Individual Responsibility

State Law requires notification to California Department of Public Health, and patients, within 5 days of a breach incident. Reporting the event to the State outside of this window will result in fines, disciplinary action, etc. It is necessary to do your part: if you are involved in, or suspect, a breach, report it IMMEDIATELY.

In the event of a breach or suspected breach:

- If the breach involves a disclosure of PHI, immediately :
  1. Call the Privacy Office @ 415-353-2750
  2. If known, be prepared to outline exact data elements disclosed, how many patients were involved, over what time period, to whom and for what purpose the PHI was disclosed
- If the breach involves a loss or theft of UCSF information (e.g., hard copy or e-device with ePHI), immediately :
  1. Report loss to Campus Police @ 415- 476-1414 and the Privacy Office @ 415-353-2750
  2. If known, be prepared to detail exactly what PHI was lost or stolen
- In all incidents, the student should notify their instructor immediately, and the instructor can offer further details if needed
- Report erratic computer behavior or unusual or suspicious emails to IT @ 415-514-4100 Option 2

WHEN IN DOUBT……CALL THE PRIVACY OFFICE!

OTHER RESOURCES

Campus IT Security
Phone: 415-514-4100, Option 2
Website: http://security.ucsf.edu/

UCSF Risk Management
Phone: 415-476-2498
Website: https://www.rmis.ucsf.edu/Default/aspx

UCSF Police
Phone: 415-476-1414
Website: http://www.police.ucsf.edu/

WHAT IS THE PRIVACY OFFICE?

The Privacy Office is responsible for monitoring compliance with the federal and state privacy laws and regulations. The Privacy Office is responsible for overseeing departmental responses in the event of a breach of patient privacy. Additionally, the Privacy Office provides consultation on requests for all privacy related questions. The Privacy Office tracks and analyzes all privacy activities, and develops training and risk mitigation programs for the entire UCSF enterprise.

Privacy: Achieving Compliance Together

UCSF **Privacy** Office

2200 Post Street, C-509
Box# 1922

Phone: 415-353-2750
Fax: 415-353-9241
Website: http://hipaa.ucsf.edu/

Revised June 2013

UCSF PRIVACY OFFICE

UCSF PRIVACY AND SECURITY SURVIVAL TIPS FOR STUDENTS

UCSF
University of California
San Francisco

UCSF PRIVACY AND SECURITY SURVIVAL TIPS FOR STUDENTS

Protecting the privacy and confidentiality of patients' health information is a fundamental ethical concept and standard in healthcare. In today's healthcare environment of digital media, electronic data and new forms of social media communications, always knowing the best way to protect data you are exposed to in an educational environment can be a challenge. It is imperative as a member of the healthcare team, that you understand your responsibilities under state privacy laws and federal HIPAA requirements for use, access and disclosure of patient Protected Health Information (PHI).

Training

Confirm that you have:

1. Reviewed the Privacy and Confidentiality Handbook: (http://hipaa.ucsf.edu/Privacy%20Handbook.pdf);
2. Signed the Confidentiality Statement: (http://hipaa.ucsf.edu/education/downloads/ConfidentialityStatement.pdf);
3. Submitted that signed Statement to Student Affairs; and
4. Attended your school's designated privacy training, or completed the Advanced HIPAA Healthcare Provider Module: (http://hipaa.ucsf.edu/education/downloads/ProviderModule.pdf).

PHI and ePHI

PHI is individually identifiable health information which is created in the process of caring for a patient and is transmitted or maintained in any format, including electronic, written or oral. Examples include patient name, address, date of birth, age, social security #, health insurance #, medical record #, phone #, fax #, email address, etc.

All PHI including medical records, diagnoses, x-rays, photos, images, prescriptions, lab work and other test results, billing records, claim data, referral authorizations, explanation of benefits and research records of patient care must be protected.

ePHI is electronic protected health information. It must be kept on an encrypted computer, and students are responsible for securing home and mobile devices (laptops, phones, memory sticks, etc.) which contain confidential information/ePHI.

Access to PHI

- Utilize the following concepts relating to patient privacy in the clinical environment:
  - A student may access, use or disclose PHI or ePHI for the purposes of Treatment, Payment or Operations (TPO)
  - If a student's access, use, or disclosure is not for TPO and not otherwise covered by the Notice of Privacy Practices (NPP), then an authorization from the patient must be obtained prior to proceeding
  - See pages 2 and 3 of NPP for details:

    http://www.ucsfhealth.org/pdf/3-03ucsfhipaa.pdf
- Students and trainees are **NOT** permitted to remove PHI from UCSF premises under any circumstances
- When you are finished using the PHI, place it in the confidential shred bin to be destroyed—do not place it in the recycle or trash bin

Know Where Your Data Lives

- You are individually responsible for properly containing and securing PHI
- Be cognizant of what PHI you are storing and where this information is being kept: your computer, backup drive, cell phone, memory card, thumb drive, etc



Photography

- Photography is allowed for treatment or safety purposes
- All other photography requires patient consent, including photographs for student education
- Patient photos taken with personal cell phones are **NOT** allowed

Social Media

- **NEVER**, under any circumstance, share PHI on any social media, including social media chat windows (e.g. Facebook, Twitter, YouTube, Instagram, etc):

  http://www.ucsf.edu/about/social-media-guidelines

Email

- When sending ePHI to any email address, students should always use their UCSF account and secure the email by typing one of the following in the subject line: "SECURE:" or "ePHI:" or "PHI:"
- A secure email sent to a non-UCSF recipient will send the message to the recipient to view your email through a UCSF -secured web interface
- **NEVER** send PHI through a personal email account or email chat (e.g. G-Mail, G-Chat, Yahoo Mail, Hotmail, Comcast, etc) not provided by UCSF

Encryption

- Required when your computer, tablet, mobile phone, external hard drive or USB flash drive (personal or UCSF owned) is storing ePHI and/or used to transmit ePHI via UCSF email
- In the event that your electronic device is lost or stolen, encryption prevents others from gaining access to your data
- For more information about encrypting your device:
  - Visit the IT website: http://it.ucsf.edu/services/encryption
  - Contact the IT Service Desk at (415) 514-4100

Minimum Necessary

- You are permitted to access and use only the minimum necessary patient information to do your job
- You are expected to apply the minimum necessary standard when you access PHI and when it is shared in an educational setting:
  1. Access only the minimum information you need to know
  2. Share only the minimum information necessary to accomplish the purpose of the disclosure
- Whenever possible:
  1. Remove or omit patient names (use initials or first name only or blackout the name)
  2. Remove or omit reference to a medical facility:
     - Use blank paper without facility letterhead or blank progress note forms
     - Do NOT include a facility name or logo attached or hand-written in any form
     - Cut and paste patient notes to remove the facility header before submitting to your instructor
  3. Provide De-identified Data