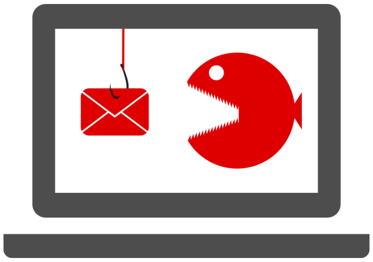
UCSF
University of California
San Francisco

Spotlight Feature: Privacy and Security Pop-Up Event

In January, the Privacy Office teamed up with the School of Medicine Information Services Unit to hold a Privacy and Security Pop-Up event at Mission Hall. The event, attended by a diverse group of individuals representing academic and research, was a success. The discussion covered various topics ranging from de-identified vs. protected health information (hint: it's harder to de-identify than you think!), how to work with cloud storage vendors, and real-life privacy and security pit falls (and how you can protect yourself).

More events are planned for the near future and we'd like to solicit topics of interest. For example, are you interested in human subjects research participant recruitment issues? Or best practices for security personal information? Or strategies when developing or using a mobile app that stores/transmits confidential data? Please let us know! Email som-dsc.program@ucsf.edu.

Phishing Attacks: Don't Get Caught on a Hook!



UCSF has been under sustained attack by hackers attempting to infiltrate our network. You may have noticed regular IT Service Desk Announcements urging caution regarding phishing emails. **Phishing** is an attempt by a hacker to trick a computer user into revealing their passwords, disclosing confidential, personal or financial information, clicking on malicious links, opening harmful attachments, and even sending money. These can happen over the phone, via email, instant message, text message, Facebook, Twitter, or any other communication platform. Hackers have adopted this form of attack because it's easier than trying to directly break into our network. Why scale a barbed wire fence when you can get someone to open the gate and let you in?

According to the FBI's Sacramento office, most breaches they investigated last year began with a **spear phishing intrusion**. This is a sophisticated, targeted phishing attack designed so the message a user receives looks like it came from someone of authority at their business or institution.

The frequency of these attacks is on the rise, so UCSF workforce members must remain vigilant and learn how to defend against them. Here are some easy tips:

- Be suspicious of unknown links and odd-looking attachments in emails, regardless of who appears to be the sender.
- Be aware that phishing attacks can come from virtually any communication platform.
- Never share your password with anyone, including the IT Helpdesk— they will never ask for your password.
- Never provide private information (yours or someone else's) to anyone you don't now or who doesn't have a legitimate business need for that information.
- Read all UCSF IT service desk announcements that mention "Phishing Attempt" to ensure you know what the latest attack looks like and can avoid opening the message.
- If in the course of your workday you receive what looks like a suspicious looking email or you fear you may have opened and clicked on a suspicious message, call the IT Helpdesk (415-514-4100) immediately. Helpdesk personnel will help you limit the impact of the hacking intrusion, but they can only do so if they are informed. Waiting to alert IT can provide the virus or malware the time it needs to replicate and further infiltrate UCSF computer systems.

If you suspect you are the target of a phishing attack it is better to err on the side of caution, so… **when in doubt, throw the message out!**

Kudos Corner: School of Dentistry

The UCSF School of Dentistry (SOD) has been busy getting audit-ready. As you may have heard, the Office for Civil Rights (OCR) is currently conducting HIPAA compliance audits of covered entities (including healthcare providers). In preparation for a potential audit, SOD has a number of proactive efforts underway, including:

- Revising privacy-related policies and procedures
- Assessing physical environments to ensure the Notice of Privacy Practices (NPP) posters are prominently posted in the various clinics, with a supply of NPP brochures immediately available
- Identifying individuals to escort the OCR surveyors (for an on-site audit)
- Ensuring all workforce members have evidence of privacy and security training completion in the UC Learning Center

Big kudos to Mark Kirkland, DDS (Associate Dean, Clinical Affairs) and Leslie McGarvey, DDS (Compliance Liaison) in the School of Dentistry for their hard work. For customized tips to prepare for an OCR audit, please contact the Privacy Office at privacy@ucsf.edu or (415) 353-2750.

Inside this issue:

QUICK TIP

FYI: You are provided access to APeX (or other systems where confidential information is stored) so that you can perform functions necessary to your job. Accessing records when it is not related to your work violates UCSF policy, as well as certain state and federal laws. Your access history may be audited to verify that you are using these systems appropriately.

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

UPDATED: UCSF Social Media Guidelines and Best Practices

Do you ever have questions about whether something is okay to post on social media? Looking for guidance on how to speak to staff members about social media behaviors and how their individual actions may reflect upon UCSF? Look no further. The Office of University Relations and Digital Communications recently updated two key documents: the UCSF Social Media Individual Use Policy (formerly the UCSF Social Media Guidelines) and the Social Media Policies for Branded Accounts (formerly the UCSF Social Media Best Practices).

The updated documents address social media behaviors that breach patient confidentiality, such as:

- Posting verbal "gossip" about a patient to unauthorized individuals, even if the name is not disclosed
- Sharing of photographs, videos or any form of PHI without written consent from a patient
- Sharing of comments or pictures that may happen to have visible patient information in someone's hands, in the background, etc.

In addition to guidance on how to remain compliant with federal and state privacy laws and policies, there are other great tips on how to facilitate meaningful conversation and promote community involvement on social media. For more information, contact University Relations at socialmedia@ucsf.edu.

Handling Fundraising and PHI

UCSF Policy 450-10 requires that all fundraising activities be coordinated through UCSF Development and Alumni Relations (UDAR). Fundraising activities are those that request or include a mechanism for a gift.

- In accordance with the UCSF's Patient Privacy Policy, UDAR determines the PHI (i.e., clinical department, division, or provider) that can be used in identifying patients for a solicitation. When communicating patient information with UDAR, please use ePHI: or Secure: in your email subject line and do not share medical record numbers.
- UDAR also maintains the university's database of patients, friends and donors who have asked not to receive any fundraising communications from UCSF. UDAR must review all lists of contacts who will be asked for a gift in order to identify and remove anyone who has opted-out of solicitations. This review and removal is critical for the university's compliance with HIPAA.
- The development office also ensures that fundraising communications contain the correct and current policy language.
- UDAR can also verify that any 3rd parties who will be handling patient and donor information have been approved and vetted by the university. For example, printers and mail shops that produce patient communications should have completed a Business Associates Agreement and a Data Security Risk Assessment.

For questions about fundraising or to initiate projects with UDAR, please contact your designated development officer or Megan Smith, Senior Director, Annual & Special Giving, at megan.smith@ucsf.edu or (415) 476-9160.

Privacy Tips: Preventing the Major "Misses"

For the first half of FY17, the Privacy Office has noticed an increasing trend in "mis-" type privacy breach incidents: mis-emailed, mis-handed, and mis-mailed documents.

These breaches are often attributed to a combination of factors: a workforce member being in a rush, not paying attention, and/or deviating from best practices. Below are some tips on how to prevent these three common types of breach incidents from occurring.

PRO TIP: Cut out this section of the newsletter and post it somewhere highly visible to the staff who are normally responsible for these tasks!

Prevent Mis-Emailing

- Verify the email address of the intended recipient — ensure that spelling and domain name (i.e., Gmail, Yahoo, etc.) are correct
- If your email account auto-populates email addresses based on your message history, **double-check** the email address for the recipient. Don't allow an email to go out to Mr. Roberts when you meant to send it to *Mr. Robertson*!
- When contacting patients, encourage the use of MyChart to communicate any confidential information
- Before you respond to a group email with any confidential/sensitive information, ensure that each person on the email thread is authorized to receive that information. It's common for people to be added to a long email chain — don't assume that everyone on the thread has a UCSF email address or is permitted to receive any confidential/sensitive information!
- When sending emails that contain confidential/sensitive information, use our secure email system. Include one of the secure triggers — ePHI:, SECURE:, or PHI: in your email subject line. The triggers are not case sensitive, but make sure to insert the colon.

Prevent Mis-Handing

- Review each page of a document before handing it to a patient — highlight multiple patient identifiers such as name, MRN, and/or DOB to ensure that each page belongs to the same patient!
- Staple all highlighted/verified pages of a document together to prevent any pages from coming loose, or from unintentionally mixing another patient's information with the packet
- When retrieving documents from the printer, check to make sure that you are grabbing only your documents and not including someone else's print out

Prevent Mis-Mailing

- Review each page of a document before stuffing it into an envelope for mailing — highlight multiple patient identifiers
- Make sure the address mailing label matches the contact information for the recipient's document(s) inside

Would you like a privacy in-service "refresher" training on any of the above topics for your department? Let us know! Contact Privacy at privacy@ucsf.edu or at (415) 353-2750.