UCSF
University of California
San Francisco

Inside this issue:

UCSF Box Enhancement for Storing PHI and Other Restricted Data

Great news! You may now use Box to store PHI and other restricted information!

UCSF has added new features to UCSF Box which will allow you to use Box for files containing PHI or other restricted data, when collaborating within UCSF. This new version of Box is called Secure Box and it went live across the organization on October 3, 2016.

To create this new Secure Box, UCSF integrated an application called CipherCloud into UCSF Box. CipherCloud encrypts files that contain UCSF PHI, and the file remains encrypted even if you download it onto your computer.

There are two parts to Secure Box:

1. **Secure folders**: Each user will have a secure folder in their Box account, where they can proactively place files that contain restricted data. Every file in the secure folder is encrypted by CipherCloud, and will need to be decrypted with the CipherCloud agent. UCSF is pushing the CipherCloud agent to all UCSF IT-managed computers, and you can also download it from software.ucsf.edu as well as the Apple App Store for iOS and the Google Play Store for Android. Note that you will not be able to preview these files in Box, nor will you be able to share these files with anyone outside of UCSF.
2. **Scanning**: CipherCloud monitors for changes to files in the rest of your Box account, and scans them for UCSF PHI. If a file contains UCSF PHI, CipherCloud will encrypt it and place a PDF marker file in the same folder. This PDF file explains which file was encrypted, how to access the file, and notes that external collaborators can no longer view it. You will need to have the CipherCloud agent – which is only available to UCSF users – to open these files.

Please remember that UCSF Box is for UCSF business only. To find out more details about the Secure Box project please visit the Secure Box website at http://tiny.ucsf.edu/securebox.

If you have any questions about Secure Box, you may contact the following:

- Support questions: IT Service Desk at (415) 514-4100
- General questions about Box use: Erik Wieland or Jill Cozen-Harel

Spotlight Feature: UCSF Compliance Week

In case you missed it, UCSF held its first Compliance Week Panel Discussion featuring UCSF leaders discussing the current state of UCSF's Culture of Compliance on October 24, 2016! The panel included Lieutenant Kevin McNiff (UC Police Department), Robert Fries (Chief Financial Officer, Benioff Children's Hospital Oakland), Patrick Phelan (Information Security Officer), Terri O'Lonergan (Associate Vice Chancellor, Chief Ethics & Compliance Officer), Christopher Ryan (Director, Human Research Protection Program), Dan Lowenstein (Executive Vice Chancellor and Provost), David Lane (UC Systemwide Deputy Compliance Officer) and Susan Penney (Director, Risk Management). Each panelist shared their perspectives on what compliance means to them. You may access the recording of the panel discussion here: http://tiny.ucsf.edu/2016complianceweekpaneldiscussion.

Kudos Corner : One Year Breach-Free!

On Friday, September 23, 2016, the **Orthopaedic Institute** (clinics, periop, and pediatrics) celebrated the incredible achievement of operating one full year without a single reportable privacy breach. The celebration featured a social lunch catered by a local food truck.

Please join us in congratulating the Orthopaedic Institute for all their efforts in securing patient privacy and remaining breach-free!

Is your department a Privacy All-Star? Do you have any great tips to share about promoting best practices around information privacy? Tell us — we'd love to hear from you so we can feature you in our next **Kudos Corner**! *Email* **Bianca Paraguya** at the Privacy Office *with details*.

Pictured above: Orthopaedic Institute staff, providers, and interns assembled for the celebratory lunch.

SPOTLIGHT

UCSF Compliance Week

There is still time to join the celebration. Join us at the Compliance Week Fair on Thursday, October 27th at the Parnassus Millberry Union, City Lights Room from 11:30am - 1:30pm. For more information visit the UCSF Events Calendar.

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

UCSF Health Achieving Zero Harm

The success realized by the Orthopaedic Institute is aligned with UCSF Health's organizational goal to achieve zero harm. As prescribed by the goal to Achieve Zero Harm, providers and staff will collectively decrease the total number of events that cause harm to patients (including reportable privacy breaches). As demonstrated by the Orthopaedic Institute, we know that achieving zero reportable privacy breaches is possible, but requires significant dedication and diligence. Below are some tips that you can implement to prevent privacy breaches in your departments/units:

- Internally publicize the number of days without a privacy breach, so that the goal remains on everyone's radar
- Do not interrupt a co-worker that is sending or providing PHI
- Do not multi-task when sending or providing PHI
- Carefully verify each document handed, mailed and/or faxed to patients, family members, and third parties using two patient identifiers (e.g., patient first and last name, date of birth or medical record number)
    - Highlight the patient's name and DOB on each page of the multi-page document and staple the document together when mailing or handing to patients
    - Confirm the patient's name on a mailing envelope matches the documents you are inserting into the envelope; confirm the address matches the name on the envelope
    - When removing documents containing PHI from the printer or fax machine, **CHECK EACH PAGE**. Do not assume they are all for the same patient. Separate documents from the printer/fax machine carefully.
- When registering and/or checking in patients in APeX, verify the patient's PCP and/or referring provider using at least **TWO** identifiers. Acceptable provider identifiers include:
    - Full name (first and last)
    - Full address (street address, city, state, zip code)
    - Medical or surgical specialty

If you have any questions, ask your supervisor or contact the UCSF Privacy Office at (415) 353-2750. Thank you for your partnership in preventing privacy breaches across UCSF!

Traveling Overseas with Your Laptop

Republished with permission by Owen Buckvar, IT Security

The minimum security standards still apply when traveling overseas to a foreign nation. All laptops carrying confidential UCSF information including PHI must be encrypted before undertaking any trip whether for business or pleasure.

The core Information Security advice for UCSF students, faculty, and personnel traveling is:

- Ensure the laptop is encrypted. Dell Data Protection Encryption (DDPE) is our standard encryption solution and is free to UCSF personnel. Available at: http://software.ucsf.edu.
- Make a backup of your data before you leave the country, and leave that backup in the U.S.
- Be aware of your surroundings, and do not leave a laptop unattended. (Travelers are often targeted, and we have had several cases where laptops have been stolen while away on business.)
- Visit the UCSF Risk Management Travel Safety site (http://rmis.ucsf.edu) for available services when traveling abroad.

Laptops and mobile devices are not usually subject to export controls if you are using it as part of your work, but if you have sophisticated or specialized software, you may require a license to travel with it. Academic and scientific staff may take their laptops or other Internet connected electronic devices (containing confidential UCSF information including PHI) with them overseas without needing a license as long as all of the following conditions are met:

- Laptop is used for activities related to your university work of teaching and research
- Laptop must remain in your physical possession and may not be lent to or used by foreign persons
- Encryption commodities and software must be pre-loaded on the laptop (however, not all encryption software may be temporarily exported, so if you have some high-powered or unusual encryption software that you use in your work, contact exportcontrol@ucsf.edu to make sure that such encryption software is eligible for the temporary/tools of trade exception)
- The laptop may accompany you or be shipped no more than one month in advance of your departure and must be returned as soon as possible but no later than one year after export
- This exception to a license requirement may **not** be used for travel to Cuba or Sudan

* This exception can also cover other types of equipment used to support university sponsored research or educational activities conducted abroad and is not limited to laptops. If you are traveling abroad to conduct research and need equipment shipped from the U.S. to the foreign country, consult with your campus office responsible for export compliance because the exception may extend to all the equipment and supplies that will be used in the research.

Business Associate Listing: OCR Audits, Phase 2

As you may recall from prior newsletters, the Office for Civil Rights (OCR) is conducting audits of randomly selected Covered Entities. While UCSF has NOT been selected for an audit at this time, we know what OCR plans to request and review during their audits. Selected auditees will be requested to identify and provide detailed information regarding their Business Associates. The information is being collected by OCR and will be used to identify Business Associates for these audits, as OCR plans to audit Business Associates as well.

In preparation, the Privacy Office has worked with Medical Center Procurement to achieve the following:

- Produce a list of all the existing Business Associates stored in their contract repository in the preferred format.
- For all new Business Associate Agreements (BAAs), a cover sheet with required fields will accompany any submission of new BAAs so we have the required fields populated in the future and will be in compliance with the OCR requirements.

All contracting staff (Medical Center and Campus), please forward all fully executed BAAs to Senami Randolph in Medical Center Procurement (Senami.Randolph@ucsf.edu).