvement with the care or payment for care of the patient.
- AHA guidelines for release:
 - What is this person's relationship to the patient?
 - Is it in the patient's best interest to release the information?
 - What would the patient want?



Caring for Minors as Patients

- What can I tell the parents of a minor who is my patient?
 - Generally, you can tell parents everything except when:
 - They are suspected of abusing or harming the minor
 - Minor is emancipated – In Hawaii a minor is emancipated once they are or have been married. Emancipated minors have the same rights as adults.
 - The parent is requesting access to information about care the minor legally consented to without parental involvement. In Hawaii minors (ages 14- 17) can consent on their own for:
 - Pregnancy care; family planning; treatment of venereal disease
 - Drug/alcohol abuse counseling
 - Care when requesting termination of pregnancy <12 weeks. Check facility policy
 - Care when minor is active duty in military

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 and fellow students may only access your PHI to perform their treatment, payment processing, and healthcare operations responsibilities.

Accessing Personal and Family Member Records

- 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.
- **Never** use your facility granted medical record privileges to conduct personal business.

Access to Your Child's Records

- If you are a parent, you have the right to obtain a copy of your minor child's medical record through the facility's medical records unit.
- **WARNING:** You MAY NOT use your facility granted medical record privileges to access your minor child's medical records.

Other Permitted/Required Disclosures

- The privacy rule permits the disclosure of PHI without authorization or consent for other purposes that are specifically permitted or required by law.
- These releases must conform with the requirements of the law.
- Many of these releases involve disclosure to law enforcement or other public officials
- Be sure you know and follow the facility's policies and procedures in regards to these disclosures.

Other Permitted/Required Disclosures

(No Authorization Required)

- ▶ Law Enforcement
- ▶ Public Health
- ▶ Abuse/Neglect Reports
- ▶ Health Oversight
- ▶ Research
- ▶ Subpoenas/court orders
- ▶ Organ Donation
- ▶ Required by law
- ▶ Medical examiners
- ▶ Mortuaries
- ▶ Specialized Gov't functions (military)
- ▶ Workers' compensation
- ▶ Serious threat to health/safety

Identity & Authority Verification



- You may release PHI to individuals or entities whose identity and authority is previously known to you.
- Otherwise, you must verify the identity of the Requestor and their authority to have the PHI prior to releasing the PHI.
- Check with your facility about verification processes and when such requests are to be referred to Medical Records.
- Your facility may specifically require documentation of identity or verification of authority prior to releasing information to law enforcement, researchers & public officials.

Release of Information (ROI)

- ▶ A valid authorization from the patient is required for use/disclosure of PHI for purposes other than:
 - Treatment, payment or health care operations
 - Facility Directory
 - Disclosures for persons involved in the patient's care
 - Other Releases permitted or required by law
- **Exception:** Disclosing substance abuse treatment records requires a valid authorization from the patient.
- All releases of information to law enforcement and public health officials must be documented.



Release of information to unauthorized persons may result in a privacy violation.

Release of Information To A Patient's Employer

- Patient Information should NEVER be released to the patient's EMPLOYER without prior authorization or explicit permission from the patient. A "best practice" is to release the information to the patient to give to his/her employer.
- Requests related to worker's compensation should be referred to the facility's Medical Records unit.

Minimum Necessary

- You must only access, use or disclose the minimum amount of patient information needed for the intended purpose.



- All uses/disclosures of PHI must comply with the minimum necessary standard except for
 - Disclosures to the patient.
 - Treatment disclosures
- Do not disclose or request the entire medical record, unless it is justified as the amount reasonably needed.

Leaving a Message

- When calling patients to discuss treatment, test results or billing and you get voicemail, limit the information you leave and give call back information.



- **NOTE:** Be sure there are no restrictions to communications or requests for alternative communications. For example, if patient asks you to only call their cell, it would be *inappropriate* to call and leave a message on their home phone. Refer to department specific procedures.

Disclosures Over the Phone

- When answering a caller's request for treatment or billing information, you must:
 - reasonably verify the caller's identity and authority to receive the information.
 - If unable to verify, refer the caller to the appropriate Health Information Management/Billing department as appropriate
- Before releasing information, be sure the request falls within your scope of responsibilities. For example, do not release billing information if your department does not disclose this information or if the information relates to an encounter at another department. Refer the caller to the appropriate department or your facility's Health Information Management unit.
- Refer to department specific procedures.

Gossiping Is A Violation

- It is NEVER okay to share patient information outside of work or beyond your scope of responsibility.
- Regardless of how harmless the information may seem to you; how much you trust the person you are talking to; or whether you think the patient may not care, you must ALWAYS refrain from “socially” talking about patients.
- You are NOT permitted to share PHI with people at work who don't need the information to perform their jobs or when it is beyond your scope of responsibility. This includes mentioning the patient's name, appointments, reason for appointments or patient directory information.
- Violations of this nature are subject to disciplinary action.

Use of Social Media

- You 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.
- Be careful about giving medical advice to “friends” online as the online message creates an electronic record of the exchange which could create liability.
- Do not disclose or discuss patients or work-related issues online.

Incidental Disclosures

- Incidental disclosures may occur when routine clinical activities result in PHI being inadvertently seen or overheard, for example, discussions during teaching rounds, shift changes & patient registration.
- The following are examples of incidental disclosures that can be perceived as privacy breaches and cause patients to be uncomfortable or dissatisfied:
 - Staff asking about private information in public areas, waiting rooms, service areas, hallways, or elevators.
 - Being asked to provide personal information out loud
 - Overhearing conversations about PHI by staff doing their job

Incidental Disclosures

- Reasonable measures must be taken to reduce or prevent circumstances where spoken, written or electronic PHI can be inadvertently seen by or overheard by others who don't need the information. Such measure may include:
 - Use of cubicles, curtains, dividers or other shields between beds
 - Log off computers when leaving them
 - Privacy screens on computers
 - Speaking quietly when discussing patient's condition with family/others in waiting room
 - Limit amount of PHI disclosed
- Although incidental disclosures are not considered to be privacy violations, our patients can be concerned and have in fact complained about such practices.

Scenario: Minimum Necessary

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



Scenario: Minimum Necessary

- **NO.** This is not okay.
- Although sharing patient information with your spouse may seem harmless, it is considered to be a violation of the patient's privacy. A patient's name and location in the facility is considered PHI.
- Never share information about patients you saw or provided care for with anyone, including friends and family, who does not need the information.

Scenario: Access and Minimum Necessary

- A patient you cared for in the ICU was transferred to another unit.
- Can you look in the patient's record to see how she is doing?
- Can you call the unit and talk to the nurse who is now caring for her?

Scenario: Access and Minimum Necessary

- **NO.** These activities are 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.
- You may access the patient's record if there is job-related reason. For example, if you have to complete a note in her record after she has left your unit, you may access her record to complete your note.

Role-Based Access

- Your access to patient information and the facility's information systems is a privilege based on your job role and responsibilities.
- You should only view and access patient lists, patient headers, and PHI needed to do your job. Looking at patients in other units or clinics may be a breach of their privacy.
- Each user is assigned a unique user ID. Your access is monitored for compliance with HIPAA security and privacy policies.
- You are responsible and held accountable for all activity that occurs under your User ID. Inappropriate access, use or disclosure of protected information may result in discipline, up to and including termination.



- Never share your User IDs or passwords.
- Never intentionally attempt to access systems or records you do not need to do your job.
- Never use anyone else's user ID, authentication code or password to access any information system.

Password Requirements

- Choosing a strong password – one that is not easily guessed – is an essential step in securing the information in our organization.
- Your password must be kept confidential and never shared or written down on post-its or hidden under the keyboard.



Break the Glass



"Attention: These records are monitored. As required by law, sanctions are imposed for accessing these records inappropriately or under false pretense. Sanctions may include loss of privileges and disciplinary action up to and including termination."

- Break the Glass is a special flag placed on certain records in the electronic medical record. If you have a legitimate reason to access that record, enter your reason and password in order to enter.
- Never misuse your privileges to access PHI about relatives, friends, neighbors, "interesting cases" or patients located in other hospital units or being seen in another clinic UNLESS you need it to perform your job.

Safeguarding PHI

- Failing to reasonably safeguard PHI can be a HIPAA violation.
- You must ensure PHI is not easily accessed or viewed by consistently using reasonable safeguards. This means:
 - Computer monitors in public areas are not easily viewable.
 - Always logging off computers when stepping away, even for a minute.
 - Locking, shutting or monitoring doors to nonpublic areas, as appropriate.
 - Storing/filing documents, patient labels, films and other media containing PHI out of public view/access.
 - Fax machines, copiers and printers are located in secure or well-attended areas.
 - PHI should not be emailed unless encrypted.
 - Badges are visibly worn at all times.
 - Report any problems to Nurse Manager/Instructor.



Safeguarding PHI: Encryption

- Students are not permitted to remove PHI from facility except as specifically described with in this training
- All PHI in electronic format must be encrypted
- Emails containing PHI must be encrypted
- Password protection is not adequate
- See slide on De-identified Information
- Use of personal email accounts such as yahoo, Gmail, roadrunner, etc. are generally not secured
- Contact facility for specific requirements

Computers & Portable Devices



- Facility-provided workstations or portable devices are for business use only.
- Never place PHI on portable devices or media (e.g., disk, flash drives, CDs, DVD, phones) for storage or transfer unless the data is encrypted to prevent unauthorized access.
- Students are not permitted to use their personal devices to take any patient photographs.

Safeguarding PHI and the Computer Systems



- Never plug external devices (computers, thumb drives and CDs) brought from home into the computer network
- Do not surf the Internet or access sites unrelated to your work responsibilities
- Do not attempt to download or access files sent from unknown or suspicious sources
- Do not click on hyperlinks on websites or in emails unless you are confident about their origin



Disposal of PHI

- Paper containing PHI must be shredded. Never place PHI in public trash cans, even in the exam rooms.
- Containers holding "To Be Shredded" documents must be reasonably secured. Never leave documents to be shredded in public 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 portable storage devices 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.

Scenarios: Safeguarding PHI

Scenario 1: You are using a computer in a non-public but open area and need to step away for a non-urgent matter. PHI is viewable on the screen. Do you need to log off your computer? What if you need to step away for an emergency situation?

Yes. You are expected to secure or log off when you step away from your computer, even for a minute, and whenever you are reasonably able to do so. If you are attending to a non-urgent matter, it is reasonable for you to log off. In an urgent situation, use professional judgment to make sure PHI is not easily viewable; minimize the screen or ask a staff member to secure the computer.

Scenarios: Safeguarding PHI

Scenario 2: Before checking on patients, you secure your computer and shut your office door. On your way to a patient, you see PHI on an unattended computer. Nearby you see an unattended office with the door propped open. The staff persons may be back any second. Should you go ahead and secure the computer and office?

Yes. Secure the computer and shut (don't lock) the door. Ensuring your department is reasonably safeguarded is an individual responsibility and a team effort given the ongoing occurrences of time-sensitive demands. Let your supervisor know about these lapses when you are able to do so.

Phishing Emails: *Danger!*

phish·ing /fɪʃɪŋ/

noun

is the attempt to acquire **sensitive information** such as usernames, **passwords**, and **credit card** details (and sometimes, indirectly, **money**) by masquerading as a trustworthy entity in an **electronic communication**.

Phishing attacks are becoming more wide-spread, frequent and extremely sophisticated.

It only takes *ONE* on click on the wrong link or opening the wrong attachment to take down an entire network.

You are our weakest link and our last defense!



Result of opening the wrong attachment...



Credit: [Hollywood Presbyterian Medical Center](#)

Network was offline for more than a week.
\$3.6 million demanded as ransom.

CSO Feb 14, 2016 3:434 PM PT

How emails can be dangerous.

"91% of targeted attacks involve spear-phishing emails, reinforcing the belief that spear phishing is a primary means by which APT attackers infiltrate target networks." - TrendLabs APT Research Team

Spear-phishers use email to:

1. Deliver file attachments that can infect your computer with malware.
2. Entice you to click on links that take you to web sites that will infect your computer with malware just by visiting it.
3. Trick you into handing over your user credentials so that they can gain access to your network or other sites.



Just because you don't work in IT or aren't a part of the management team doesn't mean phishers will ignore you. Every user **will** be targeted at some point.

If you think that you have been the victim of a spear-phishing attack notify someone immediately using our procedures.

How do I spot a phishing attack?

To protect yourself from phishing attacks, look out for emails and messages that have these characteristics:

1. You are asked to click on links or open attachments.
2. The message creates a sense of urgency.
3. The message invokes strong emotions like greed or fear.
4. Sensitive data is requested.



Legitimate companies will never ask for passwords, social security and other sensitive data via email.

Always check the URL of the site you are visiting. Many times phishers direct you to a website that appears legitimate, but is used to steal your password or other sensitive data.



Does the subject use sensational claims to plant a false sense of urgency?



Do you recognize the sender? Does the sender's domain match that of its organization? Does the tone of the email seem out of place for this sender?



Does the email open with a generic greeting or is it specifically addressed to you?

From: Oskar Wolf <oskar.acme@bigbadphish.com>
Subject: Urgent - Prevent your account from being deactivated



Can you spot typos or grammatical errors? Does the email seem like it was translated with inferior software?

Dear Sir/Madam,

It has come to our attenshun that your account may have been compromised.



Does the email rush you into clicking a link before you have time to think?

To prevent the deactivation of your account, please [click here](#) within 24 hours to log in and reset your password.

Thank you,
Acme IT Support Desk



Does the email solicit sensitive data, like your password or payment information?



Does the sender claim to be a person of authority to trick you into trusting them?

Safeguarding Computers

**See something suspicious?
What to do...?**

**DON'T CLICK or PEEK
JUST DELETE!**

Avoid Errors: Always Double Check



Errors due to carelessness can and should be curbed.

- Carelessness can result in harm to the patient and/or a privacy violation. Examples include:
 - selecting the wrong provider or patient
 - dialing the wrong fax number,
 - selecting the wrong e-Mail address,
 - double-stuffing envelopes, or
 - giving patient information to the wrong patient.
- You are expected to mindfully adhere to reasonable procedural controls to safeguard patient information, such as double-checking names and addresses and calling before and after sending a confidential fax.

Scenario: Avoidable Errors

Misdialing A Fax Number:

An employee faxes a patient's medical record to the wrong number. The record contains sensitive diagnosis. The error was discovered days later when the requesting physician office calls, claiming the fax was never received. Your attempts to identify and retrieve the errant fax were unsuccessful. The facility is now required to send a breach notification letter to the affected patient who consequently changes service providers.

Discussion: Double checking the fax number and calling the intended recipient before or after sending a medical record could have minimized the severity of this error.

Patient Breach Notification

When a privacy breach occurs, federal law requires providers to notify patients affected by the breach in a timely manner.



Immediately reporting a breach ensures timely corrective actions and notification steps can be taken.

Obligation to Report a Breach



- Students **MUST IMMEDIATELY** report any suspected or actual privacy or security breaches. Notify your supervisor or the facility's Privacy Office. Examples of when events must be reported:
 - Careless errors (patient is given wrong discharge papers or lab order, PHI is faxed to wrong number)
 - Loss or theft (backpacks, notebooks, cellphones with PHI, misplaced patient files or notes)
 - Unauthorized access or disclosure (gossiping or snooping in patient records)
- Failure to promptly report a breach may result in disciplinary action or loss of privileges.

Sanctions/Disciplinary Actions



- Non-compliance and failure to report a breach can result in progressive disciplinary actions, up to and including suspension or termination.
- Students may lose access privileges, face cancellation of their contract, or participation in educational opportunities. Violations may also be reported to licensing agencies and law enforcement officials.

Consequences & Enforcement



- Failure to safeguard patient information or report a breach can be a HIPAA violation and consequently costly.
- The Office for Civil Rights is required to investigate and impose penalties for violations, as well as conduct information security and privacy audits.
- Individuals, including students, can be held personally accountable for HIPAA violations. This means civil suits can be brought against you for the violation.

Use of PHI for Educational Purposes

- Training of health care professionals defined as a health care operation so permitted without patient consent or authorization
- Parameters of use/disclosure include:
 - Appropriate access
 - Minimum necessary for the purpose
 - Protect/safeguard PHI
- Access is a privilege.
 - Access patient information only in relation to your assigned duties/responsibilities
 - Ask questions if you are not sure

Permitted Educational Access or Use

- Treatment
- Observation
- Teaching rounds
- Retrospective record/data reviews
- Research (with IRB approval)
- Case presentations
- Patient logs
- **Access or use of PHI by students for purposes other than these may be a violation of the facility's policies and could result in sanctions against the student.**

Facially De-Identified PHI

- Policy permits use of PHI that is “facially de-identified” for educational purposes
- To facially de-identify information, you must remove the same identifiers as in de-identified information, except you may leave in:
 - Patient medical record number
 - Dates of service
 - Zip codes
- This information is still considered identifiable under HIPAA and Hawai'i law and must be protected against misuse, disclosure or loss

De-identified Information

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

- Name
- Address, including **zip codes***
- 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.

***Permitted in facially de-identified information. Facially de-identified information is subject to HIPAA Privacy and Security Rules and must be protected.**

Do's and Don'ts: Treatment & Observation

■ Can Do:

- Access medical records of the patients you are treating or caring for
- Prepare class work with patient identifiers properly removed
- Observe patient care with approval from dept. manager or supervising faculty

■ Cannot Do:

- Do not access medical records of patients you are not treating or caring for
- Do not use data from your cases that have patient identifiers such as name, address, birth date, left in
- Do not observe patient care without appropriate approval or where the patient objects

Do's & Don'ts: Teaching Rounds

- **Can Do:**

- Share patient information during teaching rounds
- Prepare class work using data from your cases with patient identifiers removed

- **Cannot Do:**

- Do not discuss patients in public areas; be aware of your surroundings
- Do not include family members in rounds, unless patient has agreed or physician determines that inclusion is in the patient's best interest

Do's and Don'ts: Photographing Patients

■ Can Do:

- Take identifiable photographs of patients with written HIPAA compliant authorization from patient or personal representative
- Take de-identified photos of patient conditions/injuries with documented agreement of patient or personal representative

■ Cannot Do:

- **Use of camera phones or PDAs to photograph patients is strictly prohibited**
- Take any photos of patients or their bodies/injuries for educational purposes without documented patient agreement or authorization

Do's & Don'ts: Record Reviews/Research

■ Can Do:

- Access medical records with written approval by supervising faculty member
- Prepare class work using collected data with patient identifiers properly removed
- Use aggregate or de-identified patient information

■ Cannot Do:

- Do not use information collected for research without IRB approval
- Do not publish or publicly present findings without IRB approval or waiver of authorization
- Do not contact the patient or the patient's physician
- Do not abstract patient identifiers

Summary

- Only access/use or disclose PHI as permitted by the privacy rule
- Do not access PHI that is outside your job responsibilities
- Access, use and disclose the minimum necessary information for the purpose
- Obtain patient agreement for disclosures to family members. Limit disclosures to PHI relevant to their involvement
- Check facility policies before disclosing PHI to law enforcement or public health officials
- Immediately report breaches
- Don't discuss patients outside work or on any kind of social media

Summary (continued)

- Question people that you don't recognize, appear suspicious or seem lost
- Never share your passwords
- Encrypt all outbound confidential email and removable storage devices
- Do not open emails from suspicious or unknown senders or unknown senders with attachments from original sources
- Do not store PHI on computer hard drives – data must be encrypted
- Properly destroy electronic or hardcopy PHI
- Don't walk away from a computer without signing off or activating a secured screensaver

Summary (continued)

- Don't leave documents unattended in unsecured areas
- Lock entrances to areas used to house or store PHI
- Never download or install unauthorized software or screensavers on your computer
- Discuss possible security and/or privacy violation scenarios with the nurse manager or instructor.

Conclusion

- ▶ This completes the Information Security and Privacy Policies and Practices Training (HIPPA) training course.
- ▶ Individual facility Information Security and Privacy Policies can be found at each location.
- ▶ You must now complete a Information Security and Privacy Policies and Practices Training (HIPPA) **Post Test** to receive credit for this course.
- ▶ Go to https://www.surveymonkey.com/r/Hawaii_HIPAA_PostTest
- ▶ **PRINT** acknowledgment document before clicking on 'done'. Submit to your instructor.