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

• Report erratic computer behavior or unusual or suspicious emails to IT @ 415-514-4100 Option 2

WHEN IN DOUBT......CALL THE PRIVACY OFFICE!
415-353-2750

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.
Access to PHI

- Utilize the following concepts relating to patient privacy:
  - You may access, use or disclose PHI or ePHI for the purposes of Treatment, Payment or Operations (TPO)
  - If your access, use, or disclosure is not for TPO and not otherwise covered by the Notice of Privacy Practice (NPP), then an authorization from the patient must be obtained prior to proceeding
  - See pages 2 and 3 of NPP for details: http://hims.ucsfmedicalcenter.org/HIPAA_Forms/Notice_Of_Privacy_Practice.pdf
  - Use and disclose only the minimum necessary patient information to do your job

For Verbal Information

- Ensure conversations of a sensitive nature are conducted in an appropriate environment (e.g., not in a public waiting area, elevator or shuttle)
- When leaving a voicemail, leave a generic message requesting the patient to contact you for further discussion; do not leave details unless you have the patient’s authorization to do so

For Hard Copy Information

- You should not take PHI off the premises. If you do, you are responsible for securing the records from unauthorized access (e.g., do not leave it unattended in your car, bag, home, public transportation, etc.). Keep it secured and on you at all times.
- 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
- When faxing documents, verify the fax number and recipient is correct before sending documents. Remember: You are responsible if the document is faxed to the wrong person

For Electronic Information

- ePHI should only be stored on a secure server, share point or system; consult with IT Security if you are unsure whether a system is secure
- If you access or store ePHI on an electronic device (e.g., laptop, tablet, mobile phone, external hard drive or USB flash drive) or if you use a mobile device to access ePHI via UCSF email, the device must be encrypted
- You are individually responsible for properly securing PHI
- 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

Email

- When sending ePHI to any email address, use your UCSF account and secure the email by typing one of the following in the subject line: “SECURE:” or “ePHI:” or “PHI:"

- A secure (encrypted) 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

- Never respond to any correspondence asking for your personal user ID, password, SSN or other personal information. These may be phishing scams and can compromise your email account, computer and network.

Photography

- Photography is allowed for treatment or safety purposes
- All other photography requires patient consent
- 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