University of California San Francisco

Inside this issue:

Reviewing Data Privacy Month: January 28th—February 28th

Data Privacy Month was from January 28 through the end of February. The purpose of Data Privacy Month was to raise awareness of privacy and security issues.

Even though Data Privacy Month "officially" ended last month, we are reminded that every month is an opportunity to bring awareness to best practices for protecting UCSF against adverse privacy and security incidents. This year, our focus is on protecting against phishing attempts and promoting strong password protection. The Privacy Office circulated UCSF Branding-approved posters on the shuttles and shared privacy tips in each of our email signatures.

If you are interested in displaying posters in your department, you may download them from our website under "Data Privacy Awareness Posters" here: http://hipaa.ucsf.edu/workforce-resources-and-guidance.

Upcoming Events

Documentary Screening: *Terms and Conditions May Apply*

The UCSF Privacy Office invites you to a screening of *Terms and Conditions May Apply* (2013). The documentary inspects the language used in user-service agreements on the web. Come learn about how companies like Google, Facebook and LinkedIn utilize information based on these agreements.

Where: Laurel Heights Auditorium, S1 Level
When: Friday, March 16th from 1:30-2:45 P.M.
Cost: Free for UCSF faculty, staff and students

No advance registration required.

Application Security Training 2-Day Workshop

UCSF IT Security and SOM Tech are pleased to announce this year's **Application Security Training 2-Day Workshop** at Mission Bay!

What: Platform and technology agnostic remediation strategies against application security vulnerabilities and hands-on experience with application vulnerability attacks and secure coding.
When: May 14: Full-day lecture for all attendees. May 15–18: Full-day lab workshops (attendees select one day)
Cost: Free for UCSF and UCOP staff and students.
Sign up here: https://applicationsecuritytraining.eventbrite.com/

Vulnerabilities continue to evolve, so we encourage both new and returning attendees to register. The 2-day training will cover the latest OWASP Top 10 2017, with newer vulnerabilities added to the mix such as the XML external entity injection, insecure deserialization, and insufficient logging and monitoring vulnerabilities.

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

Mailing Postcards to Patients and Research Study Participants

The Privacy Office has seen an uptick in privacy incidents related to the mailing of postcards to patients and study participants. We would like to offer some guidance on the minimum necessary standard under HIPAA in relation to contacting patients and participants via mail.

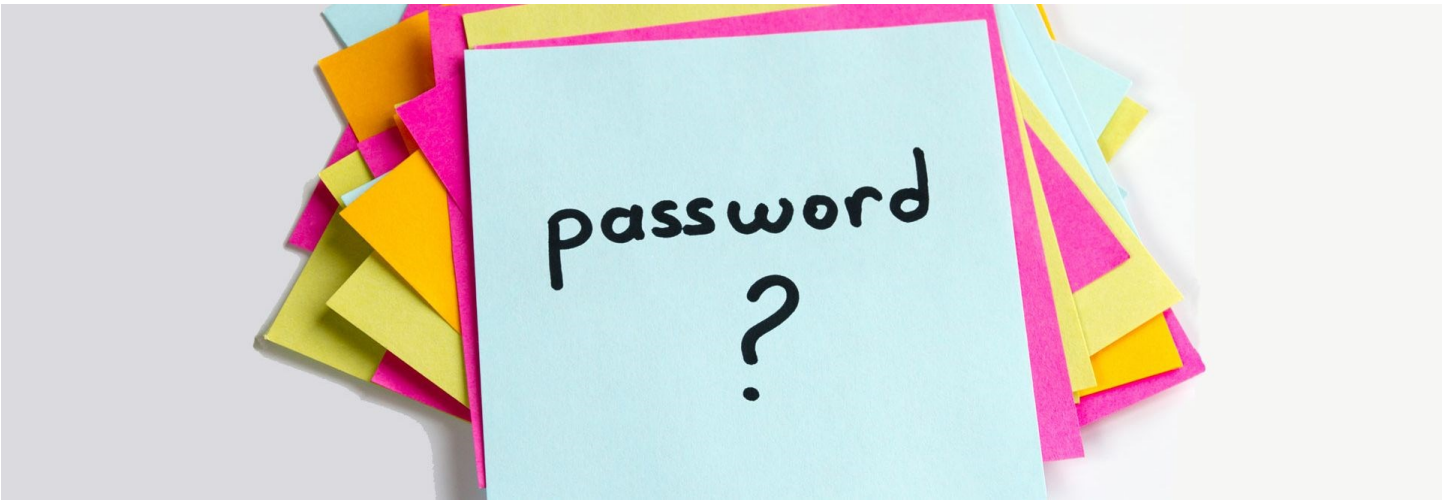
UCSF has many specialty clinics and conducts many studies whose titles inherently reveal potential patient diagnoses. In light of this fact, we recommend the following:

- Review proposed mailings to patients or study participants with your supervisors. Contact the Privacy Office if you have specific concerns.
- Utilize letters mailed in non-windowed envelopes, as opposed to postcards
- Remove clinic names or study titles that contain inherent patient diagnoses or treatment from the return address information on envelopes

Even if a sealed envelope mailing from a descriptive department or study (e.g., Breast Oncology Program or Epilepsy Center) was inadvertently sent to the wrong address, the unintended recipient could infer that the person to whom the mailing is addressed has the diagnosis inherent in the clinic title. More evidently, if the mailing was via postcard, the unintended recipient would see this correlation immediately as there would be nothing to open – the information is not concealed in an envelope. If, however, the patient or research subject is sent a mailing where the return address simply states UCSF and the return address, the risk of a breach of patient privacy is greatly reduced.

Although the overall cost of using letters in sealed envelopes is higher, the cost may be less than fines or penalties that might be levied by state and federal governments for a privacy breach (which could potentially be in the millions). This practice will help UCSF comply with the minimum necessary standard under HIPAA and reduce privacy incidents arising from the use of mailings to communicate with patients.

When Sharing *Isn't* Caring: Being Accountable for Your Login Credentials



In the era of electronic health records, credential sharing is a problem facing many healthcare facilities. Sharing your UCSF login credentials is a violation of UCSF policy. It is also a risk to patient/participant data, could expose UCSF to costly fines and reputational harm, and could potentially expose you to personal liability.

HIPAA Security Rule

The HIPAA Security Rule requires UCSF to assign a unique name or number to identify and track a workforce member's account identity. This enables UCSF to hold users accountable for actions performed in a system with electronic PHI (ePHI).

An audit can be generated for any UCSF employee who can access, view, or edit the electronic health record. Thus, if necessary, UCSF can review logs to determine which workforce member accessed a particular patient's record.

Unfortunately, sharing passwords makes it almost impossible to separate one person's access from another. The following example illustrates this difficulty.

A patient comes into a clinic to check in for her appointment. At the front desk, Susan is on the phone with another patient, so she shares her APeX credentials with Bob so that he can complete patient check-in. ***Continued on Page 3.***

When Sharing *Isn't* Caring (continued from Page 2)

Bob makes a mistake during check-in. However, based on the audit log, Susan is listed as having accessed this patient's medical record and would be accountable for any action taken under her log-in credentials.

If Susan did not share her credentials with Bob, Bob's access (and error) would have been logged under his own account and not Susan's, and Susan would not have been on the hook for Bob's error.

What You Can Do

IT Security has developed best practices to reinforce the importance of credential security and to prevent inadvertent credential sharing.

- Don't write down your password or make your password easily accessible for others to view
- Choose a good password that is difficult for other people or bots to guess, and is easy for you to remember
- Properly log out of your accounts
- Never share your password, and never let others watch while you type your password
- Regularly change your password. Never reuse the same one!

For more information, please visit: https://it.ucsf.edu/policies/keep-your-accounts-secure; https://it.ucsf.edu/policies/choose-right-password.

If you have any questions about credential login or security, or if you suspect unusual access to your UCSF accounts, contact IT Security at (415) 514-4100 or ITServiceDesk@ucsf.edu.

Test Your Privacy Knowledge— Complete the Quiz

Congratulations to the winner of our Fall 2017 Privacy Quiz, **Charlie Toohey** of the **UCSF Memory and Aging Center**. We hope you enjoy your gift card!

Test your privacy knowledge! For your chance to win a $10 Amazon gift card, submit your answer to the question below to privacy@ucsf.edu and include "Privacy Quiz – Winter 2018" in the email subject line. One lucky winner will be chosen out of the correct responses to receive a gift card.

Before your team meeting, you walk into a conference room and notice that several consult notes with patient information are on the table. What should you do? Select the best answer.

A. Throw the documents in the trash.
B. Submit a request for the custodial staff to clean the room.
C. If you can determine who left the documents, return the consult notes to the individual. Otherwise, give the documents to your supervisor or dispose of them in a secure shred bin.