University of California
San Francisco

UCSF MISSION HALL PRIVACY FAQS

Protecting the privacy and confidentiality of patients' health information is a fundamental ethical concept and standard in healthcare. In an Activity-Based Workspace (ABW), always knowing the best way to protect your patients' information (as well as your personal information) can be a challenge. These Frequently Asked Questions (FAQs), developed in conjunction with UCSF faculty, provide best practices for common ABW-related privacy issues. These best practices are consistent with Federal and State privacy regulations. Following these best practices will help you prevent privacy breaches and subsequent consequences for privacy non-compliance.

Note: Should you encounter an issue that raises privacy questions not covered in these FAQs, contact the UCSF Privacy Office at (415) 353-2750.

Securing Hard Copy Documents

1. ***While reviewing medical records in my workspace, I am urgently called to the hospital. What do I need to do with the records on my desk?***

If you need to leave the workspace, put away files containing PHI or other confidential information. If you're in a hurry, turn the documents over so they're not easily viewable to passers-by.

Tip #1: In the event you need to immediately leave your workspace and don't have time to file records away, consider designating a "miscellaneous" spot in your locked cabinet to store files temporarily.

Tip #2: Where possible, access/view the information electronically and avoid handling paper records. When you need to step away from your workstation, lock your screen (e.g., typing Ctrl + Alt + Delete for PCs).

2. ***What constitutes a double-lock at Mission Hall?***

Research records should always be securely stored. Double-lock is a recommended practice, which requires research records to be stored in a locked file room or locked cabinet located in the secured, badge access-protected floor. (The floor badge access lock serves as the first lock.) If you have additional questions about how to store research records, please contact the Committee on Human Research (CHR) at (415) 476-1814.

3. ***I have auditors coming to conduct a multi-day on-site records review and need to secure the records from access to anyone other than the auditors. Can I lock the records in a Huddle Room or Focus Room for the week?***

The Focus and Huddle Rooms can be used for unscheduled, short term use, or for unique situations as determined by each floor. Refer to the Mission Hall ABW page for additional info on the use of these rooms: http://space.ucsf.edu/mission-hall. For this scenario, you may have the auditors use the Focus or Huddle Rooms to conduct their review; however, if the focus rooms do not lock, you should secure the documents in a locked file room at the end of the day. If there are issues with the use of these rooms, contact the appropriate Sandwich Leadership Group.

Protecting Confidentiality of Verbal Discussions

4. ***What should I do when I need to make/receive a call during which PHI or other confidential information will be discussed?***

HIPAA recognizes and permits "incidental disclosures", which are PHI disclosures made incidental to an otherwise permitted disclosure (e.g., treatment purposes). (These include disclosures made within your "neighborhood", which consists of individuals on your ABW floor.) However, you must implement reasonable safeguards to protect the information. Handle this scenario as you would at a nursing station or inpatient unit.

If you need to discuss PHI in an ABW area, use the following safeguards:

- Use professional judgment as to when to take the conversation to the Focus or Huddle Room
- Limit the discussion to the minimum necessary (e.g., don't use patient identifiers in your conversation if unneeded)
- Use a handset or headset to take phone calls (avoid using speakerphone)

5. ***What if a colleague comes by my workspace to discuss a patient case?***

These discussions are related to treatment or educational purposes, and any incidental disclosures are permitted under HIPAA, as long as reasonable safeguards are implemented. Refer to the recommended safeguards above.

6. ***May I put calls on speakerphone in an ABW?***

Out of respect for your neighbors, as well as the privacy and confidentiality of the information being exchanged, conference calls

should be taken via the handset or headset. If you need to jump on a conference call that includes multiple people listening in from one office, use the Focus or Huddle Room (but keep the speaker volume on low). If one isn't available, each person should dial in separately from their respective workspaces.

Security

7. ***I am concerned about people "tailgating" their way onto my floor, which requires a keycard to obtain access. What should I do if I witness such activity?***

   If you see someone without a UCSF badge and/or a keycard trying to gain access to a secured floor, refer them to the security guard on the first floor. If they are unwilling to comply or otherwise seem suspicious, contact UCSF Security at (415) 476-5190. Regardless of whether you're at Mission Bay, Parnassus or Mt Zion, we all need to do our part to report suspicious activity.

8. ***How will FedEx, UPS, or other mail carriers deliver packages?***

   UCSF Security will grant the mail carrier access to the designated floor. The mail carrier will then leave the packages at the reception desk on the designated floor. They will not gain access to the secure area.

Remember: **HIPAA compliance in an ABW is similar to that of a hospital environment. It is important to note that it is one's behavior, not the environment, that needs to be HIPAA compliant. Please follow the HIPAA minimum necessary standard, UCSF Minimum Security Standards (http://tiny.ucsf.edu/mss), and other privacy safeguards outlined in these FAQs.**

IMPORTANT! Encryption Requirements

One of the greatest privacy/security risks to UCSF is the use of unencrypted computing devices (e.g., desktop, laptop, tablet, smartphone, USB drives) for UCSF work purposes. Devices that access, store, or transmit Protected Health Information (PHI), Personally Identifiable Information (PII), or other confidential UCSF information must be encrypted. Failure to do so may result in disciplinary action, civil fines for which you may personally responsible, as well as criminal sanctions.

Below are available resources to encrypt your device:

- **Self-guided encryption installation instructions:** http://tiny.ucsf.edu/9bTkaB
- **Encryption Frequently Asked Questions (FAQs):** http://tiny.ucsf.edu/ZAayfD
- **IT Service Desk:** (415) 514-4100

Privacy and Security Resources

All UCSF workforce are required to complete **HIPAA privacy and security training** upon hire and annually. For refresher training, review the training modules below:

- **HIPAA 101**: http://hipaa.ucsf.edu/education/downloads/HIPAA101Training.pdf
- **Advanced HIPAA Healthcare Provider**: http://hipaa.ucsf.edu/education/downloads/ProviderModule.pdf
- Or visit the UC Learning Center and search by "privacy" to access the privacy online training modules

Review the **UCSF Privacy and Confidentiality Handbook**, which provides a general introduction to the federal and state privacy and security laws, as well as University privacy and security policies: http://hipaa.ucsf.edu/Privacy_Handbook.pdf

Review the **Committee on Human Research (CHR)** website for questions regarding research HIPAA authorizations, waiver of authorization, informed consent, research records, and other research-related issues: http://www.research.ucsf.edu/chr/index.asp

IT Security would also like to remind you to always practice safe computing: encrypting and physically securing all of your devices, locking your workstation whenever you are away, and using strong passwords. To find out more about securing your information and the many free IT Security services available to you, visit our website: http://security.ucsf.edu

Key Contact Info

- **UCSF Privacy Office**
  (415) 353-2750 | http://hipaa.ucsf.edu
- **UCSF Risk Management and Insurance Services**
  (415) 476-2498 | http://rmis.ucsf.edu/
- **UCSF Police**
  (415) 476-1414 | http://www.police.ucsf.edu
- **UCSF Committee on Human Research (CHR)**
  (415) 476-1814 | http://www.research.ucsf.edu/chr
- **UCSF Mission Hall Security**
  (415) 476-5190
- **UCSF IT Security**
  (415) 514-4100 | http://security.ucsf.edu