(2024) Privacy & Security Training: Federal & State Healthcare Privacy Laws

UCI Health

This training is created based on federal and state law, UCI Health policies and procedures, and provides guidance on preventing the types of privacy and security incidents UCI Health experience in the prior year.

- Introduction
- Privacy Laws and PHI
- Use and Disclosure of Patient Information
- Accessing Protected Health Information (PHI)
- Written Authorization and Communication
- Protecting Patient Information
- Associated Risks
- Privacy & Security
- Confidentiality Agreement
- Quiz
- Completion

Introduction

Maintaining Privacy is the Right Thing to Do

We've all probably been there before: ***having some sort of medical information we want kept private***.

Maybe it's something deeply personal, something you're just tired of having to talk about, or something that is so embarrassing that you hesitate to mention it even to a doctor.

You want it kept private, and understandably so: **you have a right to that privacy**.

Our patients have the same fundamental right. They place their trust in us. As members of the UCI workforce bound by the **UC Statement of Ethical values** and other policies, and federal and state laws, we have a moral, ethical, and legal responsibility to safeguard their personal and health information as though it were our own, or that of our loved ones.

1

Introduction

The **University of California** is a **Single Health Care Component (SHCC)** under the **HIPAA Privacy Rule**.

At UCI Health, the UCI Medical Center, clinics, and the UCI College of Health Sciences are part of the SHCC. ***This training and our Privacy & Security program applies to all of us - faculty, staff, students, trainees, volunteers, and other workforce members who are a part of the UCI Health community.***

The training is updated annually to reflect changes in federal and/or state law, changes to our policies and procedures, and to provide guidance on preventing the types of incidents we experience.

All workforce members are responsible for understanding their responsibilities in protecting patient information and the content of this training. In the event you are involved in a privacy or security incident, regulators will request proof of your training.

At Least 50 Northwestern Hospital Employees Fired for Accessing Smollett's Profile, Records: Sources

At least 50 employees may have been fired from Northwestern Memorial Hospital for accessing the medical profile and records of "Empire" actor Jussie Smollett without authorization, sources with knowledge of the situation said.

One of those employees – identified simply as Susan to protect her identity – said that with one click of her mouse, she was fired from her job as a surgical nurse last week.

"Simply put, it was just morbid curiosity," she said. "I went into the charting system and started to search his name."

"I clicked just once," Susan said. "I never clicked into his chart."

Intentionally and inappropriately accessing a patient's record is a violation of HIPAA.

Patients always have privacy rights and deserve equal protection of their health care record regardless of the circumstances.

3

The following questions should guide your thinking as you progress through this course:

- ☐ *What types of information must be protected?*
- ☐ *How can I maintain the privacy of protected information and why is it important?*
- ☐ *What rights do patients have regarding access and use of their medical information?*
- ☐ *What are my responsibilities for reporting privacy and security incidents?*

Privacy Laws and PHI

Privacy Laws

State and federal privacy laws require that we protect an individual's personal and medical information.

At the end of this section, you will be able to:

- Identify the types of information required to be protected under California state privacy laws
- Identify the types of information required to be protected under the federal Health Insurance Portability and Accountability Act (HIPAA)
- Identify if the information you come in contact with at work needs to be protected

1

State Privacy Laws: Personal Information

Click the tabs to read more on each section.

CALIFORNIA PRIVACY LAWS | PERSONAL INFORMATION | MEDICAL INFORMATION

California privacy laws require that we protect individuals' personal and medical information. This includes:

- *Protecting personal and financial information*
- *Protecting medical and health information*

CALIFORNIA PRIVACY LAWS | PERSONAL INFORMATION | MEDICAL INFORMATION

Personal information includes:

- *Name*
- *Social Security Number (SSN)*
- *Driver's license*
- *California identification number*
- *Credit or debit card or bank account number*

- ***Medical information***
- ***Email address and password***
- ***Other identifiers***

CALIFORNIA PRIVACY LAWS	PERSONAL INFORMATION	MEDICAL INFORMATION

- ***Medical Information*** *is individually identifiable information in the possession of or derived from a provider of a healthcare service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment.*
- *The* ***California Confidentiality of Medical Information Act (CMIA)*** *prohibits access, use, or disclosure of "medical information" without prior authorization unless permitted by law.*
- ***This applies to all patient information at UCI Health.***

Federal Privacy Laws: Health Insurance Portability & Accountability Act (HIPAA)

The **Health Insurance Portability and Accountability Act (HIPAA)** helps patients by making it easier for their health information to be shared among the entities who are involved in their health care.

This increase in information sharing, however, comes with requirements to implement privacy and security safeguards.

HIPAA requires UCI Health to:

1. Protect the privacy of a patient's health information.
2. Describe how patient information can be accessed, used, and/or disclosed.
3. Provide for the physical and electronic security of Protected Health Information ("PHI")
4. Specify the rights of patients relating to their health information.

We must protect all forms of Protected Health Information including

Written	e.g. Documents, Mail, Printed Records
Spoken	e.g. Phone Calls, Conversations
Electronic	e.g. EMR, Billing, Data on flash drives, Laptops, iPads, Smart Phones, Email, Devices, and other systems containing PHI

Protected Health Information: PHI

Protected Health Information (PHI) is **individually identifiable health information** created, held or transmitted by a **covered entity** or its **business associate**, in **any form or media**, whether electronic, paper, or oral.

Click the plus sign below to review each section.

Individually Identifiable Health Information

Information, including demographic data, that:

1. Relates to an individual's past, present or future physical or mental health condition; the provision of health care or payment for health care, and
2. Directly identifies the individual or there is a reasonable basis to believe it could be used to identify the individual.

Elements not identifiable on their own could become identifiable if presented together.

Err on the side of caution and consult experts.

Covered Entity

The rules apply to **all** health plans, health care providers, and health care billing companies, as well as any businesses that receive or share health information from these entities.

UCI Health is a covered entity.

Business Associate

A person or entity, other than a UCI workforce member, who performs functions or activities on behalf of, or provides certain services to, UCI

Health that involve access by the business associate to protected health information.

Any Form or Media

We must protect all forms of Protected Health Information including:

- Written *(e.g. Documents, Mail, Printed Records)*
- Spoken *(e.g. Phone Calls, Conversations)*
- Electronic *(e.g. EMR, Billing, Data on flash drives, Laptops, iPads, Smart Phones, Email, Devices, and all other systems containing PHI)*

Identifiers

The following identifiers qualify as PHI and must be safeguarded.

- Name
- Social Security number
- Medical Record Number
- Full face photos and other comparable images
- Health plan beneficiary number
- Telephone number
- Fax number
- Email address *(with or without password)*
- Device identifiers and their serial numbers
- Biometric identifiers *(finger and voice prints)*

- Postal address
- URL address
- IP address
- Account numbers
- License/CA ID numbers
- Credit or debit card or bank account number
- All elements of dates except year
- Vehicle identifiers and serial number
- Individually identifiable information regarding a patient's medical history, mental or physical condition, or treatment
- Individually identifiable health information, including history, lab results, medical bills
- Any other unique identifying number, code, or characteristic

5

De-identification of PHI

Under certain, limited circumstances, "de-identified" PHI may be disclosed.

De-identification is a complex process, typically involving either a formal determination by specially qualified personnel, or the removal of all the PHI identifiers listed previously.

De-identification is challenging and risky, so consult with your Instructor/Coordinator or the Compliance & Privacy Office before disclosing any possible PHI that you've de-identified.

6

Perspective

There are many different pieces of information we need to protect in the course of our work. Because of this, it can be difficult to remember all of it.

Instead of trying to remember all of the details, take a step back and look at the bigger picture.

Ask yourself, ***"Does the information I am using help identify a person in some way? Or could it be combined with other information to identify the person?"***

If it does, you should treat it as protected information.

If you are not sure, you should STOP and ask your Instructor/Coordinator. Your Instructor/Coordinator can provide direction and support.

Summary

You should now be able to:

- [ ] Identify the types of information required to be protected under California state privacy laws
- [ ] Identify the types of information required to be protected under the federal Health Insurance Portability and Accountability Act (HIPAA)
- [ ] Identify the information you encounter at work which needs to be protected

Use and Disclosure of Patient Information

Introduction

It is important to protect every patient's Protected Health Information (PHI).

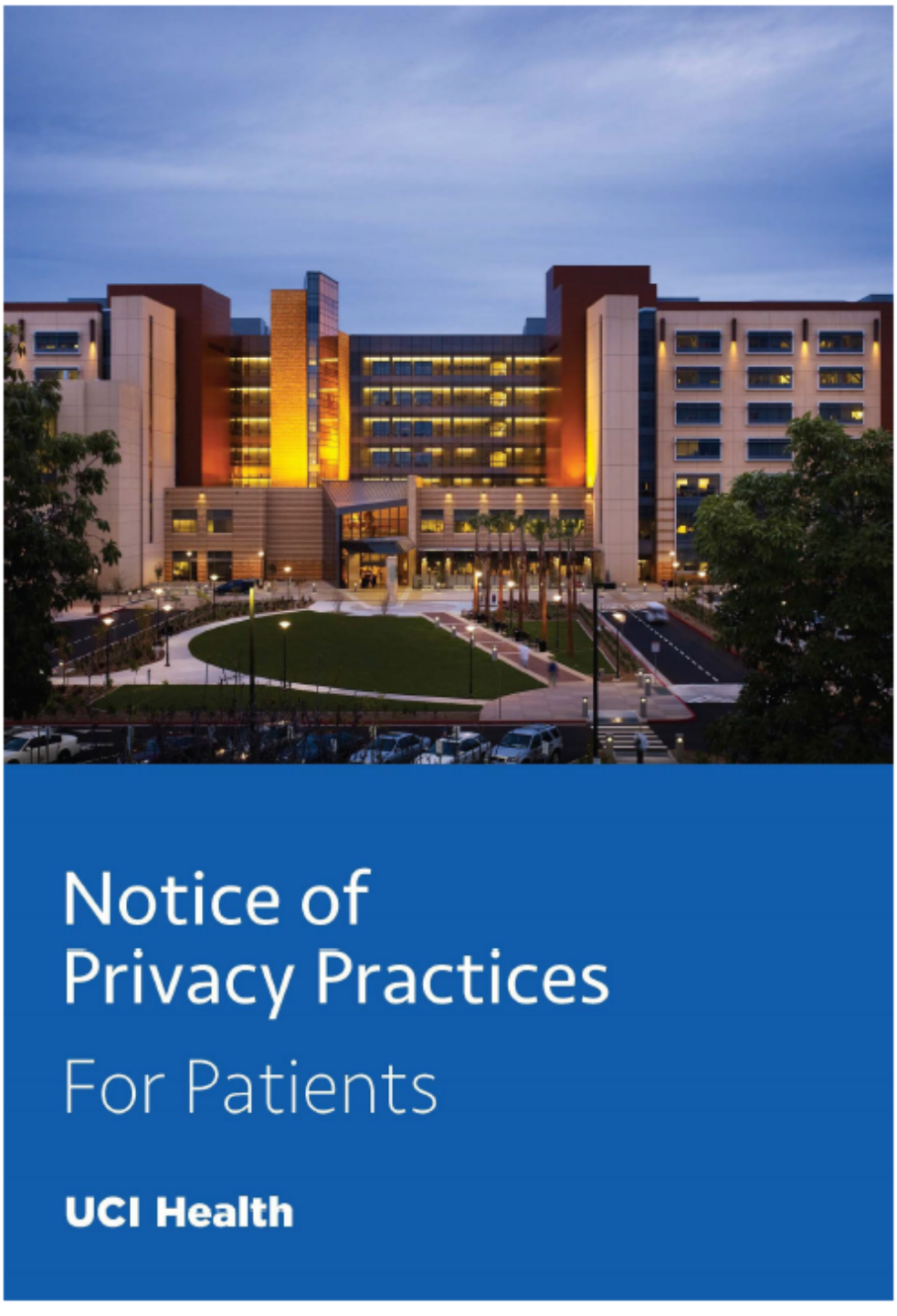
At the end of this section, you will be able to:

- Identify guidelines for when you can/cannot access, use, or disclose a patient's PHI
- Identify specific examples of what you can do to protect patient information
- Identify guidelines for when it is okay to use/disclose PHI during Patient Treatment, Payment Services, and our internal processes (Healthcare Operations)
- Identify examples of patient privacy rights that patients have to their own health information

1

Notice of Privacy Practices

One way that we protect patient information is by giving each patient a Notice of Privacy Practices before collecting, using, storing, or disclosing the patient's PHI.



This notice:

- Describes how UCI Health may use and disclose their PHI
- Advises the patient of their privacy rights

UCI Health must attempt to obtain the patient's signature acknowledging receipt of the Notice, except in emergency situations. If a signature is not obtained, UCI Health must document the reason why.

Please refer to PolicyStat to review the **Notice of Privacy Practices** so that you are familiar with the notice and what we have told patients about their information.

The notice must be posted and copies available at all times in all patient registration areas.

Patient Specific Privacy Rights

Patient rights protected under HIPAA and described in the NPP include:

Right to Inspect

The right to inspect and/or obtain a copy of their medical record.

Right to Amend

The right to amend or request additions to their medical record.

Right to Request Certain Restrictions

The right to request certain restrictions on disclosures of their information.

Right to Request Accounting/Report

The right to request an accounting or report of who obtained their information.

Right to Receive Notice of Privacy Practices

The right to be notified about how their information is used.

Right to File a Complaint

The right to file a complaint with state or federal regulators.

Right to Request Confidential Forms

The right to request confidential forms of communication, for example:

- *Mail to P.O. Box instead of address*
- *No message on answering machines*

The right for their PHI to be kept private and confidential, with permissible use/disclosure exceptions.

We must agree to reasonable requests.

3

Patient Requests for Restriction of PHI

Patients have the right to request a restriction on the use or disclosure of their PHI.

For most restrictions, we are not required to restrict the information if we are unable to comply with the patient's request. ***NOTE: You should consult with Health Information Management and the Privacy Officer before granting such requests.***

However, there is one restriction request we must honor: **If a patient requests to pay in full for a service and asks that we not bill their health insurance, we are required to honor this request.** This also applies if a family member or other individual pays for the service on behalf of the patient.

In this case, we cannot bill the patient's insurance and we are not permitted to provide the information to the insurance company

when submitting information on other services.

Please refer to PolicyStat to the **Patient Requests for Restriction of PHI** policy for details on honoring this restriction request including the form patients must complete to request this restriction.

4

Prevention of Information Blocking

- [ ] In 2021, regulations changed to strengthen patients' rights to access and share their electronic PHI.
- [ ] Under the new rules, UCI Health now shares more patient information in MyChart, including most clinical notes and lab results.
- [ ] There are very limited exceptions to patients' rights to access and share their PHI, such as:
    - *Psychotherapy & Confidential Note Types*

- *Staff messages & Routing comments*
- *Manually blocked information for limited reasons, including preventing physical harm, protecting patient privacy, and legal/administrative infeasibility*
    - *Misuse of these exceptions may place UCI Health at risk of liability under the information blocking regulations. If you have a question on whether it's appropriate to manually block a note, please refer to PolicyStat to consult the **UCI Health Information Blocking** policy, your Instructor/Coordinator, or the Compliance & Privacy Office.*

☐ Notes from all clinical providers documented in EMR are shared.

☐ All workforce members should consider the following best practices:

- *Write more "patient friendly" notes by wording them as if you were presenting the information directly to the patient*
- *Share your screen with the patients when writing the note or read notes out loud to them if possible*
- *Remove personal contact information, such as your pager number, from the signature line*
- *Remove any images of your hand-written signature*

Patient Requests for Amendment or Addendum of PHI

Due to the new information blocking regulations, patients now have immediate access to more medical information than ever before.

With this increased access, patients may raise questions or concerns with their medical records. Under HIPAA and California

privacy laws, patients have a right to request an amendment or addendum to their medical records. UCI Health is not required to honor all patient requests.

All requests for amendments or addendums should be directed to Health Information Management (HIM) at the address below:

UCI Health

Health Information Management

101 The City Drive South, Bldg. 25

Orange, CA 92868

ROI@hs.uci.edu

HIM will not agree to any requests without first speaking to the provider.

Use and Disclosure of PHI

UCI Health can use or disclose PHI without the patient's authorization as follows:

TREATMENT | PAYMENT | OPERATIONS

You may use and disclose medical information about a patient to those involved in the patient's care, such as doctors, nurses, technicians, or providers.

TREATMENT | **PAYMENT** | OPERATIONS

You may use and disclose medical information about the patient in order to bill and collect payment for the services the patient received.

TREATMENT | PAYMENT | **OPERATIONS**

You may use and disclose medical information for healthcare operation purposes, such as: teaching, medical staff peer review, legal purposes, internal auditing, to conduct customer service surveys, and general business management.

For more information on **Treatment**, **Payment** and **Operations**:

Patient Treatment more info –
Treatment means the provision, coordination, or management of healthcare and related services by one or more healthcare providers, including the coordination or management of healthcare by a healthcare provider with a third party; consultation between healthcare providers relating to a patient; or the referral of a patient for healthcare from one healthcare provider to another.

Payment Services more info –
Payment means:
1. The activities undertaken by: A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or A healthcare provider or health plan to obtain or provide reimbursement for the provision of healthcare; and
2. The activities in paragraph (1) of this definition relate to the individual to whom healthcare is provided and include, but are not limited to: Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims; Risk adjusting amounts due based on enrollee health status and demographic characteristics; Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related healthcare data processing; Review of healthcare services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; Utilization review activities, including precertification and preauthorization of services, concurrent and retrospectice review of services; and Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement:
(A) Name and address;
(B) Date of birth;
(C) Social Security number;
(D) Payment history;
(E) Account number; and
(F) Name and address of the healthcare provider and/or health plan.

Healthcare Operations more info –
Healthcare Operations means any of the following activities of the covered entity to the extent that the activities are related to covered functions:
1. Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing healthcare costs, protocol development, case management and care coordination, contacting of healthcare providers and patients with information about treatment alternatives; and related functions that do not include treatment;
2. Reviewing the competence or qualifications of healthcare professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of healthcare learn under supervision to practice or improve their skills as healthcare providers, training of non-healthcare professionals, accreditation, certification, licensing, or credentialing activities;
3. Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for healthcare (including stop-loss insurance and excess of loss insurance). If a health plan receives PHI for the purpose of underwriting, premium rating, or other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and if such health insurance or health benefits are not placed with the health plan, such health plan may not use or disclose such PHI for any other purpose, except as may be required by law;
4. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
5. Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and
6. Business management and general administrative activities of the entity, including, but not limited to: Management activities relating to implementation of and compliance with the requirements of this subchapter; Customer service, including the provision of data analyses for policyholders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policyholder, plan sponsor, or customer. Resolution of internal grievances; The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and Consistent with the applicable requirements of HIPAA, creating identified health information or a limited data set, and fundraising for the benefit of the covered entity.

If you are not sure what constitutes a TPO purpose, you should STOP and ask your Instructor/Coordinator. Your ask your Instructor/Coordinator can provide direction and support.

Accessing Protected Health Information (PHI)

Whenever you use or disclose PHI, there are two overarching rules to which you must adhere.

The first universal privacy rule is the **"need to know" principle**.

It holds that you should only access, use, or disclose PHI that is necessary in order for you to do your job duties.

If you are unsure whether your access, use, or disclosure of PHI is permitted, ask yourself the following:

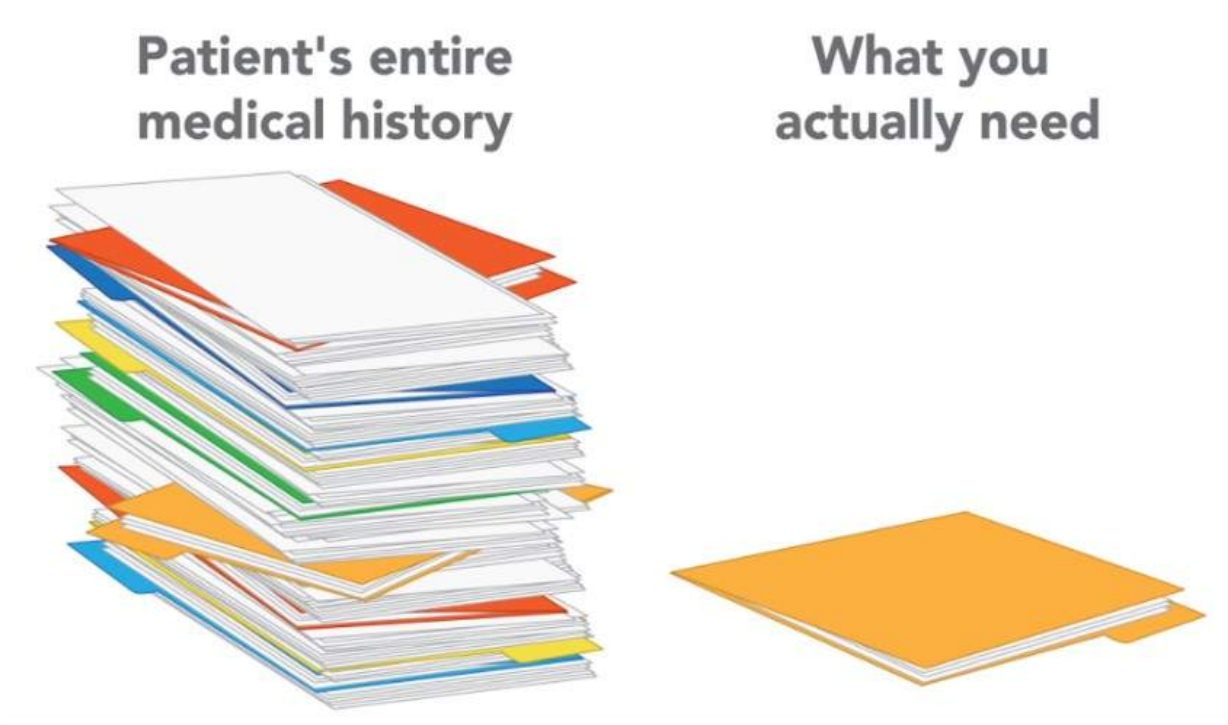
- Do I need to access the Protected Health Information to do my job here at UCI?
- How would l feel if someone viewed or discussed my Protected Health Information without authorization?

Ask your ask your Instructor/Coordinator before accessing or modifying your coworker's record, family member's record, or your own record.

This is only allowed under certain, very limited, circumstances.

The second universal privacy rule is the **minimum necessary standard**.

The **minimum necessary standard** requires that you make reasonable efforts to ensure **only the minimum amount of PHI needed** to **accomplish your intended purpose be accessed, used, or disclosed**. This means that if you are working on a task that can only be accomplished by accessing, using, or disclosing PHI, you must make sure to do so only with the minimum PHI needed to get that job done.



For example: if you're helping an insurer process a payment, and they need the patient's name, date of birth, and an invoice number, you should:

1. Attempt to find the name, date of birth and invoice number in a way that exposes you to as little other PHI as possible, and
2. Make sure you provide the insurer with only the name, date of birth, invoice number **AND NO OTHER PHI**

However, the need to know principle does not apply in certain circumstances, which include:

1. If you are disclosing information to a healthcare provider for treatment purposes.
2. If you are disclosing to the patient who is the subject of the information.
3. If you are using or disclosing information pursuant to an authorization.

1

Inappropriate Access to PHI

Searches of, or access to coworkers', friends' family members', neighbors', and your OWN records, or the records of any other patient without a business purpose is **prohibited**.

DO NOT search or enter records:

Out of curiosity

DO NOT search or enter records:

Due to concern about someone's well-being

DO NOT search or enter records:

To assist someone who is not your patient in obtaining information

EMR must not be used as a search tool to locate addresses, name spelling, birthdates, or phone numbers. Demographic information that appears when searching an individual is still considered protected health information.

UCI Health workforce members must go through proper channels, such as MyChart, to obtain information about their or their loved ones' healthcare.

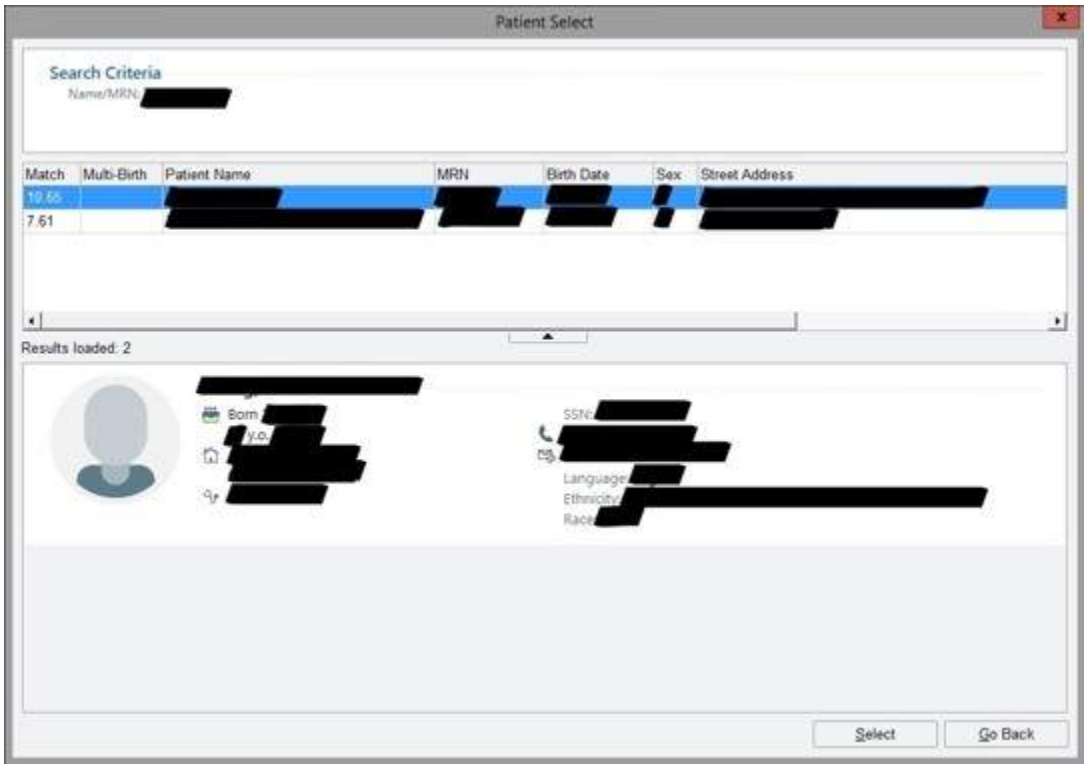
Ask your Instructor/Coordinator before accessing or modifying your coworker's record, family member's record, or your own record.

This is only allowed under certain, very limited, circumstances.

Patient Identity Reports

Searching for any information in EMR without a business purpose is strictly prohibited.

The information contained in the **"Identity Report" is PHI** – even if you view only the Identity Report, you have violated privacy laws and UCI policy if you did not have a business need to view the patient's information.



3

Attestation

By clicking Continue below, you attest that you understand the following:

- You will only use PHI if it's necessary to perform your job duties. If you don't "need to know" the information to do your job, you shouldn't access, view, or use the information.
- You will only access or use the minimum information necessary to perform your job. If you're not sure, ask your Instructor/Coordinator for guidance.

- You will not use EMR without a business or clinical need, including to search or access the medical records of coworkers, family members, or yourself.
- You will follow UCI Health policies and procedures for information confidentiality.
- You understand that you are responsible for any access, use, or disclosure of UCI data that occurs under your UCI Health login credentials, including in EMR.

Policies can be found under the UCI Health Policies and Procedures website, under General Administrative Policies, then Privacy and Security Policies: UCI Health Policies & Procedures.

4

Remember:

- [ ] Only use PHI if it's necessary to perform your job duties. If you don't "need to know" the information to do your job, you shouldn't access, view, or use the information.

- [ ] Only access or use the minimum information necessary to perform your job. If you're not sure, ask your Instructor/Coordinator for guidance.

- [ ] Do not use EMR without a business or clinical need, including to search or access the medical records of coworkers, family members, or yourself.

- [ ] Follow UCI Health policies and procedures for information confidentiality.

Policies can be found in PolicyStat under the UCI Health Policies and Procedures website, under General Administrative Policies, then Privacy and Security Policies:

UCI Health Policies & Procedures

Written Authorization and Communication

When We Need to Get Written Authorization

There are many situations in which we need to get a patient's (or legal representative's) prior written authorization before being able to access, use, or disclose PHI, and there are official UCIHealth forms to use in these situations.

For example, we need prior written authorization before disclosing:

- *Medical information or records to someone other than the patient*
- *Information for use in research (clinical trials)*
- *Patient information for marketing, fundraising, or mass communication (TV, radio, news)*

Always use the applicable UCI Health HIPAA authorization form.

Special protections apply to mental health, HIV, substance abuse, and genetic information.

To release this information, the patient must initial the applicable section on the authorization form, otherwise the sensitive information must be withheld or redacted.

If you receive an authorization form from another organization, consult with the Health Information Management department before acting on the authorization.

1

Communication with a Patient's Family and Friends

Unless the patient has prohibited a disclosure, care providers must use professional judgment when determining when and what information to share with family and friends.

Do Not reveal past medical problems unrelated to the patient's currentondition.

It is appropriate to share information about a patient with family and friends when:

- The patient implicitly or explicitly consents to the sharing. For example, when a patient asks to bring their spouse or family member in with them to an office visit where their treatment options will be discussed.
- In your best judgment, limited information should be shared to assist with the care of the patient. For example:

Patient's Mobility Limitations

You can give information about a patient's mobility limitations to a friend driving the patient home from the hospital.

Patient's Payment Options

You can discuss a patient's payment options with their adult daughter.

Patient's Friend

You can instruct a patient's friend, family member, or other caregiver about proper medicine dosage when they come to pick the patient up from the hospital.

Patient's Condition

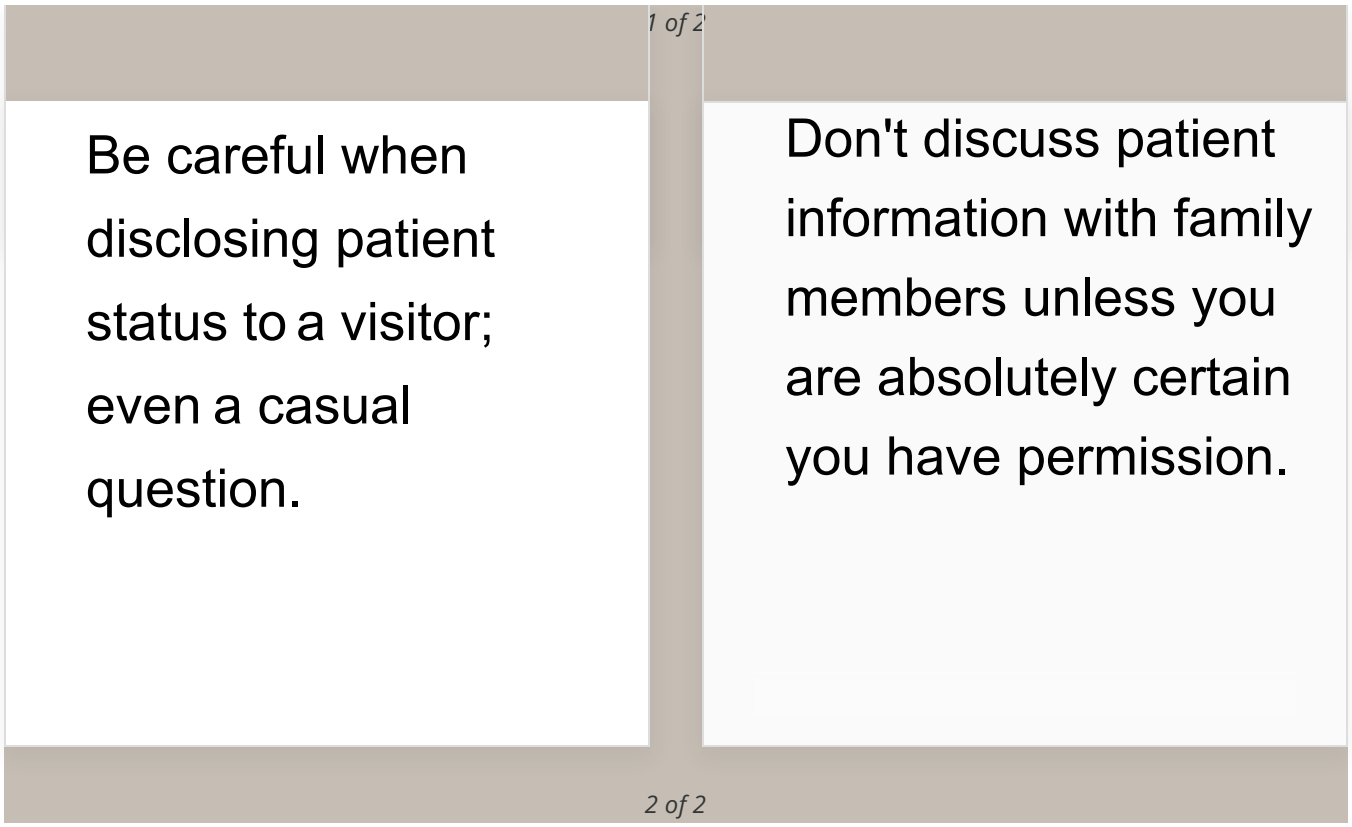
A surgeon who did emergency surgery on a patient may tell the patient's spouse about the patient's condition while the patient is unconscious.

Always be cautious when discussing sensitive information such as HIV/AIDS, STIs, or mental health issues with family members present.

Tips:

Always ask a visitor to leave the room if you are going to discuss health information with the patient.

Let the patient know that you need to talk to them about their confidential health information.



2

Disclosure by Phone

Facility Census/Directory: Unless a patient has opted-out and does not want to be listed in the directory/census, we can only disclose the location and general health status of a patient to a caller if the caller identifies the patient by name.

- If a caller requests additional information on the patient, you can provide information to friends and family **involved** in the care of the patient.

- There is often difficulty in identifying which friends and family are those involved in the patient's care—contact the Privacy Officer or your Instructor/Coordinator with any questions or concerns.

General Guidelines:

Certain departments may have more stringent requirements than what is listed here - contact the Privacy Officer or your Instructor/Coordinator with any questions or concerns.

GENERAL CONDITION	CONSENT	OTHERWISE...
Provide information about general condition (unless opted-out of directory) ***only*** *and refer caller to designated family representative for details.* • *If the patient is alert and awake, ask the patient if they want to talk with the caller.*		

GENERAL CONDITION	CONSENT	OTHERWISE...

If the patient is able and consents to take the call, transfer caller to patient.

GENERAL CONDITION	CONSENT	OTHERWISE...

Otherwise, no information can be provided until a written authorization to disclose the information to the caller is obtained from the patient.

3

Phone Calls

Remember to inform the caller that we must ask a few questions to protect their privacy and verify their identity

When asking a question, **do not provide** the information, instead **verify** the information.

For example :

Instead of "is your address still 123 Main"?	*Ask "what is your address?"*
Instead of "are the last four digits of your SSN 1234?"	*Ask "what are the last four digits of your SSN?"*
If the patient provides information different than in EMR or our files...	*Ask them to provide prior information by saying "do you have a phone number that starts with..."*

Phone Calls: Outpatient Areas

If a friend or family member of a patient is calling to verify an appointment or obtain information about a specific patient, **before sharing any PHI**:

Check any restrictions on disclosures.

Ask to speak with the patient, if available, to confirm their consent.

Use your best judgment if you know that the caller has been involved with patient care/clinic visits and implied consent by patient.

In emergency situations, use your best judgment.

If the patient has signed an authorization, verify with caller the patient information that they would be expected to know (e.g. full date of birth, full name, mother's maiden name, last 4 digits of Social Security Number, etc.).

- Only provide the **minimum necessary** amount of information *(e.g. only say that patient is ready to be picked up from appointment)*.

Summary

You should now have knowledge of:

- [ ] Examples of patient privacy rights that help protect patients' own health information.
- [ ] Specific examples of what you can do to protect patient information.
- [ ] Guidelines for when you can/cannot use or disclose a patient's Protected Health Information (PHI).
- [ ] Guidelines for using or disclosing PHI during Patient Treatment, Payment Services, and Health Care Operations.

Protecting Patient Information

Introduction

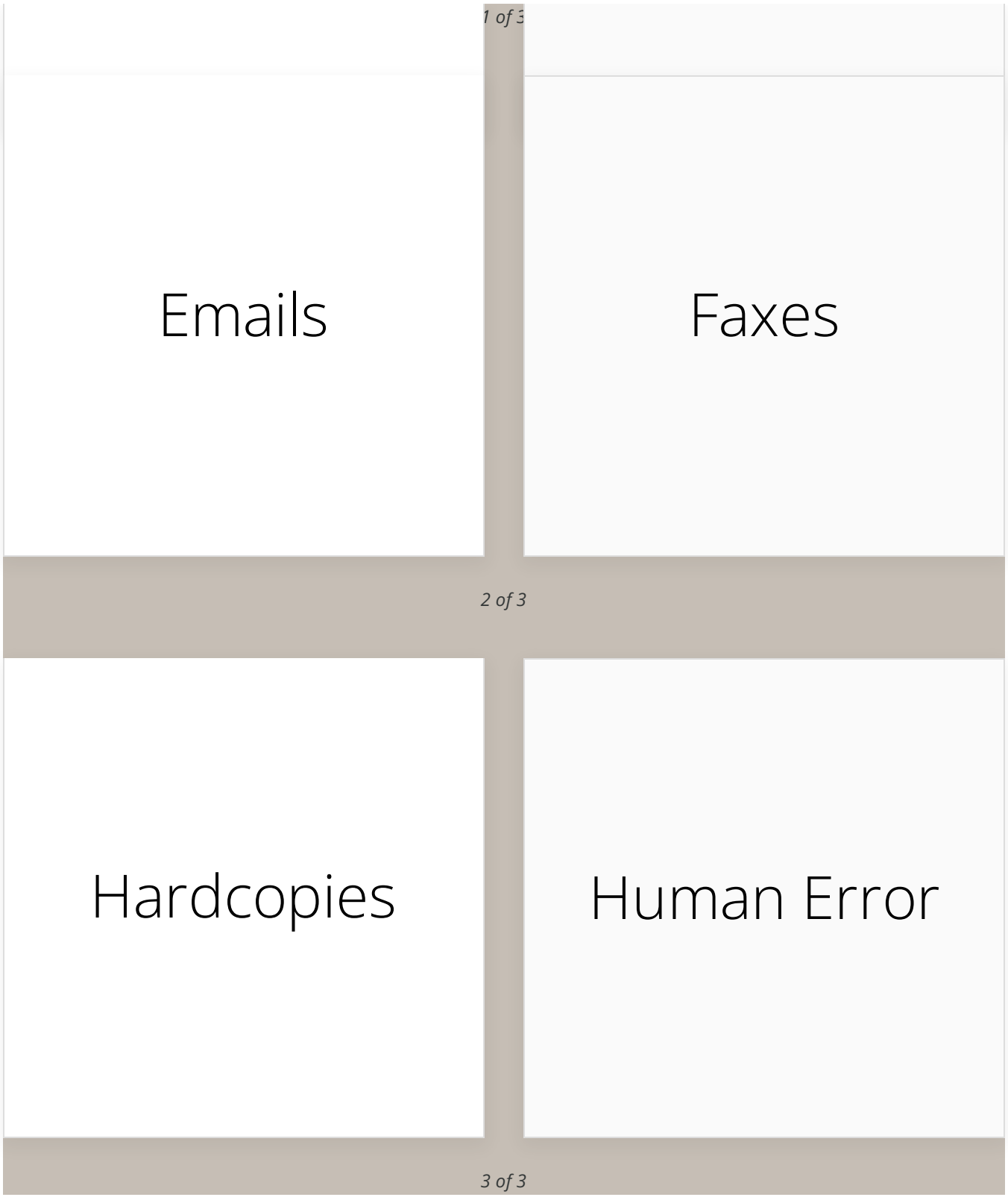
In this section of the training, we will outline the various ways that you can protect and secure patient information. We will also cover common types of errors that can occur, which may result in patient information being breached or placed at risk.

While the Information Security (IS) department is responsible for many aspects of information security, **each employee plays a vital role in protecting our patients' information**.

The risks of a breach of patient information include the following:

Electronic Databases

Portable Devices



At the end of this lesson, you will be able to:

- Identify how to prevent patient information from a breach or unauthorized disclosure

1

Associated Risks: Electronic Databases

The greatest risk of a data breach is the loss of electronic data or access to computer systems with patient information in the EMR, including but not limited to Word, Text, Excel, and EMR.

If you are creating such a database, or using a computer program accessible via the internet, please ensure that **Information Services** knows about the sensitive information it contains, so that they can ensure it is appropriately protected.

If you share information about patients with other departments using a SharePoint or a shared network drive, make sure that the permissions on the folders are kept up to date with only those individuals who need the information. Also ensure only the minimum amount of patient information is included in the shared drive.

2

Associated Risks: Portable Devices and Media Security

Another risk of a breach comes from databases or files of patient information that are on a portable device.

Examples of such devices include, but are not limited to:

- Laptops
- Desktops
- Mobile phones (“smart phones”)
- USB memory sticks
- CDs
- DVDs
- iPads and other tablets
- Portable Hard Drives

Do not *store PHI on personal cloud service accounts, such as iCloud or Dropbox. Personal accounts created heightened risk of data breaches. PHI must only be stored on platforms approved by the University to appropriately protect PHI.*

Do not *use third party messaging or texting applications (such as WhatsApp, Skype, or Viber) with patient information. The version you are using may be sending patient information in clear text for anyone to intercept. Even encrypted versions of messaging applications may not be robust enough and can be intercepted.*

Mobile smart phones are often used for email communications. If an email message received on your smart phone includes protected health or other confidential information, this can pose a risk of unauthorized access if the device is lost or stolen since messages can be easily retrieved from the device.

The following are fundamental smart phone practices that will help protect confidential information on the device from unauthorized access:

- *In the event the phone becomes lost or stolen, immediately contact the Information Security Team at **714.456.3333** and request a remote wipe of the phone. Wait to discontinue the service for the phone until after the remote wipe is accomplished. If you discontinue the service on the phone, remote wipe will no longer be available.*

- *You must enable PIN/password protection on your phone. The more complex the PIN/password, the better. Information Services can help with this, contact them at **714.456.3333**. (NOTE: Devices using the Information Services Exchange system already have this PIN policy applied.)*
- *Enable the device encryption setting, if available. Information Security can help with this, contact them at **714.456.3333**. Do not store restricted information on the phone's memory card (SD card) or any external storage that has NOT been encrypted.*

- *Enroll your device with Airwatch with Information Services so that we can remotely wipe your lost or stolen mobile device*
- *Turn off Bluetooth, Wi-Fi, NFC, and GPS when not specifically in use*
- *Turn on your computer's firewall*
- *Go to the following link to see which devices Information Services supports and recommends: http://it.health.uci.edu/Service-Desk/Mobility-Documentation.asp*
- *Never use Facetime, Skype for personal use, or other similar applications with patient information, since the connection may not be secure and the University does not have a business associate agreement or contract for these services*

- *Consult with Information Services to set up a secure connection using approved equipment*

PROTECT YOUR PORTABLE DEVICES

Never leave laptops, mobile phones, or tablets unattended or locked in a parked car.

Report lost or stolen mobile devices to your Instructor/Coordinator and IT Support immediately.

Privacy and Information Security can help mitigate risk to the information

3

Portable Devices

- Enable passwords and passcodes by using strong passphrases. **Refer to PolicyStat for the UCI Health Password Policy**.
- Activate a PIN number on a mobile device such as a iPad, mobile phone, etc. if the device is connected to the UCI email, or if the device has any type of PHI on it.
- Do not share passwords to these devices.

- Log off portable devices when done.
- Ensure that it is absolutely necessary for business purposes to store patient information on any portable device.
- Only store minimum information necessary to accomplish the business purpose.
- All UCI-owned laptops and desktops must be encrypted. Other portable media should be encrypted where applicable. Encrypt patient information appropriately. ***(Please contact Information Services for assistance.)***
- Physically secure the portable device at all times.
- When disposing of old computers, they must be given to the Information Services department to permanently remove any confidential information on the machine before disposal.
- Minimize the amount of PHI via text or page using Information Services approved methods.
- Do not connect devices for power charging to UCI Health computers. This can introduce viruses into our protected network.

Associated Risks

Emails

A lot of personal information is often communicated via email, and much of it is routinely kept within email accounts. Remember that including restricted information in your email communication presents a security risk. If an unauthorized person gains access to the email accounts, this personal information is potentially vulnerable.

In order to protect patient information in email accounts, minimize your use of email for communicating confidential and personal information.

- Encourage patients to use Secure Health Messaging and the Patient Portal (**https://www.ucihealth.org/mychart**) when communicating with their healthcare providers.
- Please refer to PolicyStat for the **Email and Use of Patient Confidential Information** policy. A consent form must be completed and uploaded into the patient's chart prior to communicating PHI to patients via email.

In the rare cases where it is a business requirement to send PHI to an external e-mail account (such as an interfacility transfer/referral or a State reporting event), then the information being transmitted should be sent appropriately using **[ucsecure]**, which will be explained below.

1

Secure Email & DLP

The HIPAA Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic PHI.

Data Loss Prevention (DLP)

UCI Health has implemented Data Loss Prevention (DLP) technology to prevent the unencrypted transmission of PHI from UCI Health email accounts.

Proactive Service

DLP is a proactive service that scans all email content for PHI.

DLP Technology

This DLP technology blocks any unencrypted email message that it identifies as possibly containing PHI.

Compliance & Privacy Office

The Compliance & Privacy Office is responsible for monitoring DLP and any unsecured PHI that is leaving the organization, as well as any PHI that is sent secure to an outside entity.

How to send Secure:

Include **[ucsecure]** in square brackets in the subject line. The **[ucsecure]** HTML tag must be included within the first 150 characters of the subject line for the secure email gateway to detect it.

Things to remember:

- **Do not include PHI in the subject line**. DLP technology encrypts the e-mail as well as any attachments; it does not encrypt the e-mail subject line. That means any PHI included in the subject line will be viewable by third parties.
- Verify the recipient's email address. ***Be careful with autofill!***
- Verify the information being sent. Sending the wrong information to an intended party is a potential privacy breach.
- Limit the amount of data being sent.
    - For example, if you are attaching an Excel file with 17 columns of data but the recipient only needs the first 3 columns, we recommend deleting the other 14 columns.
    - For more information, visit the **ITS website**.

2

Protecting Patient Information When Using Email

- [ ] **Never** share your password with anyone!
- [ ] Protect the email account by using strong passphrases. Refer to PolicyStat **for the UCI Health Password Policy.**

- [ ] Verify the email address to whom you are sending the email.
- [ ] If the email containing PHI is being sent outside of the UCI Health email exchange, it must be encrypted using **[ucsecure]**.
- [ ] **Do not** send PHI or other information to patients via text message or email unless using department-approved tools and procedures.
- [ ] Communicate only the minimum confidential information or PHI necessary.
- [ ] Emails being sent over the Internet from public locations away from the University should not include restricted information, since these emails are not encrypted.
- [ ] **Resist temptation to open attachments or click on links from an unknown or unverified source. Don’t respond to or forward spam. Delete it.**
- [ ] Make sure that you have installed the latest security updates (or "patches") for your operating system and applications.

- [ ] Never deactivate your computer's antivirus or protective software.
- [ ] Make sure that protective software and accompanying definition files are updated frequently and automatically.
- [ ] Don’t respond to or forward suspicious emails to colleagues. Immediately notify Information Security by forwarding suspicious emails to **security@hs.uci.edu** and subsequently delete the email.
- [ ] Configure your antivirus to scan all downloaded files, removable media, and email attachments automatically.
- [ ] Don't click on unknown links in email, texts, instant messages, social networking sites, ads, or pop-ups.
- [ ] Only download files and plug-ins from trusted sources, and don't use untrusted portable media, such as a stranger's flash drive. Also, don't download plug-ins to view pictures, videos, music and other content online without verifying their legitimacy. These often contain malware.

- [ ] Contact the **Service Desk** at **714.456.3333** if you believe your computer is infected with malware. Disconnect the computer from the network immediately to keep the infection from spreading or sending information to an attacker.

- [ ] Be prudent when browsing the web, opening email attachments, clicking on links, and downloading shared files.

- [ ] If you believe your user ID and password have been compromised, immediately change your password and contact the Service Desk.

- [ ] Do not write down your passwords or post them in your work area *(such as Post-Its on screen/drawer)*.

3

Ransomware

Ransomware is a type of malware (malicious software) that encrypts data with a key known only to the hacker and makes the data inaccessible to authorized users. After the data is encrypted,

the hacker demands that authorized users pay a ransom in order to obtain a key to decrypt the data.

Ransomware frequently infects devices and systems through spam, phishing messages, websites, and email attachments and enters the computer when a user clicks on the malicious link or opens the attachment.

One of the biggest current threats to health information privacy is the serious compromise of the integrity and availability of data caused by malicious cyber-attacks on electronic health information systems, such as through ransomware. **The FBI has reported an increase in ransomware attacks and media have reported a number of ransomware attacks on hospitals.**

The **Security Management Process** standard of the HIPAA Security Rule includes requirements for all covered entities and business associates to conduct an accurate and thorough risk analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all of the ePHI the entities create, receive, maintain, or transmit and to implement security measures sufficient to reduce those identified risks and vulnerabilities to a reasonable and appropriate level.

For additional information please call the Information Services Help Desk at **714.456.3333**.

4

Faxes

The most commonly reported violation of patient privacy occurs when patient information is either faxed to the wrong fax number, or the fax includes information on another patient, by mistake.

The number of faxes going to the wrong fax number has increased with the use of E-Faxing. **You can help reduce these by**:

- Verifying with patient the name of their current primary care provider (PCP).
- You can also ask the patient to initial or sign the face sheet verifying the information is correct and add to the patient's chart.
- Verify you have selected the correct provider.
- Notify HIM if you learn that the provider has a new fax number.

To protect patient information when sending faxes:

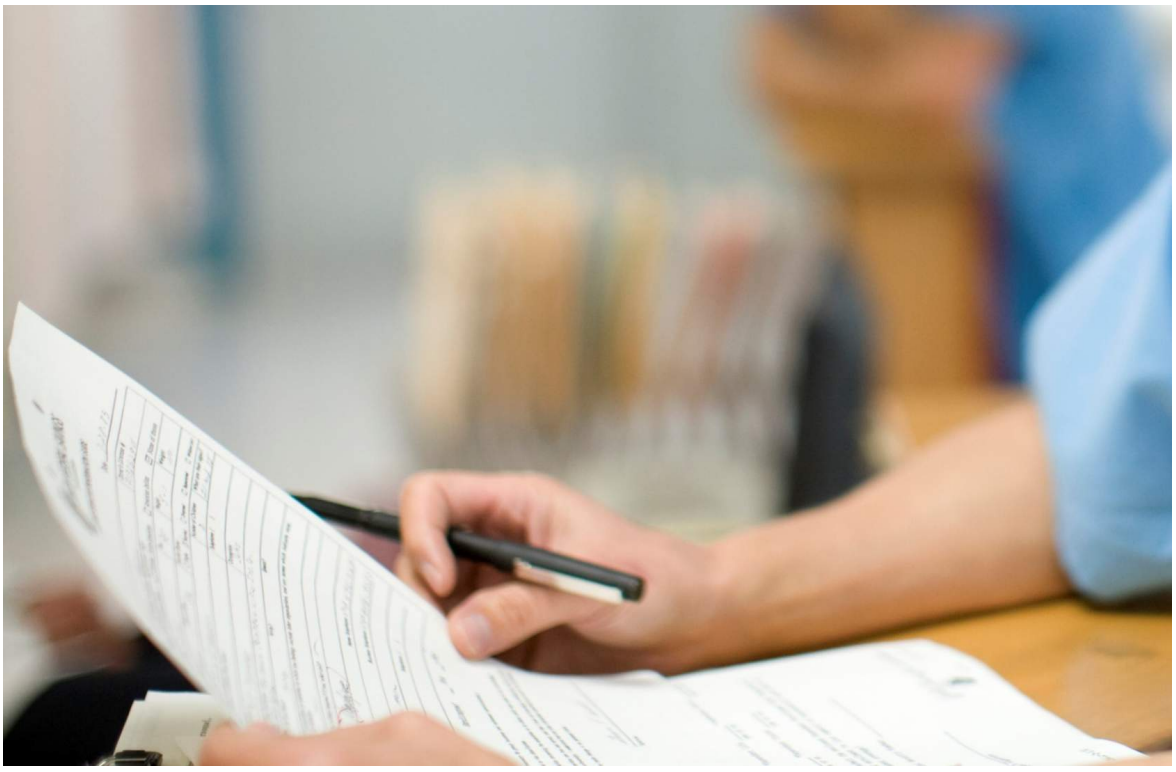
1. Verify the fax number before pushing the send button.
2. Double check that only the information on the correct patient is included in the information being faxed.
3. When dictating reports, make sure the referring physician is correctly listed (i.e. full name or spelled out).
4. Only use the official **UCI Health fax cover sheet**.

Paper

Another risk to patient privacy occurs when patient information is left unattended in areas that are accessible to non-UCI Health workforce members.

NOTE: Even areas that are designated as "staff only" areas can cause problems if the door to the area is unlocked or unmonitored, and anyone can wander into the area.

To protect patient information left in unattended areas:



Keep documents and paperwork containing confidential information covered and placed in an appropriately secured area, folder, or cabinet.

Ensure that when you leave the area unattended, no patient information is left out.

Dispose of material containing patient health information in a confidential shred container.

Ensure that patient information on computer screens or whiteboards is not visible to anyone walking by.

Do not prop doors open, making confidential information accessible to anyone walking by.

If you see someone in an area where patient information is being used, verify that they have a job responsibility to be there by confirming they have an ID badge. If the individual is a vendor, they should be accompanied by a UCI Health workforce member and have a vendor badge with their photo and current date.

Human Error

Another common problem can occur when a patient is being discharged and another patient's file is mixed into the file of the patient being discharged. This can be particularly harmful for the patient if the information includes their diagnosis, treatments, and medications.

When mailing information to a patient, make sure the information is placed in the correctly addressed envelope. Double check before sealing the envelope.

To protect patient information when discharging patients:

Double check that you have the correct patient and the correct information.

Ensure that you've correctly registered the patient under the correct Medical Record Number.

Ensure that you've correctly entered the information into the correct record.

Confirm that you have printed out the correct record.

Confirm that the correct patient's information is on each page.

6

Photography

- ☐ PHI includes any photograph of a patient that is identifiable. It is often impossible to de-identify the image of a patient's face or other unique features such as a tattoo or scar.
- ☐ If the photo is being used for patient care, the photo must be included in the patient's medical record. No authorization is required.

- [ ] If the photo is being used for any other purpose, such as teaching or research, an appropriate authorization must be obtained.

- [ ] Refer to the Photography and Multi-Media Recording Patients policy on the Policy and Procedures website: **Photography and Multi-Media Recording Patients Policy**.

- [ ] The authorization forms are on the **Compliance & Privacy website**.

- [ ] If the image is being used for teaching or research purposes, the image must be downloaded to a secure encrypted server as quickly as possible.

- [ ] The images must then be deleted from the camera or recording device after download, or if the image is no longer needed.

- [ ] The images must not be uploaded to a third-party cloud computing site unless the Chief Information Security Officer has approved the third-party cloud computing.

- [ ] Patients and their families may only record staff and providers with express permission.

Social Media

Social media poses significant risks to patient privacy.

Staff working in healthcare often want to relieve stress of job by sharing information with others.

Risks are present even when patients are not identified by name. Enough circumstantial information can be provided that others will be able to identify the patient.

NO patient information should ever be posted to social media sites, regardless of whether it includes the patient's name or identity.

Posting photos (even if they are deidentified) is prohibited.

Privacy

Never *post Protected Health Information (PHI) -* ***no*** *exceptions.*

Responsiveness

Monitor your web page and respond to questions and concerns. When appropriate, respond offline.

Reporting

Contact the Compliance and Privacy Office should you have concerns about what you have viewed on a social network.

Respect

You are a member of the UCI community. Be mindful of the information you place on a social media site.

Social Networking Policy

Refer to PolicyStat for the Social Networking Policy

7

Social Engineering

Social engineering is the process of obtaining information by manipulating and exploiting the goodwill of others.

The “social engineer” typically calls or sends an email pretending to be someone else or shows up at your workplace under false pretext. Social engineers are interested in gaining access to organizational and personal information, primarily to perpetuate

fraud, commit industrial espionage, or simply to disrupt activities.

A social engineer is on the lookout for bits of information that can help him or her assume someone else's identity, usually without that person's knowledge.

The information they want includes:

Passwords	Personal information
Bank Accounts and credit card information	Sensitive business information
Social engineers exploit the trust, courtesy, naiveté, lack of	Social engineering attacks can easily be prevented.

The following best practices will help ensure better protection for your personal information and the University's sensitive and confidential information

DON'T GIVE... | BE CAUTIOUS... | YOUR PASSWORDS...

Don't give private information to anyone you don't know or who doesn't have a legitimate need for it (whether in person, over the phone, via email or the Internet).

DON'T GIVE... | BE CAUTIOUS... | YOUR PASSWORDS...

Be cautious about what you say in elevators, restaurants, trains, buses, and other public places.

DON'T GIVE... | BE CAUTIOUS... | YOUR PASSWORDS...

*Your passwords belong to you. **Never** disclose them to anyone.*

SHRED... | IF AN UNKNOWN PARTY... | REPORT...

*Shred sensitive and confidential information in a confidential shred container. **Never** put it in the garbage intact.*

SHRED... | IF AN UNKNOWN PARTY... | REPORT...

If an unknown party is present in your office, request identification and escort the stranger to their host. If they do not know the location of their host, direct them to the Security Office or front desk reception area.

SHRED...	IF AN UNKNOWN PARTY...	REPORT...

Report suspicious behavior and calls to your Instructor/Coordinator.

Summary

You should now have knowledge of :

- [ ] Ways to prevent a data breach or unauthorized disclosure of patient information
- [ ] Specific examples of what you can do to protect patient information

Privacy & Security

Importance of Privacy & Security

It is important for employees to maintain the privacy and security of patient information and understand your responsibilities.

At the end of this section, you will be able to:

- Know how and when to report violations in privacy and security or unauthorized disclosure of patient information
- Identify the importance of maintaining the privacy and security of patient information

1

Reporting a Privacy or Security Violation

To report a privacy or security violation:

Notify

Notify your supervisor or manager immediately.

Complete an online incident report on the Safety & Quality Information System (SQIS) located on the UCI Health Intranet: Incident Report.

Immediately contact the Compliance & Privacy Office: 888-456-7006 or hacompliance@hs.uci.edu.

If it involves electronic information also contact Information Services: 714-456-3333.

Theft

If there has been theft of a computer, notify the UCI Medical Center Security Department and/or UCI Police Department.

2

Everyone at UCI is responsible for identifying and reporting privacy breaches on the day you become aware.

Privacy Violations

Privacy Violations can result in Fines & Penalties

- HIPAA and California's information privacy laws impose significant fines for breaches or other misuses of patient information
- Fines depend on whether the breach could have been avoided and whether the organization acted quickly to correct the breach
- This is why we rely on each workforce member to take immediate action when they know of or suspect a breach!

Click the front of each card below to flip for more.

Privacy violations can result in fines & penalties.

HIPAA and California's information privacy laws impose significant fines

Fines are dependent on whether the breach could have been

Additional penalties can be levied at the State level as well by the California

Privacy violations will result in disciplinary action

In addition to possibly being fined, employees who access, use, or disclose patient information without authorization will face disciplinary action up to and including

Potential Federal Fines & Penalties

As of 3/17/2022:

VIOLATION CATEGORY	PENALTY RANGE FOR EACH VIOLATION	MAXIMUM PENALTY FOR ALL VIOLATIONS OF AN IDENTICAL PROVISION IN A CALENDAR YEAR
Did not know (and by exercising reasonable diligence, would not have known) that it violated the applicable provision	$127 to $63,973	$1,919,173
Violation is due to reasonable cause and not to willful neglect	$1,280 to $63,973	$1,919,173
Violation is due to willful neglect and was corrected during the 30 day period beginning on first day entity knew (or should have known)	$12,794 to $63,973	$1,919,173
Violation is due to willful neglect and was not corrected during the 30 day period beginning on first day entity knew (or should have known)	$63,973 to $1,919,173	$1,919,173

Federal Register / Vol. 87, No. 52, March 17, 2022

Resources

Information Security:

- Your Instructor/Coordinator
- Chief Information Security Officer: **714.456.7839**
- Your department's IT person
- Help Desk: **714.456.3333**

Privacy and Confidentiality:

- Your Instructor/Coordinator

- Privacy Office: **714.456.7006** or Internal: **120.7006**
- Email: **hacompliance@hs.uci.edu**
- UCI Health Privacy website: **http://www.ucihealth.org/compliance/privacy-compliance/**
- UCOP Privacy Compliance website: **https://www.ucop.edu/ethics-compliance-audit-services/compliance/privacy/index.html**
- Confidential Compliance Message Line: **1.888.456.7006**

Policies And Procedures are available at: Policies & Procedures

Confidentiality Agreement

In order to receive credit for completing this course, you will need to read and sign the following confidentiality statement.

The protection of health and other confidential information is a right protected by law and enforced by individual and institutional fines, criminal penalties as well as UC policy. Safeguarding confidential information is a fundamental obligation for all employees, clinical faculty, house staff, students, technicians, staff, and volunteers.

I understand and acknowledge that:

- [ ] I will always protect the privacy and security of confidential information, both during and after my employment with the University of California has terminated.

- [ ] I agree to (a) access, use, or view confidential information to the minimum extent necessary for my assigned duties; and (b) disclose such information only to persons authorized to receive it.

- [ ] I understand that UC may conduct surveillance of users' access to electronic records. User IDs enable discovery of inappropriate access to both patient records or employee records.

- [ ] Inappropriate access, use, or disclosure of protected information will result in disciplinary action, up to and including termination of employment, and may result in a report to authorities charged with professional licensing, enforcement of privacy laws, and prosecution of criminal acts. The State of California may levy penalties to individuals or providers of healthcare up to $250,000 per violation, depending on the circumstances.

- [ ] User IDs cannot be shared. Inappropriate use of my ID (whether by me or anyone else) is my responsibility and exposes me to severe consequences.

- [ ] I must adhere to all University Privacy and Information Security policies.

☐ The Compliance & Privacy Office is available to answer any and all questions and concerns I may have regarding patient privacy. The Compliance & Privacy Office can be reached at **714.456.7006**.

By clicking **I AGREE** below, I acknowledge that I have read the University of California Privacy Training course and confidentiality statement and agree to abide by UC policy and Federal/State privacy laws.

Quiz

The quiz will cover content that you have read in the **Privacy & Security Training: Federal & State Healthcare Privacy Laws** course.

As you take the quiz, please remember:

- A score of 100% is required to pass.
- Allow time to complete the quiz.
- Answer each question by filling in the appropriate bubble on page 99.

Question

01/10

Who has to follow the HIPAA Law?

A. Physicians

B. Physicians and all other patient care providers

C. Only supervisors and other administrators

D. All UCI Health workforce members

Question

02/10

The Nursing Manager in the Emergency Department noted that Janet did an exceptional job with the unusual medical situation posed by her patient that morning in the Emergency Department. She asks Janet to present the case at the nursing staff meeting next week. ***Which of the following apply?***

A. Janet cannot discuss the case as it would violate HIPAA.

B. Janet can present the case as long as she does not provide any identifying information about the patient.

C. Janet can provide full details on the case including patient name for discussion with the other nurses since this is for education.

Question

03/10

Janet is a nurse in the Emergency Department and took care of a patient with a unique medical condition. At lunch, Janet meets friends who work in other areas of the hospital. During their conversation, Janet talks about the case including the patient's condition and treatment. ***Which of the following is correct?***

A. Since Janet's friends are all UCI Health employees, Janet can disclose information about her patient's treatment even though her friends are not involved in the patient's care.

B. Even though Janet's friends are all UCI Health employees, Janet can only discuss patient information with those who are involved with the patient's care.

C. Janet can talk about her patient's care with her friends as long as others in the area cannot hear.

Question

04/10

A patient who suffered a heart attack came into the emergency room with his wife. After successful treatment, the patient was stabilized and admitted to the cardiac care unit. Can you provide periodic updates to the patient's wife on his progress, results of treatment, and prognosis?

A. No

B. Yes

Question

05/10

After a patient received the Notice of Privacy Practices, how can UCI access, use, or disclose the patient's Protected Health Information?

A. For treatment of the patient

B. For payment of bills related to the patient's care

C. For healthcare operations

D. All of the above

06/10

A 19-year-old UCI student is admitted through the ER for injuries sustained in a motor vehicle accident. She is in stable condition, but not awake nor alert. Her father calls from Minnesota asking for information about her condition.

A. Tell the father the patient's general condition and status

B. Provide no information to the father

C. Inform the father that she had been drinking alcohol, which caused her motor vehicle accident

D. Inform the father of her general condition and status, and obtain her consent to provide any further information

Question

07/10

Your sister's best friend just had triple bypass surgery at the medical center. Your sister asks you what the friend's prognosis is. *What should you do?*

A. Ask a nurse on the floor and pass on the information

B. Log into EMR and pass on the information

C. Tell your sister that it is a privacy violation for you to ask around or look at this information in EMR

D. None of the above

08/10

You are on a work computer using the Internet. A window appears on your browser asking if you would like to have your password saved or remembered.

A. Say yes, you have too many passwords to remember.

B. Say yes, you don't have time to ask the IS department to reset your password if you forget it in the future.

C. Say no, do not let web browsers or any software to remember your passwords.

D. Say no, you can always change your mind later and say yes.

Question

09/10

A medical assistant faxes a patient's PHI to Dr. Zavier at another hospital. She receives a phone call from Dr. Zavier's office that they never received the fax. She checks the number, and realizes that she selected the wrong number that was pre-programmed into the fax machine. Dr. Smith's office calls to let her know that they received the fax. ***Is this a privacy violation? How should the employee fix the situation and prevent it from recurring?***

A. Yes, this is a violation. The medical assistant must contact the affected patient to notify them.

B. No, this is not a violation. She should fax a copy of the information that is still needed to Dr. Xavier and double check the number before faxing.

C. No, this is not a violation. However, she must report the incident immediately to her Instructor/Coordinator.

D. Yes, this is a violation. She should complete an SQIS incident report so the Compliance and Privacy Office can be notified. The Compliance and Privacy Office will investigate, get documents back, and reach out to affected parties, if needed.

Question

10/10

What does UCI Health have to do now that we know there was a breach?

A. Staff should report the breach to the Compliance and Privacy Office, and in the online SQIS reporting system.

B. The unit manager should remind all staff at the next morning's huddle to double check fax numbers before faxing information.

C. Ask the incorrect recipient to send the information back to UCI.

D. All of the above

Lesson 11 of 11

Completion

You have completed **Privacy & Security Training: Federal & State Healthcare Privacy Laws**.

UCI Health

Acknowledgement of Review of the UCI Health Privacy & Security Training: Federal & State Healthcare Privacy Laws

By signing below, I acknowledge that I have read the University of California Privacy Training course and confidentiality statement and agree to abide by UC policy and Federal/State privacy laws.

_____ _____

Student Name Student Signature

_____ _____

Date School

_____ _____

School Coordinator Date

Quiz Answers: **Score:_____**

1) Ⓐ Ⓑ Ⓒ Ⓓ
2) Ⓐ Ⓑ Ⓒ
3) Ⓐ Ⓑ Ⓒ
4) Ⓐ Ⓑ
5) Ⓐ Ⓑ Ⓒ Ⓓ
6) Ⓐ Ⓑ Ⓒ Ⓓ
7) Ⓐ Ⓑ Ⓒ Ⓓ
8) Ⓐ Ⓑ Ⓒ Ⓓ
9) Ⓐ Ⓑ Ⓒ Ⓓ
10) Ⓐ Ⓑ Ⓒ Ⓓ

Please note that only this page from this packet needs to be returned to the Education Department.