University of California
San Francisco

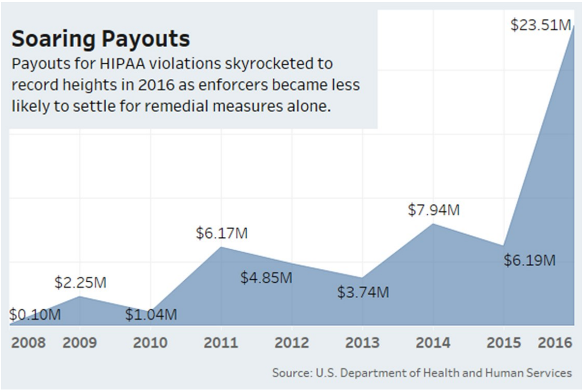
Tips from the Privacy Office

Patient Privacy and Me: My Role in Protecting PHI

At UCSF we are tasked with upholding patient rights and establishing and maintaining a culture of patient safety. Doing so supports UCSF as a business, helps us avoid penalties and fines, and guides us in our mission to Achieve Zero Harm.

Privacy breaches that result in the unauthorized access, use or disclosure of patients' protected health information (PHI) diminish patients' trust in our institution, put patients' confidential information at risk, and place UCSF at risk for regulatory fines and penalties.

We must do our part to prevent reportable breach incidents from happening by following best practices, promptly reporting any suspected breach incidents to the Privacy Office, and holding one another accountable whenever we see risky privacy practices occurring.


Soaring Payouts

Payouts for HIPAA violations skyrocketed to record heights in 2016 as enforcers became less likely to settle for remedial measures alone.

Source: U.S. Department of Health and Human Services

In 2016, the Office of Civil Rights (OCR) levied a record-breaking $23.5 million against covered entities to settle enforcement actions for HIPAA privacy breach incidents. Breaches of patient privacy are becoming increasingly costly, and the enforcement trend does not seem to be slowing any time soon. Avoid incurring penalties and fines for the institution by following our privacy best practices outlined in this tip sheet.

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

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 tips on how to prevent these three common types of breach incidents from occurring.

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. 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

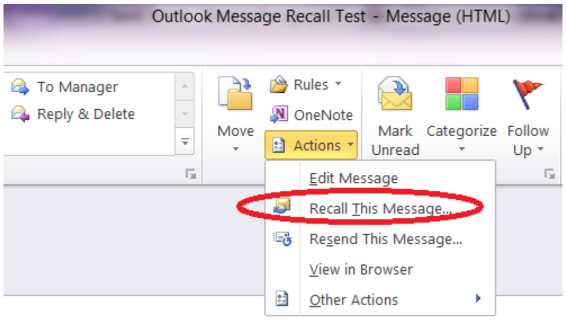
Preventing Unauthorized Disclosures via Misdirected Emails

Mistakes can happen when sending email. If you send an email that contains confidential or sensitive information to the wrong recipient, here are some tips that could potentially save the day.

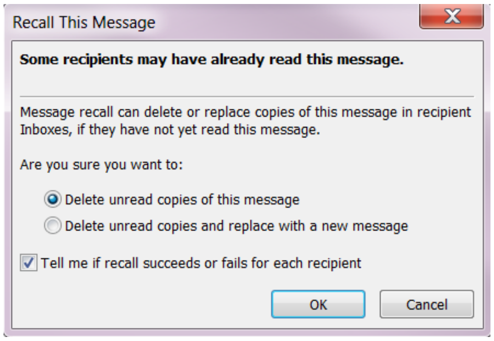
Outlook Recall for Internally Misdirected Emails

Did you inadvertently send an email containing sensitive information to the wrong person within UCSF? Act swiftly in Outlook as soon as you realize the email was sent to the wrong recipient by recalling the message.

1. Open the message in your Outbox / Sent Folder.
2. In the toolbar at the top of your screen, select **Actions.**
3. From the drop down menu select **Recall This Message**.



4. Select **Delete unread copies of this message**.



Recall This Message

Some recipients may have already read this message.

Message recall can delete or replace copies of this message in recipient Inboxes, if they have not yet read this message.

Are you sure you want to:

● Delete unread copies of this message

○ Delete unread copies and replace with a new message

☑ Tell me if recall succeeds or fails for each recipient

5. If the recipient has already opened and read the message, it is still important to contact them to let them know the email was misdirected to their inbox. Instruct them to delete the message from both their inbox and their email trash bin.

CISCO Secure Email to Lock Externally Misdirected Emails

Did you send an email securely to the incorrect recipient outside of UCSF? Great — there could be a silver lining, and it's another reason why all messages containing confidential or sensitive information should be sent with a secure trigger regardless of whether the email is directed internally or externally. Again, swift action could potentially save the day.

Locking and Unlocking Messages

You can lock sent messages to prevent recipients from opening them. After you lock a message, the recipient cannot open the Registered Envelope to access the encrypted content. When you lock messages, you lock them for individual message recipients. You can also lock a message for some recipients and leave it unlocked for others.

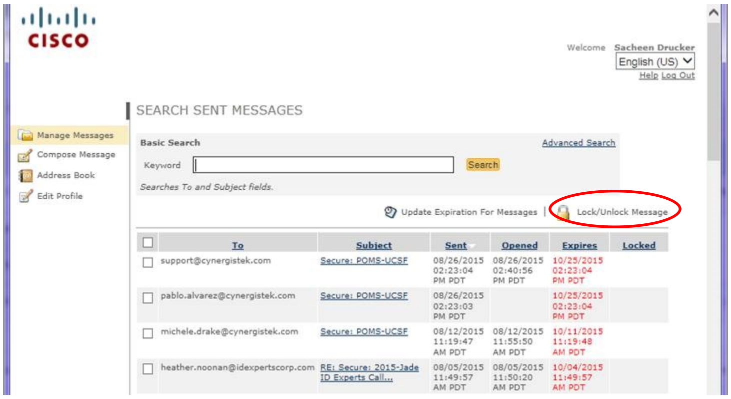
UCSF Secure Email Web link: https://res.cisco.com/websafe/

To lock one or more messages:

1. Select Manage Messages in the left-hand navigation menu.
2. Click **Search** to retrieve all sent envelopes, or else run a basic or advanced search to retrieve specific envelopes.
3. In the results list, select the check boxes for the messages you want to lock. Note: If you sent a message to multiple recipients, the same message might appear in several rows. Select the check box for each recipient you want to prevent from opening the message.
4. Click the Lock/Unlock Message icon above the results list. The Update Sent Messages page is displayed.
5. Verify that "Lock all selected messages" option is selected.
6. Optionally, enter your reason for locking the messages. The lock reason is displayed to recipients when they view the envelope.

Click **Update**.

Note — If you specify a reason for the lock, the reason is displayed to recipients when they view the Registered Envelope. To change the lock reason notification, follow the steps to lock the message, and enter a new reason before you click **Update**.



☐	To	Subject	Sent	Opened	Expires	Locked
☐	support@cynergistek.com	Secure: POMS-UCSF	08/26/2015 02:23:04 PM PDT	08/26/2015 02:40:56 PM PDT	10/25/2015 02:23:04 PM PDT	
☐	pablo.alvarez@cynergistek.com	Secure: POMS-UCSF	08/26/2015 02:23:03 PM PDT		10/25/2015 02:23:04 PM PDT	
☐	michele.drake@cynergistek.com	Secure: POMS-UCSF	08/12/2015 11:19:47 AM PDT	08/12/2015 11:55:50 AM PDT	10/11/2015 11:19:48 AM PDT	
☐	heather.noonan@idexpertscorp.com	RE: Secure: 2015-Jade ID Experts Call...	08/05/2015 11:49:57 AM PDT	08/05/2015 11:50:20 AM PDT	10/04/2015 11:49:57 AM PDT	

When a message is locked, a padlock icon appears in the Locked column of the results list.

Think Twice Before Attaching Files with Lots of PHI!

Has a colleague working from home ever asked you to forward a document containing information containing a lot of PHI? Instead of attaching the file to an email that could potentially be misdirected, save the file to a share drive and have the colleague VPN in to view the document. Alternatively, upload the document to UCSF Secure Box where the information can be encrypted and shared among internal collaborators. More information on Secure Box is available here: http://tiny.ucsf.edu/6RaREm.