WHAT IS THE PRIVACY OFFICE?

The Privacy Office is responsible for monitoring compliance with the federal and state privacy laws and regulations. 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.
UCSF PRIVACY AND SECURITY SURVIVAL TIPS

Protecting the privacy and confidentiality of patient’s health information is a fundamental ethical concept and standard in health care. However, in today’s health care environment of digital media, electronic data and new forms of social media communications, always knowing the best way to protect data using the new technology can be a challenge. Additionally, in light of increased Federal Privacy and Security regulations and State laws, it is imperative that as members of the healthcare team, you know how to protect the patient information you work with on a daily basis.

KEY CONCEPTS:

- Only use the minimum necessary information to do your job. Never keep information that you do not need.

The access, viewing, use, or disclosure of Protected Health Information (PHI) for any purpose other than Treatment, Payment, Operations (TPO), or as required by law, requires an authorization from the patient.

Failure to protect or prevent a privacy breach may result in civil and criminal liabilities not only to UCSF, but to the individual workforce member as well. These fines can go up to $1.5 million, can include imprisonment up to 10 years, and for licensed professionals, action can be taken against their licenses.

Some Critical Actions To Prevent a Privacy Breach:

1. Make sure conversations of a sensitive nature are conducted in an appropriate environment, not in a public waiting area.

2. When leaving a voice message, make sure you have the patient’s authorization to do so, or leave a generic message requesting the patient to contact your office for further discussion.

3. When faxing documents, verify the fax number and recipient is correct before sending the documents. Remember: You are responsible, if the document is faxed to the wrong location.

4. Management of Email

   - When sending PHI via email, only use a Medical Center, SOM or OAAIS email account and activate secure email by using “ePHI: or PHI: or Secure: ” in the subject line.

   - Never use a personal email account, such as Yahoo, gmail, or hotmail to send PHI.

   - When you delete email or files from your computer, make sure you delete the delete box.

   - Never save emails with attachments in your email account. If the information is needed, move it to a secure server or secure share point.

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

5. I Phones and Blackberries —

   Only use encrypted I phones or encrypted Blackberries. A password does not mean the device is encrypted. If you are not sure if your PDA is encrypted, contact IT support for guidance at the numbers listed below. Until you are sure the PDA is encrypted, do not put PHI on the device.

RESOURCES:

- If you know or suspect a privacy breach, contact the UCSF Privacy Office at 353-2750 ASAP.

- If you have a IT Security concern or question, contact OAAIS at 514-4100 option 2 (campus) or option 1 (Medical Center).

- If an electronic device is lost or stolen, contact the UCPD at 476-1414.