Inside this issue:

2014 Privacy and Security Briefing 1
Anthem Breach 1
UCSF Campus Privacy Program 1
Mission Hall 1
Campus Privacy Program Quiz 2
You May Be a Phishing Target 2
Sharing PHI with Outside Parties 2
Privacy of Ebola Patient 3
Border Firewall Project 3
Encryption Resources 3

2014 Privacy and Security Briefing—Time is Running Out!

With a call-to-action from UCSF Chancellor Sam Hawgood and UCSF Medical Center and Benioff Children’s Hospitals CEO Mark Laret, the online Privacy and Security Training Program launched with a bang in Fall 2014. As a reminder, this training program is critical for UCSF to meet its commitment to protecting confidential information. Completing this training helps ensure we conduct our business effectively and efficiently while protecting the privacy and security of information. This is critical in a world where technology continues to advance, the need to access electronic patient information is ever increasing, and we always feel the need to be “connected.”

Anthem Data Breach

As you may have heard in the news, Anthem, Inc. disclosed on February 5, 2015 that the health insurer was the target of a very sophisticated external cyber attack, and that data for its 80 million members was accessed. UC is in communications with Anthem to understand the effect of this data breach on current and former Anthem members. At this time, Anthem is reporting that their investigation to date shows that no confidential health information was accessed. If you receive questions from current and former Anthem members concerning this breach, you can direct them to Anthem’s dedicated website at: http://www.AnthemFacts.com. Members may also call (877) 263-7995. For guidance relating to phishing attacks, please refer to the phishing article on the next page.

Announcing the New Campus Privacy Program

We are excited to announce the formation of the new Campus Privacy Program. The program, mandated by UCOP, is designed to set policy guidance, educate the UCSF community, and investigate potential incidents related to non-medical and non-research privacy laws and regulations. Unlike the existing UCSF Privacy Program (which is governed by HIPAA and CMIA for the protection of PHI), the Campus Privacy Program will focus on the protection of personally identifiable information (PII) collected from students, donors, alumni, and others.

The Campus Privacy Program will report up through the existing Privacy Compliance Steering Committee. Additionally, a smaller Campus Privacy Subcommittee has been formed to review relevant topics/issues, disseminate information, and become subject matter experts in all relevant laws and regulations, including FERPA, COPPA, CalOPPA, and the First and Fourth Amendments to the U.S. Constitution.

The Campus Privacy Program has been tasked with the following:

- Creating a Campus Privacy Program charter
- Identifying and Reviewing existing policies
- Identifying Data Stewards
- Promotion and use of the UC Privacy Values, Principles and Balancing Process

If you have questions regarding the Campus Privacy Program, please contact Carol Ng-Lee in the UCSF Privacy Office at (415) 353-2750.

Occupants Move Into Mission Hall

As UCSF prepares for the opening of Mission Bay, many departments are moving into the new Mission Hall building. Mission Hall features an Activity-Based Workplace (ABW) environment, wherein faculty and staff will occupy work stations in an open space environment. Knowing the best way to protect confidential information in an ABW setting can be a challenge. To address some of these concerns, the Privacy Office developed a guidance document, “UCSF Mission Hall Privacy Frequently Asked Questions”, which contains ABW privacy best practices consistent with federal and state privacy regulations. To review the FAQs, visit http://tiny.ucsf.edu/MHFAQs.
Why Hackers are “Phishing” for You at Work

Many of us are acutely aware of our ever-present overflowing email inboxes, and are constantly working to lower our unread messages to a manageable number. While doing so, we should also be acutely aware of the phishing attempts masquerading as legitimate emails, which could be lingering among that frustratingly large number of unread messages.

As the general public has become more aware of data theft, hackers have begun using increasingly sophisticated methods to get into our computers. One of these is “spear phishing,” which involves hackers sending you an email that is designed to look legitimate and specifically tailored to contain the type of content you get on a regular basis. The email may look like it came from someone who has recently emailed you and may have logos of companies or departments you often work with. However, when you open the email, click on a link within the email, or download an attachment, the hacker gets access to your computer.

What most of us don’t realize is that our work emails are much more likely to be a target of these types of schemes than our personal accounts. Why? The answer is simple: for hackers, getting access to the computer of a big organization is much more valuable than getting access to your personal computer.

And working at an institution like UCSF means that our work emails are targeted even more than other companies. This is because health records are among the most valuable type of information on the black market. In fact, as multiple news outlets have recently reported, a person’s medical information is more than ten times as valuable to hackers as the same person’s credit card information. An example of a recent phishing attempt at UCSF is below. Notice the impersonated UCSF email address and the instruction to download a mysterious file.

![Image of a phishing email]

Reminder Not to Share PHI with Outside Parties

The Privacy Office would like to remind you that you are NOT permitted to share any other individuals’ PHI or confidential information with anyone including your family, friends, union representative or attorney. Below are some questions and answers regarding common situations:

Q1. What if I am called to an investigatory meeting about the care of one of my patients and I need to explain the medication error that occurred, am I able to make a copy of the patient’s medical record so that I can share it with my representative before the meeting?

A1. No, if you are faced with a situation where you believe that there is a need for you to share PHI with your union representative or attorney as it relates to a disciplinary proceeding then you and your representative need to contact Labor and Employee Relations (LER) to request the particular information. It is not OK for you to simply copy the information or send an email with the information to your representative.

Q2. What if my neighbor has a friend who is a patient at our facility, is it OK for me to access the patient’s record so that I can tell my neighbor about the patient’s condition?

A2. No, you cannot share this PHI. If the neighbor wants to find out information he/she must talk to the patient or the patient’s family him/herself.

Campus Privacy Program Quiz—Win an iTunes Gift Card!

Test your knowledge of the Campus Privacy Program with the following quiz and you could win an iTunes gift card! Just email your quiz answers to UCSFPrivacyOfficeDrawing@gmail.com by March 6, 2015! One lucky winner will be randomly selected from all correct responses.

1. What laws or regulations will the Campus Privacy Program rely on to protect personally identifiable information?
   a. HIPAA and FERPA
   b. FERPA, COPPA, CalOPPA, the First Amendment and the Fourth Amendment
   c. PHI and PII
   d. The First Amendment and HIPAA

2. What is the difference between the existing Medical Center Privacy Program and the new Campus Privacy Program?
   a. The existing UCSF Privacy Program is mandated by UCOP, while the Campus Privacy Program is governed by HIPAA
   b. The existing UCSF Privacy Program aims to protect Personally Identifiable Information (PII), while the Campus Privacy Program aims to protect Protected Health Information (PHI)
   c. The existing UCSF Privacy Program aims to protect Protected Health Information (PHI), while the Campus Privacy Program aims to protect Personally Identifiable Information (PII)
   d. The existing UCSF Privacy Program is mandated by UCOP, while the Campus Privacy Program is not mandated by UCOP

Below are some tips to prevent you from becoming a phishing victim:

1. Be cautious about opening attachments or downloading files from emails
2. Delete random emails that ask you to confirm or divulge your private information
3. Do not reply or click on links in a suspicious message
4. Be wary of telephone numbers listed in emails

Visit http://tiny.ucsf.edu/phishing to learn more about how to protect yourself and UCSF from phishing attempts.

Because of the value of health information, hackers are increasingly targeting people who work in the medical field in these phishing attacks. And with the growth of electronic health records this trend will only grow. In light of this reality, you must be very cautious when opening work emails and report any suspicious messages to the IT Service Desk at (415) 514-4100 immediately.
Protecting the Privacy of a Potential UCSF Ebola Patient

UCSF has been designated a priority hospital for treating patients who are suspected of having Ebola. All UCSF workforce members should be advised that if UCSF provides care for a patient diagnosed with Ebola, the Privacy Office will take all possible steps to ensure that the patient’s privacy is protected.

The media, the community, and the entire world continue to have great interest in patients with Ebola. Thus, if a patient with Ebola is treated at UCSF, numerous media reporters may congregate on-site or nearby. There may also be reports or speculation regarding the condition of the patient. UCSF continues to respect the privacy of all our patients and remains bound by federal (HIPAA) and state (CMIA) privacy compliance rules. So, despite the media attention and coverage, we will be keeping patient information strictly confidential in keeping with our routine practices around protecting our patients’ privacy.

As such, all media inquiries will be handled by UCSF News Services, and not by any individual department that is involved with the patient’s care. Thank you in advance for respecting the privacy of all our patients and their families. As a reminder, regardless of whether there is an Ebola patient in our care, UCSF workforce members should:

- **ONLY ACCESS** patient information to complete employee-specific job duties and for job-related functions
- **ONLY ACCESS** the minimum amount of patient information needed to complete the job at hand
- **NOT DISCUSS ANY** patient information in public areas (cafeteria, restrooms, elevators, etc.). Anything said that can identify a patient is considered protected information.
- **NOT POST ANY** photos or information about patients on any social media site or website (e.g., Facebook, Twitter), even if it appears to be de-identified information
- **REFER** media inquiries to UCSF News Services at (415) 502-NEWS

If a patient with Ebola is seen at UCSF, the hospital will actively monitor access to the patient’s medical record, and will also be monitoring access to any and all records of healthcare providers involved in the patient’s care. Accessing medical records without a legitimate business reason is strictly prohibited and may result in severe consequences, which could include loss of employment, suspension of privileges, or loss of medical professional license.

In the interest of patient privacy, we don’t anticipate sending frequent updates about a UCSF Ebola patient to the UCSF workforce, but we will provide information when necessary. To learn more about Ebola, UCSF safety protocols, and CDC advisories and tools to help address patient questions, please visit the Ebola information site at http://www.ucsf.edu/ebola. For more information about UCSF’s privacy policies and procedures, as well as HIPAA requirements, please visit the Privacy Office website at http://hipaa.ucsf.edu.

The Great Encrypted Thumb Drive Giveaway!

**Breaking News!** As part of IT Security’s effort to ensure everyone at UCSF is properly protecting their confidential data, they will be holding Cyber Security Fairs and giving away encrypted thumb drives as well as other great prizes! Times and locations will be posted on the main UCSF Events Calendar as well as the Information Technology Webpage.

Border Firewall Project

Beginning December 9, 2014, UCSF began the border firewall filtering initiative that focuses on preventing unwanted internet traffic from reaching UCSF systems. Unwanted traffic may, among other things, contain malicious software meant to compromise UCSF and its employees private information. Outbound traffic and internal UCSF traffic is not affected. Many types of traffic are already filtered; this effort aims to expand the filtering to all types of traffic. Filtering will be implemented in phases over the next eight months.

In each phase of the project, detailed communications, including the simple exception process, website, and dates, will be sent to two lists, IT-Forum and Security-Update. People with payroll titles that include “Programmer/Analyst” or “Computer Resource” will automatically receive those communications. If you, your lab technicians, or other non-IT personnel manage servers, please subscribe to IT-Forum and/or Security-Update (http://listsrv.ucsf.edu).

For more information about the project, please go to https://secureborder.ucsf.edu (please note that this website is only accessible from the UCSF network or over VPN). There is an informative video as well as other pertinent information.

How Do I Encrypt My Personal Device?

As a reminder, UCSF has resources available to assist you with encrypting your personal devices:

- **Personal laptop/desktop**—Installation guidelines: http://tiny.ucsf.edu/9bTkab
- **Smartphone**—Enabling ActiveSync for UCSF email: http://tiny.ucsf.edu/QweBYV
- **Encryption frequently asked questions (FAQs):** http://tiny.ucsf.edu/2AayFD

If you have encryption-related questions, contact the UCSF IT Service Desk at (415) 514-4100. **Remember:** Encryption protects patients, UCSF, and you.