Announcing... the 2014 Privacy and Security Training Program

UCSF Chancellor Sam Hawgood and UCSF Medical Center and Benioff Children’s Hospital CEO Mark Laret recently sent a communication regarding the online Privacy and Security Training Program. UCSF is launching this training program as part of its commitment to protecting confidential information.

Why We Need To Do This

UCSF experienced three recent breaches involving stolen, unencrypted laptops and desktops. Each breach affected thousands of patients and required notifications to each person, as well as multiple regulatory agencies and media outlets. The incidents drew the attention of:

- Office for Civil Rights (OCR)
- Centers for Medicare and Medicaid Services (CMS)
- California Department of Public Health (CDPH)
- Department of Education (DOE)
- Office of Human Research Protection (OHRP)
- News reporters

These breaches are very costly to the University in terms of reputational damage, investigation and data breach response expenses, and come with potential fines and penalties. In addition to UCSF’s need to address these breaches, and due to amendments to HIPAA regulations made last year, we have an obligation to train our workforce on current privacy, security, and encryption requirements and best practices.

Training Module Summary

In response to these breaches and the new HIPAA regulations, UCSF assigned the Privacy and Security Briefing training module to all workforce members via the UC Learning Center. The 10-15 minute module will cover the following:

- Encryption Requirements for Electronic Devices
- Recent Privacy Regulatory Changes
- Privacy and Security Resources

The training period began August 1, 2014 and the training must be completed by January 31, 2015. Visit the [UC Learning Center](http://hipaa.ucsf.edu) and search for “Privacy and Security Briefing” to complete the course.

Unauthorized & Inappropriate Access of Patient Information—Workforce Alert

As a UCSF workforce member you likely have private and even sensitive patient information at your fingertips. However, you must not access that information if it is not an integral part of your job duties. Please be reminded that your access is subject to monitoring and auditing so that UCSF is able to determine if your access was not authorized and was not appropriate.

For example, in APeX (UCSF Medical Center’s electronic medical record) security safeguards are in place to protect UCSF patients’ privacy, and to ensure the security of UCSF’s systems. To do so, APeX access is logged, and a record of it is saved. These records may be audited and compared against the individual’s job function and responsibilities to determine whether the access was authorized and appropriate.

This means that if you’re looking at medical records that are not within your job-related needs to access, there will be a permanent audit trail of your unauthorized and inappropriate access.

UCSF keeps these records, and is required by law to fully investigate every single allegation of inappropriate access, no matter how minor the alleged inappropriate access and how long ago it occurred.
PRIVACY and CONFIDENTIALITY NEWSLETTER  
Summer 2014

Those same laws impose criminal penalties on workforce members who have snooped into patient records. Even if the snooping does not result in criminal sanctions, because UCSF values patient privacy, UCSF can take appropriate disciplinary action— even leading to termination— against any workforce members who access patient information inappropriately or without authorization.

You are required to stay out of patient records unless you have a valid UCSF business reason to access them (this includes access to your family members’ or friends’ records). This is not just a matter of respect for patients’ privacy, but also to comply with federal and state privacy laws and regulations.

How Do I Encrypt My Personal Device?
UCSF recently developed resources to assist our workforce with encrypting their personal devices:
- Personal laptop/desktop – Installation guidelines: http://tiny.ucsf.edu/9bTkaB
- Smartphone – Enabling ActiveSync for UCSF email: http://tiny.ucsf.edu/QweBYV
- Encryption frequently asked questions (FAQs): http://tiny.ucsf.edu/ZAayfD

If you have encryption-related questions, contact the UCSF IT Service Desk at (415) 514-4100

Remember: Encryption protects patients, UCSF and you.

Social Networking – Think Before You Post

Had a bad day at work and want to vent about it? Had a great day at work and want to brag about it? Lost a patient and want support? Saved a patient and want some praise? Thinking of doing this on social media? Think twice about it before you do!

In today’s electronic world we’re used to sharing almost everything that happens in our lives with our “friends,” “followers,” and “connections.” However, the repercussions of posting patient or other confidential information are severe. In fact, pursuant to HIPAA, the criminal penalties for inappropriately disclosing protected health information can be as high as a $1.5 million fine and ten years in prison. On top of that, state law imposes additional penalties that include fines, imprisonment, and loss of your medical license.

It is also important to remember that it does not take much to trigger Privacy laws. Your social media post does not have to include a patient’s name or social security number. Nor do you have to mention that you work at UCSF. In fact, you are considered to have breached a patient’s privacy if you post ANY information that can be used to identify them. Say you posted something about a patient you treated in the ED, even without identifying them in any way, and a reader of your post realized where you work from another social media site. If that reader connected that information to a news report about a particular person being taken to UCSFMC on the same day as your post, you could be found to have violated patient privacy laws. As you can see, in today’s interconnected world, it does not take much information for people to connect the dots!

So, the next time you want to share something on social media, stop and think whether there is anything in your post that could be used to identify anyone at UCSF. Remember, one click could result in fines, imprisonment, and loss of your job.

Privacy Resources

You have privacy questions and concerns. We have answers! Call us anytime at (415) 353-2750, or visit our website at http://hipaa.ucsf.edu. Additionally, check out the following resources:

- APeX Guide: Primary Care (PCP) & Referral Provider Selection: http://tiny.ucsf.edu/pK3TSx
- Updated Advanced HIPAA Healthcare Provider training: http://hipaa.ucsf.edu/education/downloads/ProviderModule.pdf
- Updated Advanced HIPAA Communications and University Relations training: http://hipaa.ucsf.edu/education/downloads/PublicRelationsModule.pdf
Research Corner: Human Research Protection Tips

You forgot to get research HIPAA authorization forms signed – Now What??

The Committee on Human Research (CHR) requires investigators to obtain signed research HIPAA authorization forms from all participants if Protected Health Information (PHI) will be used or disclosed for research purposes. Please note that the research HIPAA form is not the Notice of Privacy Practice form used with clinical patients. The template research HIPAA authorization form (translated into many languages) is posted on the CHR website.

If you enrolled participants in a research study that involves PHI, but did not obtain signed research HIPAA authorization forms, you need to immediately do the following:

- Verify the CHR requirements: Is research HIPAA authorization required for the research?
  - Sign into the iRIS system to review your CHR approval letter from the latest continuing review, or the initial approval letter for new studies. These letters specify the HIPAA requirements.
  - For more information about HIPAA and research, review the CHR HIPAA website.
  - Call the general CHR number (415) 476-1814 and ask to speak with the Quality Improvement Unit (QIU) Analyst of the Day. A QIU analyst will assist you with reviewing your CHR approval letter and/or CHR application to determine the HIPAA requirements.

- Take Corrective Actions
  - Re-Contact: If it is possible to re-contact previously enrolled participants, the QIU analyst will provide you with a CHR-approved template cover letter and phone script that researchers can use to re-contact participants and request written HIPAA authorization for the research. This should happen as soon as possible.
  - iRIS Submission: Within 10 working days of becoming aware of the problem, submit a Protocol Violation/Incident Reporting Form in the iRIS system. The QIU analyst can provide guidance on completing this form.

Tip: Before enrolling participants, review your CHR approval letter to determine whether research HIPAA authorization is required.

IT Security Corner – Establishing A Data Security Compliance Program

There are two main components of HIPAA: the Privacy Rule and the Security Rule. Doubtless you have heard a great deal over the last decade about the Privacy Rule. Depending on the circles you run in, you may not have heard much about the Security Rule. At UCSF we have established a Data Security Compliance Program (DSCP) to address the HIPAA Security Rule and other regulations (e.g., HITECH Act, the Family Educational Rights and Privacy Act (FERPA), and the California Security Breach Information Act (S.B. 1386)). The DSCP is charged with ensuring UCSF implements and maintains the security controls required by these laws and regulations.

In 2013-2014, UCSF retained Accuvant LABS to conduct an enterprise IT security risk assessment. The assessment covered 142 unique controls that must be satisfied by all 12 administrative control points, which include the schools, medical center, central IT and all of their departments, divisions and programs.

The DSCP team will be working with these control points to fill gaps and address findings identified in the 2013-2014 Enterprise Risk Assessment. All of the control points have been given recommendation plans for each risk identified. In some cases the recommendations can be addressed by the control point directly, while in other cases the risk identified belongs to the enterprise as well as the control point, and as such, a joint effort is required to satisfy the recommendation.

If you are interested in learning more about the regulatory compliance described in this article or the DSCP, please contact the DSCP Program Manager, Christine Ziegler.