HIPAA 101

Privacy and Security
Course Objectives

This training is intended to be an introduction to privacy and security at UCSF, and will include:

• Overview of federal and state privacy requirements, as well as UCSF policies and procedures which govern the protection of privacy and the security of confidential information

• Discussion of how these rules affect you and your job and what you must do to protect confidential and sensitive information

• Instructions on how to report privacy breaches and security incidents

If you have specific questions not covered in this training, please contact the UCSF Privacy Office for guidance at (415) 353-2750.
Relevant Privacy Laws

There are a number of privacy laws that UCSF is required to comply with, some of which include:

- Federal
  - HIPAA
  - HITECH
  - Final Omnibus Rule
- California Medical Information Act (CMIA)
- Information Practices Act
What is HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) is a federal law that requires UCSF to:

• Protect the privacy and security of patient health information

• Adhere to the “minimum necessary” standard for use and disclosure of protected health information

• Notify patients of their rights for access, use, and disclosure of their health information

• Report privacy violations to affected patients and Department of Health and Human Services
HIPAA Gives Patients Specific Rights

• Right to access and receive a copy of one’s own protected health information (“PHI”) (paper or electronic formats)

• Right to request amendments to information

• Right to request restriction of PHI uses and disclosures

• Right to restrict disclosure to health plans for services self-paid in full (“self-pay restriction”)

• Right to request alternative forms of communications (mail to P.O. Box not street address; no message on answering machine, etc.)

• Right to an accounting of the disclosures of PHI

• Refer to the Notice of Privacy Practices to determine where to direct these requests
California Medical Information Act (CMIA)

- Requires institutions and individuals to protect the confidentiality of medical information
- Unauthorized access includes the inappropriate review or viewing of patient medical information without a direct need for diagnosis, treatment or other lawful use
- Licensed facilities, like most UCSF Health hospitals and clinics, are required to report incidents of unauthorized access, use, or disclosure of medical information to the California Department of Public Health (CDPH), and to the affected patient within a short timeframe
- When you suspect or know of a breach you must report it to the Privacy Office immediately
  - UCSF Health employees must also submit an Incident Report
Privacy is bigger than HIPAA

• Other Federal Laws
  – Medicare Conditions of Participation promoting patient rights including privacy
  – Federal Trade Commission protection of consumer privacy
  – FERPA protection of student education records
  – HHS and multiple agencies’ protection of information
  – Computer Fraud and Abuse Act

• Other California State Laws
  – Confidentiality of Medical Information Act (CMIA)
  – Title XXII protections of patient records
  – Information Practice Act
  – Breach notifications
  – Lanterman-Petris-Short (LPS) protection of mental health records

Bottom Line: Remember the basics, and call the Privacy Office with questions!
Fines and Penalties

Privacy violations may carry penalties under federal HIPAA/HITECH, state privacy laws, and UC policies:

- **HIPAA Civil Penalties**
  - $100 - $1,500,000 / violation

- **HIPAA Criminal Penalties**
  - $50,000 - $250,000 fines
  - Imprisonment up to 10 years

- **State Laws**
  - Fines and penalties apply to individuals as well as health care providers, up to $250,000 and may impact your professional license
  - Imprisonment up to 10 years

- **UCSF corrective and disciplinary actions**
  - Up to and including loss of privileges and termination of employment
  - Refer to Campus Policy 200-32, “Workforce Sanctions for Patient Privacy Violations”
UC/UCSF Policies

• As a UCSF workforce member, you are not expected to understand every nuance of every privacy regulation

• Rather, UC and UCSF developed policies and procedures designed to help you comply with federal and state privacy laws

• You are responsible to follow these policies and procedures (posted on http://hipaa.ucsf.edu)

• For questions, ask your supervisor or contact the Privacy Office

• Remember that privacy applies to ALL verbal, written, and electronic confidential information
Workforce Privacy Training

- UCSF provides initial and ongoing privacy and security training to its *workforce members* about the University’s privacy and security policies and specific procedures which may affect the work you do.

- Privacy newsletters are published throughout the year.

- Additionally, educational resources can be found at the UCSF Privacy Office website at http://hipaa.ucsf.edu/
What Information Must Be Protected?

• You must protect an individual’s Protected Health Information (PHI) that is collected or created as a consequence of providing health care

• PHI:
  • Information related to a patient’s past, present or future physical and/or mental health or condition
  • Includes at least one of the 18 personal identifiers (see next slide)
  • In any format: written, spoken, or electronic
  • Includes health information about individuals who have been deceased less than 50 years
18 Protected Health Information (PHI) Identifiers

1. Name
2. Postal address
3. All elements of dates except year
4. Telephone number
5. Fax number
6. Email address
7. URL address
8. IP address
9. Social security number
10. Account numbers
11. License numbers
12. Medical record number
13. Health plan beneficiary #
14. Device identifiers and their serial numbers
15. Vehicle identifiers and serial number
16. Biometric identifiers (finger and voice prints)
17. Full face photos and other comparable images
18. Any other unique identifying number, code, or characteristic
Notice of Privacy Practice

In order for UCSF to use or disclose PHI:

• UCSF must give each patient a Notice of Privacy Practice (NPP) that:
  ▪ Describes how UCSF may use and disclose PHI
  ▪ Advises the patient of his/her privacy rights

• UCSF must attempt to obtain the patient’s signature acknowledging receipt of the Notice, except in emergency situations. If a signature is not obtained, UCSF must document the reason why.
UCSF’s Use and Disclosure of PHI

The NPP allows UCSF to use and disclose PHI for purposes of TPO (primarily):

- **Treatment**: Patient’s referring MD requests a copy of the patient’s recent exam at UCSF

- **Payment**: Patient’s insurance company requests a copy of the patient’s medical record for a specific service date to validate medical necessity

- **Operations**: Quality Improvement Office requests a copy of an Operative Report

- Unsure as to what constitutes TPO? Just ask your manager or the Privacy Office!

- **Note**: UCSF must have a Business Associate Agreement (BAA) with vendors who will access or use PHI when providing a service UCSF’s behalf
Other Uses and Disclosures

Other ways in which UCSF can use/disclose PHI:

- To the individual
- Directory information
- As required by law
- For public health activities
- To report abuse/neglect
- For health oversight activities
- In relation to judicial/administrative proceedings
- For law enforcement purposes
- To decedents
- For transplant procedures
- To prevent serious threat to health/safety
- For essential government functions
- Limited Data Sets
Purposes Other Than TPO

- Unless required or permitted by law, UCSF must obtain written authorization from the patient to access, use or disclose their information for purposes other than Treatment, Payment and Operations.
  - Exception: Final Omnibus Rule provided greater flexibility to release child immunization records to schools where state law requires them to have proof of immunization (e.g., California schools). While you still need to obtain parental agreement to disclose the records, this agreement can be verbal or written; verbal agreement must be documented in the patient’s record.
Purposes Other Than TPO (Research)

- PHI may be used for human subjects research only after the following have been met:
  1. An Institutional Review Board (IRB) has approved the research; and
  2. Both the Informed Consent and HIPAA Authorization have been signed by the subject, or the IRB has approved a Waiver of HIPAA Authorization

- NOTE: if you obtain or use PHI for research purposes with only an Informed Consent but without a HIPAA Authorization, it is considered an unauthorized disclosure under HIPAA.
Purposes Other Than TPO (Fundraising)

If you are involved in fundraising, additional rules apply:


- Review Policy 450-10 Authority Gifts and Private gifts at http://policies.ucsf.edu
  - UCSF policy requires coordination with UDAR for all fundraising efforts that target patients
  - Only limited patient information may be disclosed to UCSF’s Development and Alumni Relations (UDAR) office for fundraising purposes without patient authorization
  - Only a patient’s healthcare provider may request that the patient sign the Authorization; authorizations must be forwarded to UDAR
  - Contact UDAR for fundraising-related questions at giving@ucsf.edu or (415) 476-6922

- Fundraising staff must also complete the Advanced HIPAA for Fundraising module on the UC Learning Center
Minimum Necessary

• HIPAA requires users to access the minimum amount of information necessary to perform their duties
  ▪ Example: a billing clerk may need to know what laboratory test was done and on what date, but not the result

• However, for patient care and treatment, HIPAA does not impose restrictions on use and disclosure of PHI by health care providers
  ▪ Exceptions: psychotherapy information, HIV test results, and substance abuse information
Scenario 1

I do not work with patients or have access to medical records, however I see patients pass by my desk in the clinic. Can I talk about the patients with my coworkers, family and friends even if it has nothing to do with my job?

A. You may not discuss any patient information with anyone unless required for your job

B. You may only talk about the patient with your coworkers

C. You may only talk about the patient with your family and friends
Scenario 1 - Answer

The correct answer is **A.**

Information can only be used as needed for your job.

A. You may not discuss any patient information with anyone unless **required for your job**

B. You may only talk about the patient with your coworkers

C. You may only talk about the patient with your family and friends
Scenario 2

My co-worker’s husband notified me that my co-worker was recently admitted to the Emergency Department and won’t be coming into work tomorrow. My co-worker and I have a great relationship, and I’d like to know how she’s doing. May I access her records to check on her condition?

A. It is okay as we are friends, so I’m sure she wouldn’t mind me looking at her records

B. I already have approval to access patient clinical systems, so no one will know that I accessed it

C. It is not necessary for my job, so I would be violating the patient’s privacy by accessing her records. I should contact her husband to check on her condition
Scenario 2 - Answer

The correct answer is C.

It is not part of your job – your access to your co-worker’s record would be for personal reasons. Therefore, accessing the record will be a violation of your co-worker’s privacy. Furthermore, your access to the record will automatically be recorded and tracked. There could be serious consequences to your employment.

A. It is okay as we are friends, so I’m sure she wouldn’t mind me looking at her records

B. I already have approval to access patient clinical systems, so no one will know that I access it

C. It is not necessary for my job, so I would be violating the patient’s privacy by accessing her records. I should contact her husband to check on her condition
Use of Social Media

- Do not share on social media any patient information acquired through your work at UCSF, even if the information is public
  - Information obtained from your patient/provider relationship is confidential
  - Posting patient information without authorization is a violation of the patient’s right to privacy and confidentiality
- Even if you think you’ve de-identified the information, it still might be identifiable to others
- NOTE: De-identification of PHI requires removal of all 18 PHI identifiers, which includes “Any other unique identifying number, code, or characteristic” (e.g., photo of a wound; description of a patient’s condition)
- Refer to UCSF’s Social Media Best Practices: [http://www.ucsf.edu/about/social-media-overview/social-media-best-practices](http://www.ucsf.edu/about/social-media-overview/social-media-best-practices)
Scenario 3

You are very upset because a young patient of yours has just coded and was not able to be resuscitated. You want to share this experience and your thoughts and feelings with your family and friends on Facebook. Can you do this?

A. Yes, as long as you do not identify the patient by name, or identify the hospital

B. Yes, as long as you do not identify the patient by name, or identify the hospital, and limit the audience to your closest friends and family

C. You cannot post anything on Facebook that could possibly lead to identification of the patient
The correct answer is C.

- Facebook is considered public domain, and anything you post there is considered public information.
- Your Facebook profile may identify your place of work and your occupation. When linked with your posting, and with any other publicly available information, the additional details may identify the patient.
- Information you obtain from your patient/provider relationship is confidential.

A. Yes, as long as you do not identify the patient by name, or identify the hospital.

B. Yes, as long as you do not identify the patient by name, or identify the hospital, and limit the audience to your closest friends and family.

C. You cannot post anything on Facebook that could possibly lead to identification of the patient.
Sharing PHI with a Representative

- You have a right to engage a representative as needed; however, do not share PHI with an external representative (e.g., union rep, attorney, etc.)

- If you are involved in a labor-related incident and need to share PHI:
  - Contact Labor & Employee Relations
  - They will help ensure that the representative receives the necessary information without compromising patient confidentiality
Verbal Exchanges

- Patients may feel that verbal conversations as part of normal clinical operations are a violation of their privacy.
- Be aware of your surroundings when talking.
- Do not leave PHI on voicemail.
Know Where You Left Your Paperwork

- Double check!! When mailing or handing documents to patients/family members, or scanning/faxing documents, slow down and verify that each document belongs to the correct patient
  - Best practice is to verify and highlight multiple patient identifiers (e.g., full name, DOB) on each page
  - Staple all highlighted/verified pages of the document together
- Check printers, faxes, and copier machines when you are done using them
- Do not leave paper PHI laying on your desk; lock it up at the end of the day
- Be alert to how many copies you are making (e.g., if you accidentally print 2 copies, be sure to retrieve the extra copy from the machine)
Disposal of Paper Documents

- Dispose of paper and other records with PHI in secure shred bins. Do not use regular trash or recycle bins to dispose PHI.
- Shred bins only work when papers are put inside the bins.
- Consult with your manager re: location of the secure shred bin.
Protecting Hard Copy PHI

- Best practice: Do not take PHI offsite
  - Scan/email the notes to yourself or access the PHI remotely from home

- However, if you absolutely must take PHI offsite/transport between campuses, take the following precautions:
  - De-identify the information
  - **Treat PHI like it’s an infant**: It must be kept on your person at all times
Scenario 4

As you conduct patient rounds on the nursing floor, you keep handwritten notes for later reference. What is the best way to protect this information?

A. Do not take the notes off-site

B. Document only the minimum necessary (e.g., omit names, MRNs)

C. Shred the notes as soon as they are no longer needed

D. All of the above
Scenario 4 - Answer

The correct answer is D.

While notes are a critical tool used by healthcare providers to keep track of patients or note particular patient needs or concerns, it is critical these notes are protected from loss, theft, or inappropriate disposal. Follow the safeguards listed below.

A. Do not take the notes off-site
B. Document only the minimum necessary (e.g., omit names, MRNs)
C. Shred the notes as soon as they are no longer needed
D. All of the above
Security of Electronic PHI (ePHI)

- If you use your personal electronic device (e.g., phone, laptop, tablet, thumb drive) for UCSF business, it must be **encrypted**
  - Required by UCSF policy
  - You may be held liable for breaches caused by storing PHI on a personal unencrypted device
- Encryption is the only federally recognized method for securing ePHI
- For assistance with encryption, contact the IT Service Desk at (415) 514-4100
- For guidance to install encryption on your personal device: [https://it.ucsf.edu/encrypt](https://it.ucsf.edu/encrypt)
Viewing Email on Handheld Device

- Active Sync provides a secure way to view email on handheld devices. All Active Sync devices are subject to forced device encryption and the UCSF-wide mobile device security standard.

  - Active Sync allows for remote wiping of a device if it is lost or stolen (*Remote wiping may result in the possible loss of personal data on the mobile device. Prevent permanent loss of data by backing up your mobile device regularly!*)

  - Detailed instructions on how to install Active Sync on your device are available at: [https://it.ucsf.edu/services/email-mobile-access](https://it.ucsf.edu/services/email-mobile-access)

- Please note: Active Sync applies to handheld devices (e.g., phones, tablets) only and not computer laptops or desktops

© 2016 The Regents of the University of California. All Rights Reserved. The Regents of the University of California accepts no liability of any use of this presentation or reliance placed on it, as it is making no representation or warranty, express, or implied, as to the accuracy, reliability, or completeness of the presentation.
Scenario 5

I have a personal laptop at home, which I sometimes use to check my UCSF email on the weekends. However, I never save files containing PHI onto my laptop. Does it still need to be encrypted?

A. No, because I rarely use my personal laptop for UCSF business

B. Yes, because I access my UCSF email, which may result in files automatically downloading to my laptop, without my knowledge

C. No, because I don’t save files containing PHI on my laptop
Scenario 5 - Answer

The correct answer is B.

Your laptop must be encrypted. Accessing UCSF email from your personal laptop may result in your UCSF data, mail and attachments being automatically downloaded and stored on your device. Therefore, it is important that you encrypt your personal device before using it for UCSF business. If the device is lost or stolen, the information in it (both your personal and UCSF information) is secure and inaccessible to thieves.

A. No, because I rarely use my personal laptop for UCSF business

B. Yes, because I access my UCSF email, which may result in files automatically downloading to my laptop, without my knowledge

C. No, because I don’t save files containing PHI on my laptop
Computer Security

• Ensure your computer is physically secured by using lockdown cables, locked drawers, placement in a secured area, etc.

• Never leave your laptop unattended in your vehicle or bag

• Create a strong password and do not share your username or password with anyone

• Log off or lock your computer when done, and every time you walk away

• Ensure information on computer screens is not visible to passersby
  ▪ Consider a privacy screen
  ▪ Lock your PC by using the keyboard command Ctrl + Alt + Delete
  ▪ Use a password to start up or wakeup your computer

• Ensure your personal devices have anti-virus and all necessary security patches and updates

• UCSF IT website: http://it.ucsf.edu/
How to Send UCSF Emails Securely

- All emails containing PHI should be sent using the UCSF secure email system
- Note: The best practice for electronically communicating with Medical Center patients is to use MyChart
- Secure your UCSF email message by starting the subject line with one of the following trigger words:
  - ePHI:
  - PHI:
  - Secure:
- Correct spelling and use of the colon is important
- Detailed instructions are available at: http://it.ucsf.edu/services/secure-email/tutorial/how-secure-email-works
When to Use **Secure Email**

- Best practices is to use secure email when transmitting PHI regardless of whether the email is internal or external.
- If a patient doesn’t want to receive secure emails, and requests unencrypted email communications, you must do the following before honoring the request:
  - Notify the patient of the risks of sending unencrypted emails
  - Document the patient’s preference for unsecured email in the patient’s record.
Additional Security Precautions

- UCSF Medical Center IT automatically updates anti-virus software and necessary security patches weekly. Do not interrupt these updates! You can continue to work while they are being installed.

- Do not install unknown or unsolicited programs

- Practice Safe Emailing
  - Do not open, forward, or reply to suspicious emails
  - Do not open suspicious email attachments or click on unknown website addresses
  - NEVER provide your username and password to an email request
  - Delete spam and empty the “Deleted Items” folder regularly

- It is your responsibility when communicating to send all PHI securely
Scenario 6

I received an email from the Chancellor requesting my UCSF user ID and password. I should:

A. Provide my user ID and password
B. Provide my user ID, but not my password
C. Provide my password, but not my user ID
D. Never share my user ID and password
Scenario 6 - Answer

The correct answer is D.

Never share your user ID and password with anyone! The email you received is likely a scam. Do not respond to the email, delete it, and notify UCSF IT Service Desk.

A. Provide my user ID and password
B. Provide my user ID, but not my password
C. Provide my password, but not my user ID
D. Never share my user ID and password
How to Report Privacy Breaches

**Immediately** report any known or suspected privacy breaches to the Privacy Office at (415) 353-2750.
How to Report Security Incidents

- Immediately report lost or stolen electronic devices (e.g., laptops, smart phones, mobile devices, flash drives) to the UCSF Police Department at (415) 476-1414 (even outside of business hours or if you are overseas)

- Immediately report any unusual or suspected information security incidents (e.g., loss and/or theft of any form of ePHI, as well as unusual computer activity) to your Supervisor and/or the IT Service Desk at (415) 514-4100

- You can also go to the UCSF website: http://security.ucsf.edu
Importance of Immediate Reporting Of Known or Suspected Incidents

Federal and state law requires that unauthorized access, use or disclosure of patient medical information be reported within a very short timeframe to the CA Department of Public Health, US Department of Health and Human Services, and/or the affected patient(s) or their legal representative.
Remember!

1. PHI (identifiable health information) must be protected
   • De-identifying PHI requires removal of ALL 18 identifiers
2. PHI can be accessed, used, and disclosed for TPO (Treatment, Payment, and Operations) and only as required for your job
3. Access, use, and disclose the minimum necessary information to accomplish the task at hand
4. Do not take PHI off-site
5. Encrypt any and all personal electronic devices used for UCSF business
Resources for Privacy and Security

• Your Supervisor/Manager
• Privacy Office
  ▪ (415) 353-2750
  ▪ Chief Privacy Officer: Deborah Yano-Fong
• UCSF Information Security Office
  ▪ (415) 514-4100
  ▪ Information Security Officer: Patrick Phelan
• Online Resources:
  ▪ UCSF Privacy Website: http://hipaa.ucsf.edu
  ▪ UCOP HIPAA Website: http://www.universityofcalifornia.edu/hipaa
  ▪ UCSF IRB Website: http://irb.ucsf.edu/
  ▪ UCSF Security Awareness and Training Website: https://it.ucsf.edu/services/outreach