Final Omnibus Rule Amends HIPAA

Ninety four percent (94%) of the 80 healthcare organizations surveyed have suffered data breaches over the past 2 years, according to a national patient privacy and data security study conducted by Ponemon Institute LLC\(^1\). In response to the increasing privacy and security risks, federal and state governments are tightening existing privacy regulations. In fact, on January 25, 2013, the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) published the HIPAA Final Omnibus Rule, which amends and strengthens the HIPAA Rules. The compliance date is September 23, 2013. Please visit: [http://www.hhs.gov/news/press/2013pres/01/20130117b.html](http://www.hhs.gov/news/press/2013pres/01/20130117b.html)

Highlights of the Final Omnibus Rule include:

- **Business Associates (BA):**
  - Expands the definition of a BA, and makes them directly liable for compliance with certain HIPAA provisions
  - BA’s subcontractors are considered BA’s themselves, and subject to the same HIPAA provisions
  - Changes the Business Associate Agreement provisions (at UCSF, the BAA has been revised and is currently in use)

- **Breach determination:** Changes the required risk assessment to determine whether a “breach” has occurred

- **Marketing:** Requires the Covered Entity to obtain authorization for marketing communications if the Covered Entity receives financial remuneration from a third party whose product or service is marketed in the communications, with certain exceptions

- **Sale of PHI:** Prohibits a Covered Entity or Business Associate from receiving remuneration in exchange for PHI without an individual’s authorization, with limited exceptions (e.g., for treatment and payment purposes or as required by law)

- **Self-pay restrictions:** Requires the Covered Entity to agree to a patient’s request to restrict disclosure of PHI to a health plan if the PHI pertains to services for which the patient paid out of pocket and in full

- **Right to receive electronic copies of information:** Provides patients the right to obtain an electronic copy of their PHI

- **Notice of Privacy Practices:** Requires changes to the Notice of Privacy Practices (NPP); revisions to UCSF’s NPP are in progress and the updated NPP will be available in September 2013

- **Research:** Permits the use of a compound authorization for conditioned and unconditioned authorizations; permits the use of an authorization to encompass future research studies

- **Child immunization records:** Provides greater flexibility to disclose student immunization records without an authorization to schools

- **Decedent information:** Provides greater flexibility to use and disclose decedents’ PHI for 50 years after death

---

Cedars-Sinai Privacy Breach Results in Six Firings

Cedars-Sinai made recent headlines when six workforce members were fired for inappropriately accessing patient records. According to the Los Angeles Times, 14 patient medical records were accessed inappropriately between June 18 and June 24, 2013. The six workforce members who were fired included a medical assistant, employees of community physicians who were using the logins of the physicians, and an unpaid student research assistant. Those fired will permanently lose access to Cedars-Sinai patient records.

How can you avoid similar situations at UCSF? Remember TPO – you may only access patient records for the purposes of Treatment, Payment, and Operations. Access only the minimum necessary information to perform your job. Never share your login information with others and log off clinical systems as you step away from your workstation, as you are accountable for any access using your credentials.

Chicago-Area Breach May Impact 4 Million Patients

Last month, Advocate Medical Group reported that four unencrypted computers were stolen from a Chicago-area group practice. Healthcare Info Security reports that this breach may have compromised the PHI of approximately 4 million patients. Information on the stolen unencrypted computers may have included Social Security numbers and diagnoses.

As a reminder: encryption is required for all electronic devices that contain UCSF PHI, regardless of other factors, such as amount of PHI, whether personal or UCSF owned, currently in use or obsolete, functioning or broken, physical security, and storage location. Contact the IT Service Desk at (415) 514-4100 for questions regarding encryption.

OCR Pulse: National Privacy by the Numbers

Monthly reported privacy breaches affecting > 500 individuals in the US

- Feb / Mar 2013: 18 breaches affecting 104,789 people
- Apr / May 2013: 28 breaches affecting 227,819 people
- Jun / Jul 2013: 32 breaches affecting 378,048 people

2.5 Million California residents were affected by data breaches in 2012

Sources: Health Information Privacy/Security Alert, HHS Office for Civil Rights; California Healthline, Daily Edition

When is it OK to share PHI?

For guidance, please visit the FAQ section of the Privacy Website here:

http://hipaa.ucsf.edu/faqs/default.html
Should I Take PHI Off Site?
Lessons Learned

Do you ever find yourself trying to meet a deadline at the eleventh hour and want to bring your work home? Or do you work between multiple UCSF sites and need to transport PHI between sites? Before taking any PHI off site, please take a moment to consider the risks and alternatives.

Risks: Taking PHI off site is inherently risky. Take the example of a Massachusetts General Hospital employee, who inadvertently left documents on a subway while commuting to work. The documents consisted of PHI for 192 patients of Mass General’s Infectious Disease practice, including patients with HIV/AIDS. The HIPAA enforcement agency, Office for Civil Rights (OCR), found that Mass General failed to implement “reasonable, appropriate safeguards to protect the privacy of PHI” removed from Mass General’s premises, thus potentially violating the HIPAA rule. As a result, Mass General agreed to pay the U.S. government $1 million to settle the potential HIPAA violations.

The risk of lost or stolen PHI holds true not only when using public transportation, but also when you take PHI into a public area (e.g., a bar, restaurant, or airport), when you lock it in the trunk of your car, or even when you bring it into your home.

Alternatives and best practices: Federal and state regulations, as well as UCSF policy, require you to protect the privacy and confidentiality of PHI in any format, including verbal, electronic, and paper. Best practice is to refrain from taking PHI off site, and to use alternative methods for accessing information remotely, such as accessing UCSF systems via Virtual Private Network (VPN).

If your job requires you to transport PHI between UCSF sites:

+ Consider other options, such as securely emailing or faxing the PHI to yourself, or accessing it via a secure gateway from your offsite location
+ Remember that you are responsible for securing the PHI and keeping it in your possession at all times
+ Do not leave PHI unattended in your bag, briefcase, folder or your car, even if it’s locked in the trunk
+ Remove the PHI from your bag, briefcase, folder, car, etc. once onsite and secure it in your office or work area

If you have questions about protecting and/or handling PHI, please contact your manager or the Privacy Office at (415) 353-2750.

Information Security Corner: Social Networking is Not for the Faint of Heart

Social media sites, such as Facebook, Twitter, LinkedIn, and Google+, are a useful way to send out and receive information. You can easily obtain industry news, share images, catch up with family and friends, and contribute to discussion on relevant topics. However, as you use these sites, ask yourself whether you are taking the precautions to protect yourself and UCSF.

With some easy actions, you can reduce the chances of becoming a victim of cybercrime, such as identify theft, and protect your own reputation and that of UCSF. Below are some helpful guidelines:

+ Use a different password for each site, and do NOT use the same password you use for UCSF systems. Using the same password makes it easy for criminals to target you, especially your financial online accounts. In addition, use different security questions in order to thwart thieves from taking over your account.
+ To review the UCSF Social Media Guidelines, please visit: http://tiny.ucsf.edu/socialmedia
(continued from Page 3)

+ Posting confidential data via social media, such as patient data (including patient photographs, regardless of whether a facial image is shown), may violate federal, state, and UCSF policy. It may lead to termination, criminal prosecution, and civil penalties. When in doubt, check with the Privacy Office or IT Security.

+ It bears repeating: think before you post. It is nearly impossible to remove information from the Internet once it is posted. Just because you have your privacy setting configured to limit sharing does not mean your friends or colleagues do.

+ Be wary of clicking on dubious links that friends post, such as “free tickets”, or other “too good to be true” offers. Often these are links that install viruses on your computer and attempt to hijack your account and personal data.

By following these steps you can enjoy the usefulness of social media, while limiting your risk and the risk to UCSF. Remember that together, we can advance health worldwide... securely.

**Research Corner: Human Research Protection Tips**

You know you need a signed Individual HIPAA Authorization form when:

+ This is stated in your CHR approval letter
+ You are conducting human subjects research in the UCSF Medical Center or Clinics

Not all privacy forms are created equal. The [UCSF Medical Center Notice of Privacy Practices](http://hipaa.ucsf.edu/privacyHandbook.pdf) (NPP) and the [Acknowledgement of Receipt of NPP](http://hipaa.ucsf.edu/privacyHandbook.pdf) are for clinical purposes and do not substitute for a signed Individual HIPAA Authorization form.

The Individual HIPAA Authorization form is referred to by many different titles:

+ University of California Permission to Use Personal Health Information for Research (official title of form)
+ UCSF Subject Authorization For Release of PHI for Research (how CHR refers to form on website)
+ HIPAA = HIPAA Authorization = Research HIPAA (how researchers refer to the form)
+ Individual HIPAA Authorization (language on CHR approval letters)

To view the individual HIPAA Authorization form, please visit [http://tiny.ucsf.edu/Az7fOe](http://tiny.ucsf.edu/Az7fOe). When in doubt, call the CHR at (415) 476-1814 and ask to speak to the Analyst of the Day.

**Privacy Reminders**

**Revised Privacy and Confidentiality Handbook:** The Privacy Office is pleased to announce the release of our newly updated UCSF Privacy and Confidentiality Handbook for faculty, staff, trainees, students and volunteers. The handbook was updated with new guidance based on recent regulatory changes, as well as relevant privacy issues and trends facing UCSF. It also includes a revised Confidentiality Statement (Appendix 3), which all workforce are required to sign upon hire. The handbook can be downloaded at the Privacy Office Website: [http://hipaa.ucsf.edu/Privacy_Handbook.pdf](http://hipaa.ucsf.edu/Privacy_Handbook.pdf), or departments can order by contacting Judy Flannery at 502-6438.

**New BAA Reminder:** UCSF has implemented a new system-wide BAA. For more information, please contact David Pendergast in Campus Procurement at (415) 514-9649, Carol Ng-Lee in Med Center Purchasing at (415) 353-8434, or Irene Shin in Innovation, Technology & Alliances at (415) 502-1602.

**Disposal and Destruction Process:** When destroying PHI on electronic devices, it is the owner’s responsibility to properly review disposal and destruction guidelines prior to the device leaving UCSF. For a list of guidelines, please refer to page 16 of the Privacy and Confidentiality Handbook at [http://hipaa.ucsf.edu/Privacy_Handbook.pdf](http://hipaa.ucsf.edu/Privacy_Handbook.pdf).

**Voicemail Security Changes:** The campus Information Technology Services department has migrated to a modern voicemail system, Microsoft Unified Messaging. Carefully review the guidance for securely handling voicemail messages on the [Next Generation Voice project FAQ page](http://hipaa.ucsf.edu/Privacy_Handbook.pdf). Or, you may go to the How Secure Email Works tutorial for further information.

For more information visit [http://hipaa.ucsf.edu](http://hipaa.ucsf.edu) or email the Privacy Office at [privacy@ucsf.edu](mailto:privacy@ucsf.edu)