

UCSF Privacy Office

# Privacy and Confidentiality Update

Privacy Office  
2200 Post Street, C-509  
San Francisco, CA 94115-1922

Ph: 415.353.2750  
Fax: 415.353.9241  
Website: <http://hipaa.ucsf.edu/>

## Top Six Strategies to Lessen Your Personal Risk in An Environment of Increasing Legislation

In follow up to the December Newsletter, the Privacy Office received quite a few calls requesting guidance on risk reduction for personal liability and notification requirements created by the new state laws.

To help facilitate answers to the most common questions, we have devoted this month's newsletter to providing guidance on how to protect patient information and UCSF by implementing strategies that reduce the risk of a breach of patient information.

### 1. Use the secure email system (Tumbleweed)

The Privacy Office recommends that as a best practice you use it any time you place ePHI in an email, even if you only intend to send the message within the UCSF enterprise network. If you do this, you protect the information in the event that a mistake occurs and the email inadvertently goes outside the network.

For guidance on using, Medical Center IT, OAASIS, and the SOM all have guidance, the links are provided at the end of this newsletter.

#### Misconceptions:

- The ePHI is not encrypted when traveling through the UCSF enterprise network. It only becomes encrypted, when it travels outside the network.
- The system does not ensure you will not make a mistake when addressing an email. You still need to use the usual precautions and double check the recipients prior to pushing the send button.

#### How to use the system correctly:

(Summary of critical points, for details, refer to provided links or your IT control point):

- The start of the subject line must be precise in order to enable security.

*Cont'd to pg. 2*

## What To Do in The Event of a Breach of PHI/ePHI?

In our next newsletter we will provide a detailed guideline that you can use in the event of a suspected breach to facilitate acquisition of information and speed of notification under the direction of the Privacy Office. For now the most important points are as follows. Notify the Privacy Office immediately if you feel protected health information (PHI) may have been breached. We will work with you and provide the guidance on what you need to do.

If there has been a loss of an edevice, also notify UCSF Campus Police. In consideration of the five day patient and Department of Public Health notification requirement (calendar days not business days), it is imperative that we have as many of the details as quickly as possible.

#### Inside this issue:

Top Six Strategies to Lessen Your Personal Risk in An Environment of Increasing Legislation	1-3
What To Do in The Event of a Breach of PHI/ePHI?	1
Resources	3
Privacy Office Web Site	3

# Top Six Strategies to Lessen Your Personal Risk in An Environment of Increasing Legislation

*Cont'd from pg. 1*

- The system is very precise. The subject line should start out with ePHI, PHI or Secure at the beginning of the subject field followed by a colon and then a space. Examples of appropriate email subject lines:

ePHI: Your appt  
 PHI: Your appt  
 Secure: Your appt

How can you lessen your risk when sending the ePHI via email

- Address it correctly
  - ◇ Use caution when using the auto fill function, double check the correct names are in place
  - ◇ Review and eliminate any symbols inadvertently placed, such as an asterisk
- Storage:
  - ◇ If you use and store your emails in Outlook, make sure they are encrypted either on the actual device or on a server.
  - ◇ Set your deleted items folder to empty every time you close Outlook
  - ◇ Manage your folders frequently either delete or store encrypted. Don't forget about the sent items folder.

## 2. Encrypt your servers, laptops, memory sticks and CDs if they contain PHI

## 3. Add as many layers of protection to PHI as you reasonably can

- Lock your desk
- Lock down your personal computers
- Lock your office
- For areas without staff in place to provide oversight of records
  - ◇ Put away and lock up patient records
- For areas offsite: Building should be alarmed and tied into campus police monitoring system
- Use the Insta Shred system for PHI
  - ◇ Do not use the blue recycle bins. Breaches can occur when PHI is placed into recycling. Desig-

PHI is placed into recycling. Designate a temporary place at your desk and empty it at the end of every day when you go home.

- Make sure when you provide a patient with documents, it is their documents.
- Do not take any PHI off campus in any form. If you travel inter-campus with PHI, provide additional protections such as;
  - ◇ As reasonable; try to find an electronic solution that enables you not to travel with PHI (electronic or hard copy)
  - ◇ Encrypt any memory sticks or CDs
  - ◇ Encrypt laptops
  - ◇ Do not leave anything in your car; keep PHI/ePHI with you.
- Protect your mail and documents containing PHI that are being transported within the campus, to off site locations and outside the UCSF enterprise
  - ◇ If you send large amounts of information outside the UCSF enterprise and do not seal your envelopes, make sure you have an agreement with campus mail to seal the envelopes. It is not automatic.
  - ◇ Stamp envelopes with PHI as confidential
  - ◇ Make sure you have the correct address
  - ◇ If you use couriers,
    - Have a process to document transfer of document responsibility
    - Ensure same day delivery as much as possible. If not possible, require extra levels of protection while PHI/ePHI is stored with courier
- Internal Quality reviewers and researchers: Do not store your identification key in the same area or on the same device as the de-identified data.

## 4. Follow the minimum necessary standard

- Use the minimum necessary information in any forum which enables you to safely do your job.
- Only store/save information that you really need to do your job.
- Review old forms i.e.: if you no longer need some data fields don't ask for it.
- Find a way to use something besides SSN# as a way to identify a patient
- Try to de-identify the information as much as possible. When possible and if you can still provide care safely; use patient's first name and last initial when referring to patients in writing and via email.

Use caution when titling and saving large files with ePHI, you can inadvertently link the patients on the file with a

## Top Six Strategies to Lessen Your Personal Risk in An Environment of Increasing Legislation

*Cont'd from pg. 1-2*

- Use caution when naming and saving large files with ePHI, you can inadvertently link the patients on the file with a diagnosis if you use a disease or physician in the title

### 5. Monitor your access to systems

- Do not share your passwords under any circumstances
- Use complex passwords
- Do not maintain passwords or links on your computer to any databases that you no longer need to do your job

### 6. Make sure you have a Business Associates Agreement with Vendors to whom you provide PHI/ePHI.

- Your purchasing control point can help you with facilitation of this document



## Resources

Questions comments regarding the secure email solution should go to your appropriate IT control point

All other questions should go the Privacy Office 353-2750

Privacy Office Website

<http://hipaa.ucsf.edu>

Medical Center IT

[http://it.ucsfmedicalcenter.org/secure\\_email/](http://it.ucsfmedicalcenter.org/secure_email/)

Campus IT

<http://oaais.ucsf.edu/OAAIS/171-DSY>

<http://security.ucsf.edu/EIS/4809-DSY/version/default/part/AttachmentData/data/SecureEmailInstructions.pdf>

School of Medicine ISU

[http://www.medschool.ucsf.edu/help/Troubleshooting/secure\\_email.htm](http://www.medschool.ucsf.edu/help/Troubleshooting/secure_email.htm)

## Privacy Office Web Site

For further information related to privacy guidance, please visit the UCSF "Privacy Office" website which also includes privacy guidance, policies, forms, as well as educational modules related to HIPAA training and FAQs at <http://hipaa.ucsf.edu> or contact the Privacy Office at 353-2750.