University of California San Francisco

Inside this issue:

Spotlight: Duo Authentication	1
Kudos Corner	2
Honest Mistake = Huge Breach: Aetna Mailer Snafu	2
Featured Comic: "Gone Phishing"	2
Featured in the Privacy Toolkit: The Research Data Browser (RDB)	3
Test Your Privacy Knowledge—Quiz! Enter to Win a $25 Amazon Gift Card	3

Spotlight: Duo Authentication

Over the past few months, UCSF has experienced a significant increase in the volume of phishing attacks. These attacks could compromise the privacy and security of UCSF's information systems, thus potentially compromising confidential information pertaining to UCSF patients, students, workforce, research participants and business matters. In response, UCSF IT is implementing Duo two-factor authentication on December 5, 2017. To ensure no delays in your access to UCSF systems, please complete your Duo enrollment as soon as possible. Additional details and instructions are described in the November 20, 2017 announcement sent by UCSF's Chief Information Officer, Joe Bengfort:

Dear Members of the UCSF Community,

Beginning today and continuing over the next year, UCSF IT is rolling out a set of initiatives to improve the cybersecurity of UCSF's data, networks, and computer systems. These actions are in direct response to increasing global threats to UCSF systems, including a dramatic rise in phishing attacks. We are taking these steps not only to protect our data and IT systems but also to protect you from the negative consequences of being a part of a data breach.

Preventing credential theft through phishing has become urgent, requiring UCSF to take immediate action. To this end, we are implementing ***Duo two-factor authentication.*** *You are probably already using some form of two-factor authentication to protect your Gmail, Apple, and banking accounts. Duo is an app that prevents unauthorized access by asking you to approve logins.*

What this means for you: *If you use VPN or Outlook Web Access (http://email.ucsf.edu) from your home or anywhere outside of the UCSF network, you will be getting an email titled "Duo Security Enrollment" from "no-reply@duosecurity.com" with a unique link to complete your enrollment.* ***Please complete your enrollment by Dec 5th for VPN users and Dec 12th for remote Outlook Web Access users.*** *You will not need to use Duo while using Outlook Web Access on the UCSF network.*

To learn more about this and other cybersecurity initiatives, please visit the UCSF IT Security website frequently. Many of the security improvements are being made behind the scenes by our talented IT team and will not be visible to you as an end user, for example the recent rollout of a new layer of email protection that blocks many sophisticated attacks.

Also, to promote your awareness of and participation in these IT security changes, UCSF IT is launching a communications campaign with emails, newsletters, posters, town halls, and in-person support sessions throughout winter 2017-2018. As we move forward, we aim to provide transparent and direct communication so you know exactly what action to take and why, with the goal of creating a more secure IT environment.

As always, UCSF IT Service Desk is here to help. Contact us at 415-514-4100 or visit one of the IT Health Desks for in-person support.

We appreciate your efforts to help keep our environment safe.

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

Kudos Corner

The Privacy Office would like to recognize Sherry Chung, Supervisor from Neurointerventional Radiology for being a Privacy Advocate by ensuring that sensitive information was released in accordance with UCSF policy. We laud Sherry on all her efforts to ensure that correct procedures are followed in her area and protecting patient rights.

Remember – Before sharing or releasing PHI outside of UCSF for reasons other than the common "treatment, payment or operations" exceptions, check with your manager or the Privacy Office that you have the correct agreements and IT Security protections in place, when applicable.

Do you know of a Privacy Advocate that should be recognized? Let us know! Email Bianca Paraguya at bianca.paraguya@ucsf.edu to nominate someone.

Honest Mistake = Huge Breach: Aetna Mailer Snafu

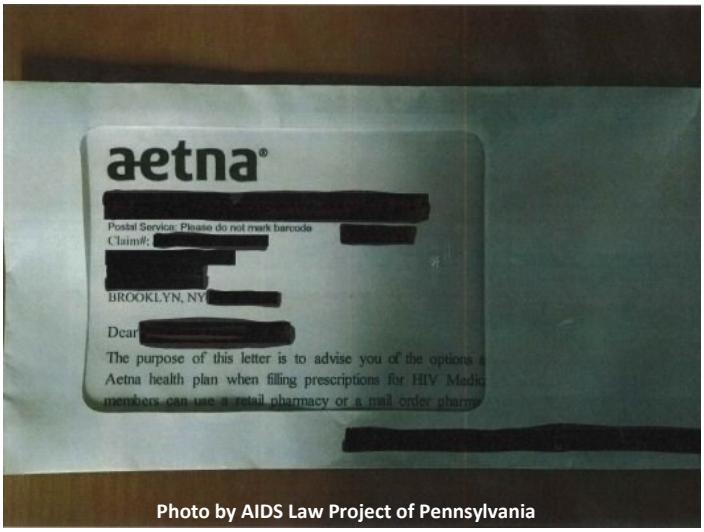


Photo by AIDS Law Project of Pennsylvania

Health insurer Aetna is facing strong criticism and a class action lawsuit for a privacy breach that potentially revealed the HIV status of thousands of its customers via letters meant to communicate the company's HIV medication ordering procedure.

On July 28, 2017, approximately 12,000 Aetna customers across the U.S. received a mailer inside a windowed envelope. Along with the recipients' address information, and clearly visible within the window, were the opening lines of the letter which stated, "*The purpose of this letter is to advise you of the options… [with] Aetna health plan when filling prescriptions for HIV medication…*" The extent of the information revealed in the letter depended on the way in which the letter was stuffed into the windowed envelope.

The letters were sent to customers currently taking medications for HIV treatment as well as for Pre-exposure Prophylaxis (PrEP), a regimen that helps prevent a person from acquiring HIV. Some of these letters had been viewed by family, roommates and neighbors, exposing the affected Aetna customers to discrimination and other trauma. Aetna has apologized for the breach.

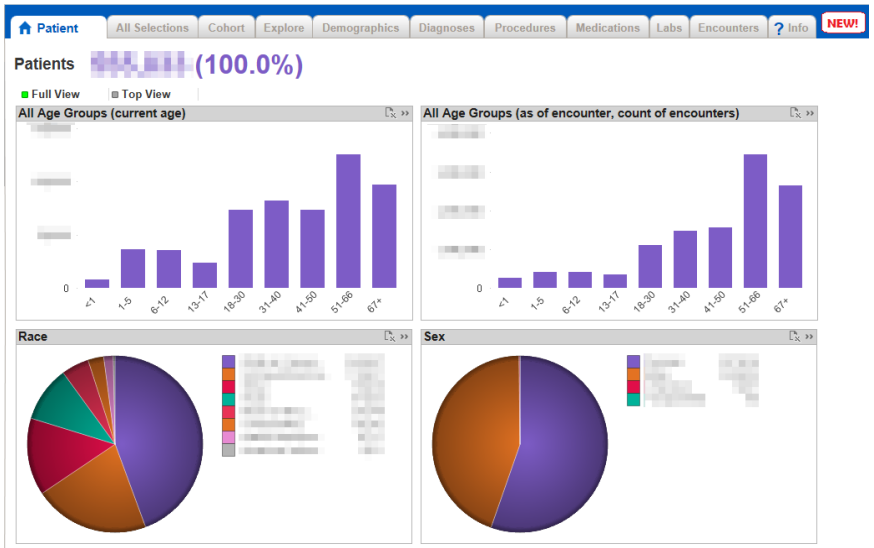
Remember – When preparing documents for mailing that may contain sensitive or confidential information, ensure that you use the correct type of envelope that obscures any sensitive or confidential information from view.

Unknown to Pirate Pete, Dual Authentication was going to make his *phishing* hobby a lot less enjoyable.

By Caitlyn Finley, Jan Kawano, Jaison Mathew, David Ta

Featured in the Privacy Toolkit: The Research Data Browser

Do you have a great research study idea but want to determine feasibility before exploring any further? The Research Data Browser (RDB) is a tool managed by Academic Research Systems and Enterprise Information Analysis for defining a query of UCSF patients without requiring the user to have specific training, such as the ability to write Structured Query Language (SQL). Once the query is defined, data may be exported for further analysis with the tools of your choice, i.e., Excel, Access, etc. The tool is broadly available to UCSF faculty, students and staff without IRB approval because the data is de-identified. To obtain access to RDB, go to http://myresearch.ucsf.edu/research-data-browser and follow the steps for "First Time Users."



Graphic by Academic Research Systems and Enterprise Information Analysis

According to Michael Deiner of Ophthalmology, some of the highlights of RDB include:

- Using a self-service tool to quickly ask whatever exploratory clinical questions you want to from the entire EHR, without IRB approval, “on the fly” and worry-free
- Using RDB to ask novel questions you normally would not have bandwidth to ask since there’s no delay of needing to submit and obtain prior IRB approval
- Using RDB to quickly gather feasibility data, including demographics, for grant proposals. With IRB approval, the datasets downloaded from RDB can be quickly re-identified for more detailed chart review and analysis. Several funded grants and publications probably would not have come to fruition for Michael without RDB.

Added bonus: the UCSF Privacy Office prefers researchers utilize the RDB as much as possible to ensure UCSF complies with the minimum necessary standard when reviewing health information for research purposes!

Special thanks to Dana Ludwig for contributing content for this article.

Test Your Privacy Knowledge—Complete the Quiz!

Congratulations to the winner of our Summer Privacy Knowledge Quiz, **Katie Kinzer (PGY3 Resident)** of Radiology.

We hope you enjoy your Amazon gift card!

Test your privacy knowledge! For your chance to win a $25 Amazon gift card, submit your answer to the question below to UCSFPrivacyOfficeDrawing@gmail.com by December 15, 2017.

One lucky winner will be chosen out of the correct responses to receive a gift card.

Quiz Question: When receiving an email communication, what is a “red flag” that you should look for that might indicate that it is a phishing message? Select all that apply.

A. An unfamiliar “from” address

B. Urgent action required

C. Generic greeting

D. Link to an unknown website