University of California San Francisco

UCSF PRIVACY BEAT—2015 Training Edition

MAINTAINING APPROPRIATE ACCESS

As a UCSF workforce member, you have agreed to only access, use, and disclose patient information in an appropriate manner. This includes:

- Accessing patient information only to complete your UCSF job duties;
- Accessing only the minimum required information needed to complete the job at hand;
- Not sharing patient information with those who don't have a legitimate business need for it;
- Never share your login credentials, or let others access patient information via your login (you'll be accountable for all access using your login credentials); and
- Report any suspected unauthorized activity immediately to your supervisor and/or the Privacy Office.

In line with UCSF's commitment to patient privacy and confidentiality, UCSF has always monitored our ePHI applications for inappropriate access. As part of this effort, in May 2015, UCSF launched an enhanced EHR access auditing and monitoring program which utilizes APeX access audit logs, user information, and advanced data analytics tools to track and identify potential inappropriate access to UCSF patients' electronic medical records. Access to patient records is evaluated for appropriateness, in accordance with existing UCSF policies and procedures, as well as federal and state laws and regulations.

If inappropriate access, use, or disclosure of confidential information is confirmed, the Privacy Office will ensure quick action is taken in accordance with UCSF Policy 200-32, *Workforce Sanctions for Patient Privacy Violations*, as well as other applicable University policies and collective bargaining agreements. Unauthorized access, use, and/or disclosure is strictly prohibited and may result in disciplinary and corrective actions up to and including termination, suspension of privileges, and loss of medical or professional licensure. Some violations may also expose involved workforce members to personal liability and/or criminal sanctions.

KEEPING HARD COPY INFORMATION SAFE

Paper documents have the potential to cause a breach just as easily as electronic records. Paper can easily be lost or misplaced and, if this happens outside of UCSF's premises, it will likely result in a breach. Paper stored in a bag or in a car is often stolen alongside items typically considered more valuable. Therefore, UCSF encourages you to limit your use of paper documents as much as possible. Rather than printing out information on a piece of paper consider the following alternatives:

- Login to UCSF systems with an encrypted computer using a VPN connection;
- Securely email documents to yourself using your UCSF email and then access it on an encrypted computer; or
- Save files to an encrypted device.

If you must use paper be sure to follow these security precautions:

- De-identify the information as much as possible;
- Secure and keep the documents on your body AT ALL TIMES—do not leave documents in unattended bags or in the your car; and
- Destroy the documents as soon as they are no longer needed—be sure to shred them, not throw them away.

Theft and loss of documents has been the source of a number of breaches so it is important that everyone be vigilant in limiting the amount of information they store on paper.

TECHNOLOGY SECURITY

According to recent reports, medical information is now worth ten times more than credit cards and social security numbers. This is because, unlike other types of information, medical information is both permanent and very detailed. This allows a person who obtains medical information to continue to use it to impersonate the individual accurately and for a long time. As evidenced by the recent incident at UCLA , the value of medical information means that institutions like UCSF are increasingly targets for hackers and thieves. In light of this, below is information about how to properly protect yourself, UCSF, and your electronic devices.

Encryption

Encryption is the only federally recognized way to secure electronic information. Therefore, the only way to prevent breaches stemming from theft of computers is to make sure that all electronic devices that are used for "UCSF business" are ENCRYPTED. "UCSF business" is a broad definition which includes

- Storing PHI or any other personally identifiable information about UCSF patients, workforce members, or research participants;
- Checking your email or maintaining your schedule; and
- Writing articles based on UCSF patient or research participant data.

(*Continued on Page 2)*

Inside this issue:

UCSF Privacy Office
3333 California Street,
Suite S1-10G
San Francisco, CA 94118
Box 1922

Phone: (415) 353-2750
Fax: (415) 353-9241
Email:Privacy@ucsf.edu
http://hipaa.ucsf.edu

CLOUD STORAGE

While cloud storage companies like Dropbox and GoogleDrive may be convenient for your personal use, **cloud storage should not be used for personally identifiable information.** These companies' servers are often not encrypted and are not guaranteed to comply with other minimum security standards, which opens up UCSF data to security risks

Additionally, based on the companies' standard contractual terms, the companies have limited obligation to resolving their users' issues. This means that if anything should happen with a document involving UCSF information, the company will likely not be required to work with UCSF to resolve the issue or retrieve the information.

This is an area to which federal oversight agencies are paying particular attention. Just last month (July 2015), a hospital was fined $218,000 for a privacy breach after their employees inappropriately stored PHI on a cloud provider.

The only cloud provider that UCSF has a contract with—and therefore may be used for UCSF work product— is Box. However, even then, as **Box is not HIPAA compliant it, cannot be used for PHI**.

Students: as part of your academic program you automatically get a free 60GB Box account. Box allows you to store files on the cloud, sync files across devices, and collaborate with people both inside and outside of UCSF. You can also set permission levels to control who can view/edit files and retain version control so that versions are not overwritten upon each other. However, **Box should not be used to store any PII, PHI, or FERPA data**, or any personal materials.

Researchers: if you need cloud storage to conduct research you can use the MyResearch function in the Integrated Data Repository (IDR). For more information visit http://myresearch.ucsf.edu/research or email ARSmyresearchsupport@ucsf.edu

PATIENT HIPAA RIGHTS

HIPAA provides patients with a number of rights with regard to their medical information. These rights are:

1. Right to receive a Notice of Privacy Practices (NPP);
2. Right to inspect and obtain a copy of the health information that UCSF maintains about them;
3. Right to request an amendment to their medical record;
4. Right to an accounting of disclosures of their health information;
5. Right to request a restriction on the use and disclosure of their health information; and
6. Right to request a restriction on the method by which UCSF communicates with them.

With the increased attention on privacy, both patients and regulatory agencies are becoming more active in exercising and enforcing these rights. Failing to adequately provide patients with these rights can result in enforcement action and potential litigation.

Impact on you: UCSF has built processes to ensure patients' rights are honored, and established procedures by which patient complaints are handled. If a patient asks you to take any action other than to provide them with a copy of the NPP DO NOT commit UCSF to anything and do not ignore request. Rather, refer them to the Patient Relations department. Contact patient relations at patient.relations@ucsf.edu or by phone at (415) 353-1936.

TECHNOLOGY SECURITY (continued from Page 1)

"Electronic device" is also a broad term. It encompasses all devices such as:

- Laptops
- Desktops
- Smart phones
- Flash Drives
- External Hard Drives

This means that any of the above devices, if used for any "UCSF business", must be encrypted. This requirement is reflected in UCSF policy as well as the newest UCSF Confidentiality Statement.

Phishing

In addition to encrypting electronic devices, it is important that all UCFS workforce members remain vigilant when clicking on links both on the internet and especially in emails that you receive. Hackers are increasingly using "phishing" emails to gain access to computer networks. Computers connected to a network that contains a lot of information—such as UCSF's—are particularly attractive targets. These emails are designed to look just like legitimate emails—they may look like they are from someone you email with and have a subject line similar to the type of emails you receive. To avoid falling victim to a phishing attack follow these tips:

- Do not click on links embedded in emails from recipients you do not trust;
- Do not open attachments or download files from emails you are not positive are legitimate; and
- Do not reply to emails that ask you to send them personal information such as username and passwords.

For more information visit: http://tiny.ucsf.edu/phishing.

Hacking

Aside from phishing attacks, hackers are also increasingly using viruses and other malicious software to gain access to networks. UCSF's IT-Security department regularly pushes out updates to UCSF computers in order to protect UCSF to ever-changing threats. It is important that you do not try to block these updates and restart your computer when asked. Additionally, if you use a personal device for UCSF business you must be sure to keep your anti-virus and other security protections up-to-date at all times.

PREVENTING MISDIRECTED DOCUMENTS

While not leading to as many headlines as larger breaches, incidents involving misdirected documents and information are a large problem for every medical institution. These incidents come in various forms: mishanded documents, missent faxes, misdirected emails, and mismailed letters. All of them have the potential to create a privacy breach. This is especially true in California, which has what is widely considered to be the strictest privacy laws in the nation.

These incidents are especially problematic because they are often not discovered until long after the underlying cause occurs. For instance, when an incorrect provider is chosen in a patient's CareTeam, the provider will begin to automatically receive updates about the patient's care. However, the first update will not occur until the patient's next encounter with UCSF, which could be many months later. Resolving the incident then requires tracing back and untangling actions taken by UCSF staff at the time the provider was chosen, which is not an easy task. Since the department where the error originally occurred is held responsible for the incident — and is tasked with resolving it — it is in everyone's best interest that these incidents not occur in the first place.

Many of these incidents arise out of a momentary lapse in attention or failure to fully check the identity of the recipient. To guard against this, every UCSF workforce member should be using **two factor identification** when handing or mailing patients documents and when entering provider information into APeX.

Two factor identification means checking both the **name and at least one other identifier** of the recipient. So, when entering a provider into the patient's CareTeam, you should confirm with the patient the provider's name *and* street address.

This also applies to choosing a patient's guarantor. There are multiple guarantors with the same name so in addition to checking first and last name, you should verify the guarantor's address.

Similarly, when handing patients documents, or mailing documents to them, you should carefully check **every page** that you are handing them to check that another patient's records did not get mixed up in the stack. Often people will print out multiple patients' documents at once and think that they have separated them correctly but miss a page or two.

Finally, since it is easy to forget to logout of one patient's chart before moving onto the next one, before charting your notes for a particular patient, you should always make sure that you are in the correct medical record.

SECURE EMAILING

As part of its effort to protect electronic information, UCSF has a secure emailing system that allows users to encrypt emails when they leave UCSF's servers. The system does not affect emails while they are sent to other @ucsf.edu emails. However, if a secure email is sent or forwarded to a non-@ucsf.edu address, the outside recipient receives a notification that there is an email waiting for them on a secure server. The recipient then has to log into the secure server to access the email.

While this system will not prevent an incorrect recipient from viewing the email, it does create an extra step for them to take in order to open the email, and also creates an opportunity for the sender to recognize the mistake and retrieve the email before it is opened.

To enable this system, a user must enter one of three terms into the beginning of the email's subject line:

- Secure:
- PHI:
- ePHI:

It is important that you use one of those terms **followed by a colon**. Once one of these terms is included into the beginning of the subject line, the email will remain secure regardless of whether the email is replied to or forwarded.

If you send a secure email to someone who should not have received it (and realize that you have done so) you can recall the email from the server until the time recipient retrieves it. To do this open the sent email and click on the "Resend or Recall" button in the email's "File" menu.

VERBAL DISCLOSURES

Communicating with, and about, patients is an important part of health care. And working in a busy and crowded medical center will necessarily involve discussing patient care in areas where the people having the conversation are not the only ones present. However, when working in this environment, it is important to take **appropriate precautions to maintain patient privacy**. These include, using the **minimum necessary** information during the course of the conversation, **limiting the conversations to non-public areas**, and speaking at an appropriate volume.

If you must have a conversation with a patient in a shared room, close the curtain around their bed and try to offer the other patients ear plugs—this will make both the patient you are talking to and the other people more comfortable.

Phone Calls: When calling patients on the phone be sure to verify the identity of the person on the other line before revealing any information about the patient. Also, do not call patients using the speakerphone unless you are in a private area where no one else can overhear the call.

Voicemails: Do not leave any PHI on a patient's voicemail — you do not know who will be the one checking the message. Instead leave a message that identifies yourself, that you are calling from UCSF (do not state the department), your phone number, and ask the patient to call you back.

PHYSICAL SECURITY

Theft is increasingly becoming a problem at UCSF, and in San Francisco as a whole. In the last few years San Francisco has seen a 20% rise in property crime, and the first two months of this year saw almost a 50% increase in car break-ins compared to the same period last year. This means that you must always be aware of your surroundings and must physically secure documents, devices, and UCSF facilities. To do this take the following steps:

- Lock all doors
- Secure computers to desks
- Lock all cabinets and desk drawers
- Use screen savers and screen timeouts
- Shred paper documents
- Do not leave PHI laying around in public spaces
- De-identify IV bags, vials, and other materials before throwing them away
- Report suspicious visitors

RESEARCH PRIVACY

UCSF workforce members who conduct research have to focus on some additional privacy requirements.

Study Application: Address privacy issues in your CHR study application. Think through how you will maintain participant's confidentiality throughout the study.

Recruitment: Researchers should not go into APeX for recruitment purposes without a Waiver of Authorization for recruitment. You must obtain this waiver prior to recruitment activities. Once you have the waiver, a good way to find participants is by requesting a report from the Clarity database. To do this contact Sayan Chatterjee at sayan.chatterjee@ucsf.edu.

Consent: Prior to using patient information for research, researchers must either get patient authorization in the form of a HIPAA Authorization form or a waiver of authorization from CHR. **Note:** the HIPAA Authorization Form is a document that is separate from the Informed Consent that participants sign. For more information, and to get a copy of the form, visit http://www.research.ucsf.edu/chr/HIPAA/chrHIPAA.asp#UCSF.

Repurposing Data: Data appropriately obtained for one purpose cannot be repurposed for another use without additional, appropriate CHR/privacy board review. This means that information obtained during treatment cannot then be used for research without CHR approval. Similarly, data used for one research study cannot be used in another study without going through the CHR and consent approval process again.

Data Security: Once you start collecting information, you must be sure that it remains secure at all times. As discussed earlier in this newsletter, do not store information on unencrypted devices or in the Cloud. If your research requires collaboration with others you can utilize the MyResearch function. For more information visit http://myresearch.ucsf.edu/myresearch.

Additionally, research pursuant to UCSF CHR approved studies is "UCSF business" for purposes of UCSF's encryption requirements. This means that any electronic device used in the course of research must be encrypted *before* research data is stored on it.

Consequences: Failure to follow privacy requirements during recruitment and collection of data may result in the CHR prohibiting you from using the data for the research. Failure to properly secure data once it is collected could result in a privacy breach, which is punishable by federal, state, and UC penalties.

PHOTOGRAPHY AND VIDEO RECORDING

Prior to taking a picture or video of a patient, research participant, or UCSF workforce member, consent from the target of the recording is required. This means that if you want to take a picture or video of someone on UCSF premises for UCSF purposes, you must acquire appropriate consent from that person. Similarly, if you see a patient taking pictures or recording a video you should stop them and make sure that they have obtained consent from everyone who is going to be in the images.

The Privacy Office has created a tip sheet to help you navigate the consent required for different types of photography. This document can be found on the Privacy Office website or directly at this link: http://tiny.ucsf.edu/dqKH32.

University of California
San Francisco

CAMPUS PRIVACY

UCSF is in the process of rolling out a comprehensive Campus Privacy Program. This program is focused on all student, academic, and financial privacy matters at UCSF. Be on the lookout for more information in the months to come. As an introduction however, below is some basic information that you should be aware of in regards these matters:

FERPA

In addition to the general and health privacy rules, UCSF workforce members who work with student information must also be aware of the regulations surrounding those records. Student information is protected by the Family Educational Rights and Privacy Act of 1974. FERPA provides *students* the right to the following:

- Inspect and review education records;
- Seek amendments of education records; and
- Control the disclosure of education records.

The law defines "education record" broadly as records that:

- Contain information that is directly related to the student; and
- Are maintained by an educational agency or institution or by a party acting for the agency or institution.

The following records are not subject to FERPA :

- Law enforcement records;
- Medical treatment records;
- Employment records;
- Alumni records (records created or received after a student leaves the institution and that are not directly related to their attendance as a student):
- Sole-possession records (records that are solely in possession of their maker and that are used only as a personal memory aid).

It is important that UCSF comply with FERPA for a number of reasons. First, students have the right to have privacy in their student records. Additionally, failure to comply with FERPA can result in a loss of federal funding to UCSF.

As mentioned earlier, the law requires UCSF to provide students with an opportunity to review their education records. As a general rule this extends to all student records other than their parent/ guardian financial information or to confidential letters of recommendation to which they have waived access.

Similarly, students' right to control disclosure means that students personally identifiable information cannot be disclosed to third parties without the student's signed and dated consent. Pursuant to this requirement, student grades cannot be publicly displayed even if students are identified by a student ID (or a partial student ID) number. FERPA does allow records to be shared among university officials who have a legitimate educational interest in the information

Computer Fraud And Abuse Act (CFAA)

The CFAA is a federal law that prohibits "unauthorized access" to electronic devices that are connected to the internet. This means that you should not use UCSF computers in ways that you are not authorized to do in the course of your job at UCSF.

Graham-Leach-Bliley Act (GLBA)

The GLBA is a federal law that applies to "financial institutions." Although it may seem like UCSF is not a financial institution, because UCSF offers loans and other financial services to its students, it does fall under this definition.

As a GLBA covered entity, UCSF is required to inform its "customers" of its privacy policy. And, under the GLBA Safeguards Rule, it must also establish administrative, technical, and physical information safeguards as well as develop a written information privacy program with a designated employee that coordinates the program.

Finally, under the FTC's "Red Flags" rules, UCSF is required to develop and implement a written ID theft prevention program when it functions as a creditor.

Contact the Privacy Office with any questions.

We are happy to offer advice, consult on projects you are working on, or audit your department or workflow.

Contact Information:

Email: privacy@ucsf.edu

Phone: 415-353-2750