Advanced HIPAA Healthcare Provider

UCSF Healthcare Provider Training Module
Objectives

• Understand the basics of federal and state patient privacy laws
• Understand your role as a healthcare provider in maintaining privacy of protected health information for: patient care, teaching, research, fundraising, marketing and media
• Be aware of consequences for non-compliance
Basics of Privacy Laws - HIPAA

- The Health Insurance Portability and Accountability Act (HIPAA) is a federal law that requires UCSF to:
  - Protect the privacy of patient health information
  - Secure patient health information (physically and electronically)
  - Adhere to the “minimum necessary” standard for use and disclosure of patient health information
  - Specify patients’ for access, use and disclosure of their health information
Basics of Privacy Laws – HITECH and Omnibus

- The Health Information Technology for Economic and Clinical Health (HITECH) Act and the HIPAA Final Omnibus Rule updated the federal HIPAA privacy and security standards.

Collectively, major updates include:
- Breach notification requirements
- Fine and penalty increases for privacy violations
- Patient right to request electronic copies of the electronic health care record
- Patient right to restrict disclosure to health plans for services self-paid in full (“self-pay restriction”)
- Mandates that Business Associates are directly liable for compliance with HIPAA provisions.
# Basics of California Privacy Laws

## Key Requirements & Fines/Penalties

<table>
<thead>
<tr>
<th>Civil Code 56.36/Health &amp; Safety Code 130200</th>
<th>Health &amp; Safety Code 1280.15</th>
</tr>
</thead>
</table>
| **Mandates the confidentiality of medical information:**  
  - Implement appropriate administrative, technical and physical safeguards to protect the privacy of a patient’s medical information, and implement reasonable safeguards to prevent unauthorized access, use, or disclosure.  
  
  **Individual Fines / Penalties:**  
  - $2,500 – $25,000 per violation  
  - $250,000 – maximum penalty  
  - Potential misdemeanor, if economic loss or personal injury  
    - Potential for civil action by consumer with statutory damages ($1000) in addition to actual damages  
    - Cal-OHI may notify licensing board for further investigation/discipline of individual providers. |  
  **Mandates prevention of unlawful or unauthorized access to, use of, or disclosure of patient medical information**  
  
  **Reporting obligations:**  
  - Incident of unlawful access, use, or disclosure of a patient’s medical information must be reported within 5 days of detection of the breach to CDPH and the affected patient(s) / legal representative.  
  
  **Institutional Fines for failure to prevent or report:**  
  - $25,000 – initial violation (per pt.)  
  - $17,500 – subsequent occurrence  
  - $250,000 – maximum penalty  
  - $100 / day for late reporting  
    - Criteria considered by CDPH included in the determination of amount of the fine.  
    - CDPH may refer violation to CalOHII |
What information must you protect?

• Information you create or receive in the course of providing treatment, obtaining payment for services or while engaged in teaching and research activities, including:
  
  – Information related to the past, present or future physical and/or mental health or condition of an individual; and
  
  – Includes **at least one of the 18 personal identifiers** (see next slide)
  
  – In any format – spoken, written or electronic – including videos, photographs and x-rays

• This information is: **PROTECTED HEALTH INFORMATION (PHI)**

• **Note:** “PHI” excludes health information about individuals who have been deceased for more than 50 years
Protected Health Information (PHI) Identifiers

The 18 Identifiers Defined by HIPAA are:

- Name
- Postal address
- All elements of dates except year
- Telephone number
- Fax number
- Email address
- URL address
- IP address
- Social security number
- Account numbers
- License numbers
- Medical record number
- Health plan beneficiary #
- Device identifiers and their serial numbers
- Vehicle identifiers and serial number
- Biometric identifiers (finger and voice prints)
- Full face photos and other comparable images
- Any other unique identifying number, code, or characteristic
In order for a UCSF Healthcare Provider 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 a patient’s signature acknowledging receipt of the Notice, EXCEPT in emergency situations. If a signature is not obtained, UCSF must document the reason it was not.
The Notice of Privacy Practice allows PHI to be used and disclosed for “TPO”:

- **Treatment**
- **Payment**
- **Operations** (teaching, medical staff/peer review, legal, auditing, quality reviews, customer service, business management)
- Other uses and disclosures required by law
- For other uses and disclosures of PHI, a written authorization from the patient is needed
  - Example: disclosures to an employer, financial institution, or the media, or for research when the IRB has not provided a waiver of authorization
Except for treatment, the “Minimum Necessary” applies

• For patient care and treatment, HIPAA does not impose restrictions on use and disclosures of PHI by health care providers.
  
  – **However,** there are restrictions on disclosure of psychotherapy notes, HIV/AIDS test results and substance abuse information.

• For other purposes, HIPAA requires users to access the least amount of information necessary to perform their duties
  
  – Example: a billing clerk may need to know what laboratory test was done, but not the result
Incidental Uses and Disclosures of PHI

• “Incidental” means a use or disclosure that cannot reasonably be prevented, is limited in nature and occurs as a by-product of an otherwise permitted use or disclosure.
  – Example: discussions during teaching rounds; calling out a patient’s name in the waiting room; sign in sheets in hospital and clinics.

• Incidental uses and disclosures are permitted, so long as reasonable safeguards are used to protect PHI and minimum necessary standards are applied.

• HELP KEEP PHI CONFIDENTIAL
HIPAA gives patients specific rights

- Right to access and receive a copy of one’s own PHI (paper or electronic formats)
- Right to request amendments to information
- Right to request restriction of PHI uses and disclosures. Granting restrictions may affect operations, such as the ability to bill for services. Restrictions should not be granted by faculty, rather refer the patient to the Patient Relations Department
- 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
Consider the following example:

1. You are a healthcare provider. Your friend’s spouse is in the hospital after an accident. Your friend asks you to review what treatment has been provided to the spouse and see if you concur. What are you able to do under HIPAA?

A. Access the person’s chart so that you can communicate with your friend about the patient’s condition.

B. Contact the charge nurse on the floor and ask her to look into the patient records for you.

C. Advise your friend that you can only look at the medical records if you are treating the patient or you receive the patient’s authorization to review the medical record.
Answer:

C. Advise your friend that you can only look at the medical records if you are treating the patient or you receive the patient’s authorization to review the medical record.

Under HIPAA you are only allowed to use information required to do your job.

Since you are not part of the patient care team, it is against the law to access the patient record or ask someone to access it on your behalf – even though you may know the person and just want to be helpful. Remember, that if you were in a similar situation, you may not want your colleagues going through your medical records or those of your spouse or close friend.
Consider the following example:

2. The father and mother of an adult married competent patient are visiting the patient. As a member of the care team, you need to review and provide education to her on the new meds ordered by the physician. One medication is Prozac, a well known anti-depressant. What is the best way to approach a patient when her relatives are in the room?

   A. Ask the patient’s relatives to leave the room.
   B. Go ahead and explain the medications to her. She won’t mind her family members overhearing.
   C. Explain to the patient that you need to discuss her medications with her, and that the information is confidential. If she says her relatives may stay in the room, go ahead explain the medications to her.
C. Explain to the patient that you need to discuss her medications with her, and that the information is confidential. If she says her relatives may stay in the room, go ahead explain the medications to her.

Never assume that the patient has shared her medical information with her relatives.

You should ideally ask the patient’s relatives to step out of the room. If the patient understands that the information is sensitive and she agrees to have her relatives present, you can go ahead and have the discussion with the patient.

The answer would be the same if it had been her husband visiting her. The patient may not have shared all of the information with her husband.
Penalties for Violations

Privacy violations may carry penalties under federal and state privacy laws and UC policies:

- **HIPAA Civil Penalties**
  - $100 - $1,500,000 / year fines
  - More fines if multiple year violations

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

- **State Laws**
  - Fines and penalties apply to individuals as well as healthcare providers, up to a maximum of $25,000
  - 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”
Use or disclosure of psychotherapy notes to a third party requires the patient’s Authorization except:

- Use by the originator of the notes for treatment purposes;
- Use or disclosure by UC for its own mental health training programs;
- Use or disclosure by UC to defend itself in a legal action or other proceeding brought by the individual;
- Use or disclosure that is required or permitted with respect to oversight of the originator of the notes.
Mental health PHI disclosures to the individual

- Unlike HIPAA, California Law allows the individual access to his/her mental health PHI, including psychotherapy notes, upon the patient’s written request.
- UC can deny access to mental health PHI if there is a substantial risk of physical harm/endangerment of life to the patient, in the professional judgment of the provider.
How does HIPAA affect teaching activities?

- Allows the use and disclosure of PHI for the teaching of University of California students (all health professions programs).
- Allows the exchange of PHI for teaching purposes between UCSF and other covered entities, so long as both institutions have a teaching relationship with the patient.
- HIPAA does not allow the use and disclosure of PHI to individuals who do not have a teaching relationship to the University or a teaching relationship to the individual (e.g., attendees at CME conferences or medical/health professions’ lectures). **USE DE-IDENTIFIED INFORMATION OR OBTAIN AUTHORIZATION.**
HIPAA allows the use of a Limited Data Set for Teaching, Research & Public Health

- Allied health professionals from a non-covered entity
- Continuing Medical Education and other education to individuals or entities who may not be part of UC
- Teaching material for undergraduate education
- Research purposes
What is a Limited Data Set?

- The only allowable PHI identifiers in a Limited Data Set are Dates and Zip Codes.
- A Limited Data Set excludes direct identifiers, such as:
  - Names
  - Postal and email addresses
  - Phone and fax numbers
  - Social security numbers
  - Account/MR numbers
  - Health plan beneficiary numbers
  - Certificate/license numbers
  - URLs, IP addresses
  - Facial identifiers
  - Device identifiers and serial numbers
  - Biometric identifiers
- A Limited Data Set may be used and disclosed if a Data Use Agreement is in place between UCSF and the PHI recipient.
- For assistance with Data Use Agreements, contact the Office of Innovation, Technology, & Alliances, Privacy Office or Campus Counsel.
Uses and Disclosures of PHI for Research

- In order to access or use PHI (including Limited Data Sets in most cases) from databases maintained by a UC health care provider or the Medical Center for research purposes, you must obtain appropriate IRB approval for the research protocol.

- Refer to the “Control of Access to and Release of Information from UCSF Medical Center Information Systems for Research Purposes” Policy.

- The IRB for UCSF is the Committee on Human Research (CHR):
  - Website: www.research.ucsf.edu/chr
  - Phone: (415) 476-1814
  - Email: chr@ucsf.edu

- You may need to complete additional education on HIPAA research requirements if you engage in research.
PHI Research Restrictions Go Beyond Clinical Trials

- Virtually all clinical trials require use of PHI. PHI is often also necessary for other research involving the following:
  - Medical Records Review (both living and deceased subjects)
  - Biological specimens (tissue, urine, saliva)
  - Biometrics (images audios, videos, fingerprints)
  - Data sets (depending on type of identifiers attached)
  - Recruitment of potential subjects for research from PHI sources (medical records, databases, etc)
What if a research investigator wants information about my patients?

- As a treating healthcare provider, you cannot discuss your patients and their PHI with research investigators unless your patient has provided a signed HIPAA research authorization to allow this, or if the IRB/Privacy Board has granted a waiver of HIPAA research authorization. However, you can inform your patients about research studies. For example:
  - Research investigators can inform you that there are research studies and clinical trials available to subjects (examples: by information letter, flyers, website, brochures)
  - You can inform your patients of research studies that they might be interested in
  - Patients can contact the investigators based on the information you shared or from advertisements, flyers
How does a researcher gain access to PHI from medical records?

- Health Information Management Services or the Integrated Data Repository will require the investigator to show one of the following as proof of authorization to view PHI:
  - Copy of CHR Approval Letter and the HIPAA research authorization form signed by the patient
  - Copy of CHR Approval Letter with statement of Waiver of Consent/Authorization of individual consent to access PHI
Uses and Disclosures of PHI by Fundraising Staff

- All fundraising activities for UCSF shall be coordinated through the University Development and Alumni Relations office (UDAR)
  - UCSF may only use **demographic information** (e.g., name, age, address) and dates of service for fundraising. Disease, diagnosis or condition may **not** be used to develop a fundraising mailing list.
  - Use of any other PHI for fundraising requires the patient’s authorization.

- Only a healthcare provider may initiate a conversation with the patient regarding the authorization for fundraising using PHI
  - If a patient signs the authorization, send the authorization form to UDAR; or
  - With the donor’s permission, forward the patient’s name to UDAR and UDAR staff will obtain the authorization.
  - Do not disclose PHI to UDAR, unless you have written authorization to do so.
Uses and Disclosures of PHI by Fundraising Staff (cont.)

- **All fundraising communications** sent to UCSF patients must include information describing how the patient may opt-out of future solicitations.
- **UDAR is the office of record** for all fundraising opt-ins and opt-outs.
- **Fundraising mailing lists** must be vetted by UDAR to remove opt-outs.
- For fundraising questions, contact UDAR at giving@support.ucsf.edu.
Uses and Disclosures of PHI for Marketing

- You may use PHI to communicate to patients about:
  - treatment
  - a product or service UCSF provides
  - general health issues: disease prevention; wellness classes, etc.

- **HOWEVER:** if UCSF will receive payment from a 3rd party in exchange for that communication, then authorization must be obtained and must state that UCSF received payment for that communication

- If you provide your patient list to a 3rd party for purposes of marketing a product, patient authorization must be obtained and must state whether UCSF has received payment for providing the list

- Any questions should be directed to the UCSF Marketing Department, to the Office of the General Counsel or to the UCSF Privacy Office
Consider the following example:

3. You are invited by a drug company rep to play golf. During the game, the rep begins talking about a new COX-2 inhibitor the drug company is developing. You give the rep names and phone numbers of a few of your patients with arthritis, believing that they could benefit from the new treatment. A week later, the patients call you complaining about being solicited by the drug company to take part in a clinical trial. What does HIPAA say about this?

A. Since you had good intentions, you have not violated HIPAA.

B. You should stop associating with drug company reps as there are many circumstances that could result in violations of federal law, including HIPAA.

C. Since PHI was disclosed for purposes other than what state and federal law allows, an authorization from the patients should have been obtained before the PHI was released.
Answer:

C. Since PHI was disclosed for purposes other than what state and federal law allows, an authorization from the patients should have been obtained before the PHI was released.

This is an example of marketing under HIPAA. PHI was IMPROPERLY disclosed.

Never provide information to a friend, colleague or business representative UNLESS it is required as part of your job and permitted under HIPAA and/or other state and federal laws. Always keep your patient’s information confidential to maintain your rapport and the patient’s trust. Providing an unauthorized release of information to a drug rep for marketing or research purposes violates state and federal law. This could be interpreted as an illegal disclosure for personal gain (the value of the round of golf) and subject you to a hefty fine and imprisonment.
Uses and Disclosures for Communications with the Media

- You, as the patient’s healthcare provider, must be the initial contact with the patient for communication with the media or for developing University communications that use PHI.

  AND

- You must also obtain the patient’s authorization for the use and disclosure to the media.
Security of ePHI – Recent Headlines

Ever evolving technology brings opportunities and efficiency – but only when managed properly. Consider these recent headlines:

October 2013 – An academic medical center notified 3,541 patients that their ePHI was compromised after the theft of an unencrypted personal laptop.

June 2013 – A healthcare organization notified 13,000 patients that their ePHI was compromised after the theft of an unencrypted laptop.

September 2012 – A healthcare organization agreed to pay the U.S. Department of Health and Human Services $1.5 million to settle HIPAA violations after the theft of an unencrypted personal laptop, containing ePHI of ~3500 patients and research subjects.

How could these incidents have been avoided?
By ENCRYPTING the device.
Do you use your personal device (e.g., laptop, iPhone, iPad, external hard drive) for UCSF business?

*Hint: This includes checking your UCSF email from your personal device.*

*Even if you don’t intentionally save PHI onto your device, your UCSF email files may download to your device without your knowledge.*
Power of Encryption

If you use your device for UCSF business, it **MUST BE ENCRYPTED!!**

- Encryption is the only federally recognized method for securing ePHI
- By having your device encrypted, you can rest assured that the information it contains is secure and inaccessible to others if the device is lost or stolen
- 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/how_do/encrypt-my-personal-laptopdesktop-installation-guidelines
- You may need to attest annually that all of your devices used for UCSF business are encrypted

**Best Practice:** Do not use your personal device to store UCSF data or access UCSF email unless absolutely necessary. And if necessary, the device must be encrypted.
Taking PHI Offsite Involves Risk

• Theft and loss of PHI is a high risk
  – Your car is burglarized and the thief takes off with the PHI (*this happens very often, especially in San Francisco*)
  – Leaving PHI in a coffee shop, restaurant or public transportation

• If your job requires you to work from home or transport PHI between sites, follow best practices:
  – Access PHI remotely via Virtual Private Network (VPN)
  – Securely fax or email the PHI to yourself and securely access it from the offsite location to avoid carrying PHI
  – Ensure all devices used to access ePHI or UCSF email are encrypted (including your personal laptop, iPad, iPhone, etc.)
  – Never leave PHI unattended in your bag, briefcase or your car (even if it’s locked in the trunk!)

• This applies to all types of PHI – paper, films, photos, cameras, CDs and ePHI stored on laptops

• *Treat PHI like it’s an infant: You are responsible for securing and keeping it in your possession at ALL TIMES*
Secure Email

- Secure your UCSF email message by starting the subject line with one of the following trigger words:
  - ePHI:
  - PHI:
  - Secure:

- Detailed instructions available at:
  [http://it.ucsf.edu/services/secure-email/tutorial/how-secure-email-works](http://it.ucsf.edu/services/secure-email/tutorial/how-secure-email-works)

- Use secure email when emailing PHI outside of UCSF, such as emails to patients, vendors or any non-UCSF email address

- Best practice: Use MyChart to electronically communicate with patients

- Note: If the patient doesn’t want to receive secure emails, and requests unencrypted email communications, you must do the following before honoring their request:
  - Notify the patient of the risks of sending unencrypted emails, and
  - Document the patient’s preference for unsecured email in the patient’s record
HIPAA Do’s and Don’ts

• **DO** ENCRYPT all mobile and electronic devices (e.g., laptops, tablets, mobile phones, thumb drives) used for UCSF business, whether personal or UCSF-owned. Note: encryption is the only federally recognized method for securing ePHI.

• **DO** treat all patient information as if you were the patient. Don’t be careless or negligent with PHI in any form, whether spoken, written or electronically stored.

• **DON’T** take PHI off-site, where possible. If you must take PHI off-site, never leave it unattended in your bag, briefcase or your car (even if it’s locked in the trunk). You are responsible for securing PHI taken off-site and keeping it in your direct possession at all times.
HIPAA Do’s and Don’ts (cont.)

• **DO** shred or properly dispose of documents containing PHI—do not place in the recycle or trash bin.

• **DO** use automatic locks on laptop computers and smartphones and log off after each time you use a computer. Purge PHI from devices as soon as possible.

• **DO** use secure networks for e-mails with PHI and add a confidentiality disclaimer to the footer of such e-mails.

• **DON’T** share passwords.

• **DO** use secure email to send PHI via email.

• **DO** discuss PHI in secure environments, or in a low voice so that others do not overhear the discussion.
Use of Social Media

- Be cautious when using social media
- Even if you think you’ve de-identified the information, it still might be identifiable to others
- Be aware that inappropriate use of social media may result in an investigation by the state medical board

- **Remember:**
  - Information obtained from your patient/provider relationship is confidential
  - Posting PHI without authorization is a violation of the patient’s right to privacy and confidentiality
  - 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)
Consider the following example:

4. 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. What must you consider before doing this?

A. Posting this on Facebook is OK as long as you do not identify the patient by name, or identify the hospital, and you are limiting the recipients to your friends and family

B. You cannot post anything on Facebook that could possibly lead to identification of the patient
Answer:

B. You **may not** post anything on Facebook that could possibly lead to identification of the patient

- Facebook is considered public domain, and anything you post there is considered public information
- Posting clinical details without authorization is a violation of your patient’s privacy and confidentiality
- 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
Consider the following example:

5. Your personal laptop contained information about your patients. The laptop was locked in your trunk and it had a complex password.

Since you locked the laptop up and you had a complex password on the device, is this enough to keep you from being personally responsible for the loss of patient information?

A. Yes, I cannot be responsible if someone steals my laptop.

B. No, I am still responsible.
Answer:

B. No, I am still responsible.

The only safe harbor is to ENCRYPT your device.

Note: You may be personally responsible for civil and monetary penalties associated with the incident, and your license may be impacted.
Consider the following example:

6. You are in the ER examining a 6-year-old boy and observe cigarette burns on the arms and hands of the boy. What does HIPAA require you to do?
   A. HIPAA requires you to protect patient confidentiality so no disclosure of PHI should be made.
   B. Patient safety is involved, and federal and state law require that you report this.
   C. HIPAA does not allow you to report this incident, but state law requires it.
Answer:

B. Patient safety is involved, and federal and state law require that you report this.

While HIPAA requires you to maintain patient confidentiality, exceptions exist which allow PHI disclosures. State law requires and HIPAA allows the reporting of child or elderly abuse and communicable diseases.
Remember:

- It is everyone's responsibility to protect PHI – failure to do so could impact your licensure and put you at personal financial risk.

- **Encrypt** all electronic devices containing PHI or used to access UCSF email containing PHI

- Only access information needed to do your job (e.g., for treatment). Do not access patient records for personal reasons (e.g., to check on a friend or family member’s health status).

- Do not post any information about your patients (including photographs) on social media or public outlets without prior authorization.

- Limit taking PHI off-site. Remember you are responsible for securing PHI taken off-site and keeping it in your direct possession at **ALL TIMES**.
Thank you!

- Help us to improve privacy / security of protected health information (PHI).

- Report suspected or known improper disclosures of PHI so UCSF can meet its obligation to mitigate consequences.

- Report privacy concerns to the UCSF Privacy Office (415) 353-2750 or the hotline (800) 403-4744.

- Contact UCSF Privacy Office at (415) 353-2750 for more information on HIPAA or visit our website: [http://hipaa.ucsf.edu](http://hipaa.ucsf.edu)
HIPAA Resources

• UCSF Privacy and Confidentiality Handbook
  – http://hipaa.ucsf.edu/Privacy_Handbook.pdf
• HIPAA 101
• UCSF Privacy Office Website
  – http://hipaa.ucsf.edu/
• UCSF Medical Center Information Technology
  – http://it.ucsfmedicalcenter.org/
• UCSF Information Security
  – http://it.ucsf.edu-security
Completing This Course

When you close this window, you will be asked if you have completed this course.

By clicking yes, you indicate you have reviewed these materials and agree to comply with the provisions of “Advanced HIPAA Healthcare Provider”.