Health Insurance Portability and Accountability Act (HIPAA) Training

UC San Diego Health Sciences Office of Compliance and Privacy

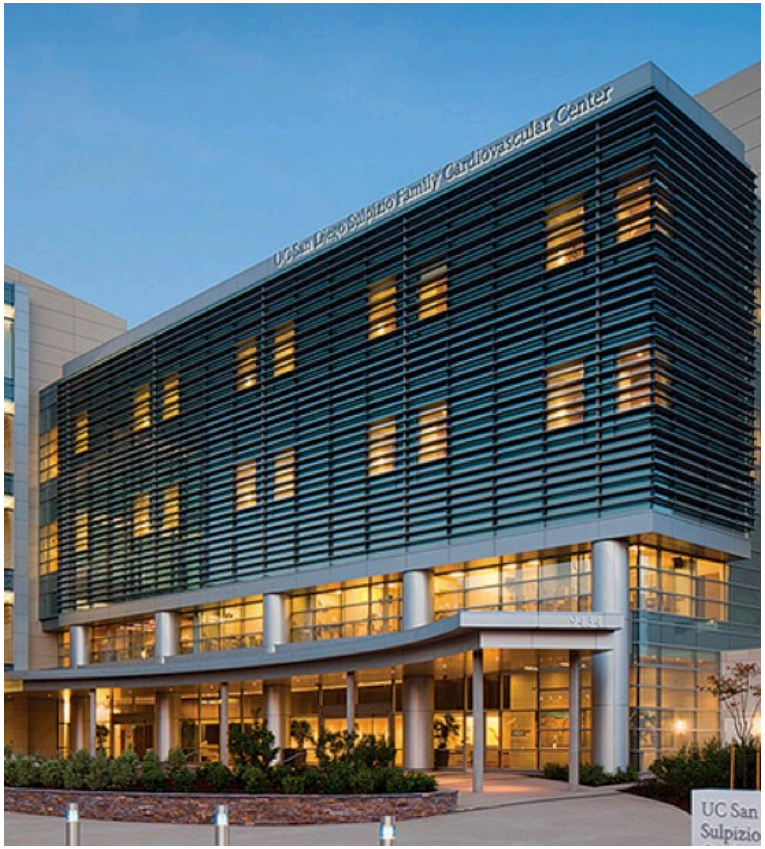
What is HIPAA?

- Health Insurance Portability and Accountability Act
- Federal law established in 1996
- Describes safeguards to prevent unauthorized access to **Protected Health Information**
- A covered entity must comply with HIPAA and may not use or disclose **Protected Health Information**, except as permitted or required by law.

UC San Diego Health is a covered entity and all team members must comply with HIPAA and other applicable privacy laws.

What is HITECH?

- Health Information Technology for Economic and Clinical Health (HITECH)
- Became effective in 2009
- HITECH addresses the privacy and security concerns associated with the electronic transmission of health information
- An enhancement to HIPAA



What makes data Protected Health Information (PHI)?

- Name
- Address
- Patient dates (DOB, Admin, Discharge Dates)
- Account #
- Fax #
- Drivers License #
- Medical Record #
- Health Plan Beneficiary #
- Full-Faced Photos
- IP Address
- Telephone #
- VIN/Serial #
- Finger Prints
- Voice Recordings
- Serial Numbers
- Devices ID Numbers
- URL Address
- Email Address
- Biometric ID
- Any other unique ID #

- Clinical Notes
- Diagnosis
- Imaging
- Prescriptions
- Demographic Information
- Patient Reports
- Dates of Service
- Bills
- CPT Code
- Invoices
- Claim Detail
- Individual insurance data
- Etc.

- Personally Identifiable Information paired with a patient's health data creates PHI.
- Protected Health Information is protected by the HIPAA regulations.

Protected Health Information (PHI)

Protected Health Information (PHI) is any personal or health information UC San Diego creates or maintains in the course of providing treatment, obtaining payment for services, or while engaged in health care operations including teaching and research activities.

• Name	• Fax	• IP Address
• MRN	• Account #	• Insurance #
• Address	• Images	• License #
• Phone	• URL Address	• Vehicle #
• Email	• SSN	• Device #
• Dates	• Biometric ID	• Other

Policy

UCSDHP 10, PHI: De-identification, Limited Data Set (LDS) and Data Use Agreement (DUA)

When Can I Use PHI?

HIPAA permits the use and disclosure of Protected Health Information (PHI) for treatment, payment and healthcare operations (TPO). If performing any of these activities as a part of your work, a patient written authorization is not required. If you need to disclose PHI for reasons other than TPO, the patient must submit written an Authorization to Release Protected Health Information. Remember, Always use the minimum amount of PHI necessary to accomplish a task.

Examples of TPO:

- Sharing a patient's demographics
- Sharing a patient's appointment date with a patient's insurance company to process your payment
- Sharing a treatment diagnosis with the patient's primary care provider who works at another hospital

How to Safeguard PHI?

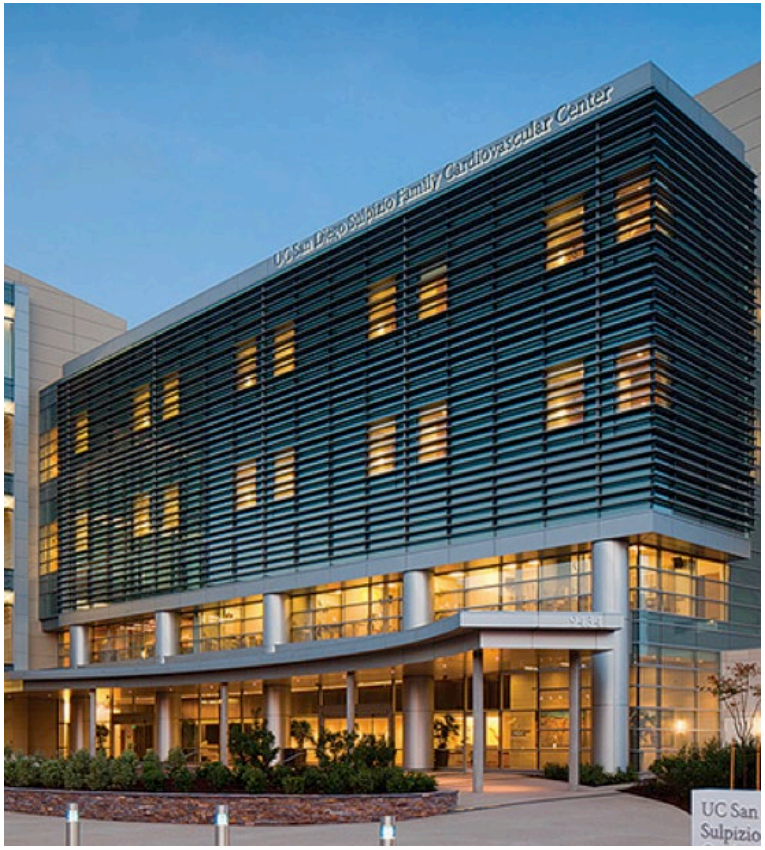
Understand the risks to privacy and information security, recognize suspicious activity, and know how to react to it.

Examples of how to protect PHI:

- Double check patient identifiers
- Only access, use or disclose patient electronic health information to perform UC San Diego job duties.
- Log-out of applications when done
- Lower your voice to keep private information from being overheard
- Be aware of your surroundings
- Avoid discussing patient / personal information in public areas

What Is Unauthorized Access Of PHI?

- Definition: Unauthorized access is viewing or using any PHI that is not required to perform your job duties.
- Unauthorized access of PHI is never acceptable.
- Failure to utilize PHI correctly could result in disciplinary action and/or termination.
- Examples of Unauthorized Access:
  - *Making a birthday list*
  - *Delivering flowers to a hospitalized co-worker*
  - *Checking a family member's appointment time*



Protect PHI

- E-Mail encryption is a security measure utilized by UC San Diego Health to protect PHI
- Add Secure: in an email subject line to encrypt the email
- Examples to protect electronic devices:
  - *Use a privacy screen*
  - *Password Protect*
  - *Auto lock/ logoff*
  - *Regularly install security updates*
  - *Install anti-virus software*
  - *Only use secure Wi-Fi connections*
  - *Use secure VPN*
  - *Delete all PHI before discarding*

Scenario

You just got hired as a UC San Diego Health employee. You have access to the UC San Diego Health Electronic Heath Record system and you want to check to make sure your co-workers have received the Flu Shot.

Is this OK?

A: Yes

B: No

Answer

B: No

It is never ok to access health information in the UC San Diego Health Electronic Health Record for personal reasons. Accessing co-worker information for personal reasons is considered unauthorized access and it is never allowed.

Failure to utilize PHI correctly could result in disciplinary action and/or termination.

Scenario

You are done with work and you are walking to the parking lot. You find a patient's after visit summary on the ground.

What should you do?

A: Notify your privacy officer, supervisor and/ or manager.

B. Contact the Accountable Care Network (if it is an Accountable Care Network related issue).

C. Answers A and B are both acceptable answers.

Answer

C: Answers A and B are both acceptable answers.

If you find patient information or detect a HIPAA violation or privacy concern, take at least one of the following actions immediately:

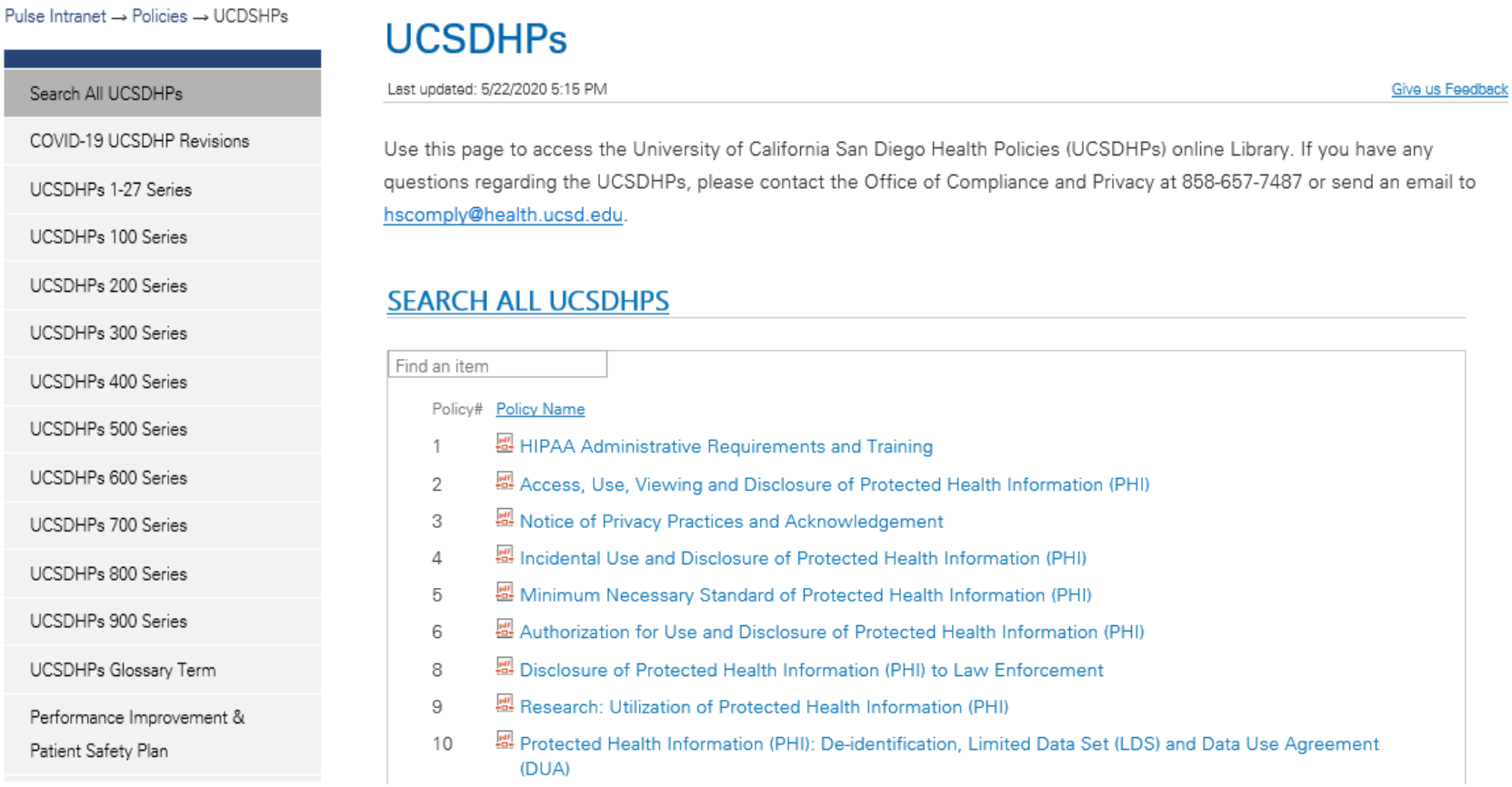
- Notify your privacy officer, supervisor and/ or manager.
- Contact the Accountable Care Network at physiciannetwork@health.ucsd.edu or 800-633-4227.

How to Report Potential Violations

Accountable Care Network:
800-633-4227,
physiciannetwork@health.ucsd.edu

REPORT ALL PRIVACY INCIDENTS TO YOUR DESIGNATED HIPAA REPRESENTATIVE

UC San Diego Health Policies (UCSDHPs)



UCSDHP Main Policy Site

Office of Compliance and Privacy Pulse Site

UC San Diego Health

Questions?

Accountable Care Network

T: 800-633-4227

physiciannetwork@health.ucsd.edu

Contact your appropriate compliance or privacy department/representative