

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/>

## Update on New State Privacy Laws

As referenced in a previous newsletter (Dec 2008), new State privacy laws were implemented on January 1, 2009. When there has been inappropriate review or viewing of patient information, the patients and the California Department of Public Health (CDPH) must be notified of the incident within **five days** of when the incident was discovered.

Therefore, it is vital, that **as soon as** you suspect or are aware that UCSF patient information may have been compromised, you or your manager immediately contacts the Privacy Office (415-353-2750) so we can evaluate the risk to the patient as well as notification requirements.

Privacy incidents can also be caused by errors with any format of medical information such as paper, verbal or electronic. Examples of simple errors include:

- Faxing patient information to the wrong number
- Mailing a patient document to the wrong address
- Emailing patient information to the wrong person
- Leaving a voice mail on the wrong answering machine.

## What Can You Do To Prevent Errors?

Simple, low tech behaviors can have a big impact on preventing loss of patient privacy. The UCSF Privacy (HIPAA) Handbook on the Privacy Website describes best practices such as:

- **Faxing PHI:**
  - o Always check that the destination fax number is current before faxing
  - o Make sure auto fax numbers are confirmed periodically to ensure accuracy
  - o Always include a cover sheet which includes a confidentiality notice which includes a contact number to call if received in error. See examples in the UCSF Privacy (HIPAA) Handbook.
  - o Call ahead to ensure that the intended recipient will pick up the fax

## The Privacy Office and You

Did you know that the UCSF Privacy Office is responsible for all privacy issues across the entire UCSF enterprise, not just the Medical Center? The UCSF Privacy Office covers all of the campus academic schools, the Medical Center, Langlely Porter Psychiatric Hospital and Clinics, Proctor Foundation, Student Health Services, and UCSF Fresno.

We provide consultations, guidance, risk mitigations as well as conduct investigations and coordinate patient, federal agency, and state agency notifications for privacy incidents. Visit the UCSF Privacy website for guidance on education, forms, privacy policies, and news updates on privacy at <http://hipaa.ucsf.edu/default.html>.

### Inside this issue:

Update on New State Privacy Laws	1
The Privacy Office and You	1
What Can You Do To Prevent Errors?	1 - 2
Unauthorized Access	2
Important Reminder	2
Privacy Office Web Site	2

## What Can You Do to Prevent Errors?

Cont'd from pg. 1

- **Mail:**
  - o Check that the name on the document matches the name on the mailing envelope before stuffing the envelope
  - o Always check that multiple sheets are not stuck together to prevent accidentally mailing another individual's documents to the wrong person
  - o Ensure that the envelopes are sealed before mailing
  
- **Email:**
  - o Always check the email address before you hit the "send" button, especially if using a distribution list
  - o Include a confidentiality notice in the footer in your message (See UCSF Privacy (HIPAA) Handbook)
  - o Do not send attachments containing ePHI unless encrypted
  - o When in doubt, use secure email (Tumbleweed) in which subject line starts with either "Secure: ", or "PHI: " or "ePHI:" (there must be a space after the colon before you type in the rest of your subject line for example:
 

SECURE: Document regarding topic  
PHI: Document regarding topic  
ePHI: Document regarding topic
  
- **Voice mail/Answering Machines:**
  - o Limit the information left on a recording as others may access or overhear the recording when played back
  - o Don't leave detailed PHI messages on voice mail
  - o Be aware of your surroundings when using a speakerphone

## Unauthorized Access

With the Kaiser case (link below), we are already seeing the Department of Public Health levy organizational penalties for breaches involving unauthorized access. Although we have yet to see how the individual cases will be handled in this breach, the potential for penalties is high. The good news is that you can virtually eliminate this risk entirely, by remembering to not look up any patient information outside of the following purposes; treatment, payment or operations. This includes family members. Many well meaning individuals have looked up family members or friends and have later found themselves under investigation when the relationship changed. This also includes viewing information for research; make sure you access only the record or data only as outlined in your CHR approval.

<http://www.propublica.org/article/kaiser-hospital-fined-250000-for-privacy-breach-in-octuplet-case-515>

## Important Reminders

**If you access Protected Health Information (PHI) or Personally Identifiable Information (PII), you are personally responsible** for ensuring the confidentiality, privacy, and security of the data entrusted to you, and you could be personally subject to statutory fines and penalties for failure to comply. You are expected to:

- Access, use, disclose only the minimum necessary amount of information
- Use safeguards to protect verbal, written, electronic health information including encryption software
- The "Secure" e-mail system must be used if ePHI is in the e-mail message
- Dispose of health information appropriately De-identify information whenever possible

## 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>.