Privacy Breaches Make Headlines

Stanford Patient Data Exposed on the Web

Earlier this month, Stanford Hospital confirmed that a detailed spreadsheet made its way from one of its vendors, a billing contractor identified as Multi-Specialty Collection Services, to a Web site called Student of Fortune, which allows students to solicit paid assistance with their school work. Listed on the spreadsheet were the names, diagnosis codes, account numbers, admission and discharge dates, and billing charges for 20,000 patients seen in Stanford Hospital’s emergency room in 2009. The breach was discovered by a patient and reported to Stanford on August 22. Stanford took aggressive steps to ensure the post was removed the next day.

“Bryan Cline, a vice president with the Health Information Trust Alliance, a nonprofit company that establishes privacy guidelines for health providers, said nearly 20 percent of breaches involved outside contractors, accounting for more than half of all the records exposed. Health care providers depend unjustifiably on legal contracts with vendors to protect medical records. “That just doesn’t work, as we can see.” “You have to do due diligence, something to assure yourself that the people you’re giving your data to can be trusted.”

Sources: The New York Times

UCLA Pays for Snooping Employees

UCLA entered into a settlement to pay $865,000 for two employees who had repeatedly and illegally viewed the medical records of celebrities such as Britney Spears, Maria Shriver, and Michael Jackson, in 2008. Federal Health Regulators found that UCLA had not adequately re-educated its workforce, disciplined staff, or remedied the situation. As part of the settlement, UCLA submitted a Corrective Action Plan, detailing how breaches would be prevented in the future. The plan includes employee sanctions, staff retraining, enactment of OCR-approved privacy and security policies and procedures, and the designation of an independent monitor to oversee UCLA’s required compliance activities for a 3 year time period.
CDPH Penalties for Late Reporting

Licensed Healthcare Facilities are required to report privacy breaches to the California Department of Public Health (CDPH) and to the affected patient no later than 5 business days after detection of the incident. Should the Licensed Facility fail to report within that timeframe, CDPH assesses an administrative penalty of $100 per day per patient.

What does this mean for you? Now, more than ever, it is critical that you report any known or suspected privacy incidents to the Privacy Office immediately, in order to avoid potential penalties for you, your Department, and the institution.

OCR Pulse: Privacy by the Numbers

- 11.5 million people in US affected due to 292 privacy breaches in 1 month (June – July 2011)
  - Laptops remain the #1 vulnerability, followed by unauthorized access or disclosure
  - California reported the most breaches (32), followed by Texas (24)
  - About 1 in 4 breaches was caused by a Business Associate
- Privacy Complaints to OCR remain steady
  - About 22% of all complaints require corrective action
  - OCR is making more use of the Resolution Agreement, which impose fines and Corrective Action Plans

Sources: Health Information Privacy/Security Alert; HHS Office for Civil Rights

Data Security for End-of-Life Electronics

Many of the electronic devices we use every day to do our jobs inevitably store confidential patient information. Federal law, state law, and UC policy dictate that at the end of their useful life, we must dispose of the electronic storage media appropriately to ensure that any confidential information residing on the device is rendered “unusable, unreadable, or indecipherable”. Often times, simply deleting files or re-formatting discs is not enough, as invisible data persists, which may be impossible for the average user to remove. For example, most modern digital copiers contain a hard drive that amasses images of every document copied, scanned, faxed, or e-mailed.

CDs, DVDs, and medical cards can be cross-cut shredded into unreadable bits by most sophisticated office shredders, but may also be placed in media bins provided by Cintas, along with videotapes and films.

Other types of electronics, such as hard drives, require special processing. ITS now offers a free, campus-wide service to properly dispose of certain types of electronic media. Simply drop off your laptop or computer hard drives and data tapes in person at their facility, and information will be wiped clean. The user will receive a certificate of destruction for their records.

To request a media bin for your unit, contact Environmental Services.

Cont’d to page 3
Data Security for End-of-Life Electronics

Cont’d from page 2

Should you have items not accepted by Cintas or the ITS service, such as PDAs, phones, cameras, or fax machines, you should secure a vendor (complete with a contract and Business Associate agreement) that utilizes HIPAA and NIST compliant data destruction methods appropriate to render any confidential information unusable, unreadable, and indecipherable, such as:

- Clearing / Overwriting (not acceptable for extremely sensitive or confidential data)
- Secure Erasure / Sanitization
- Physical Destruction (deforming, grinding, pulverizing, melting, incinerating, shredding, pulping, etc.)
- Purging / Degaussing (exposure to strong magnetic fields to disrupt magnetic domains)

For questions regarding the ITS service, electronic data destruction, or to request vendor recommendations, please contact the IT Service Desk at (415) 514-4100, visit the ITS website at http://security.ucsf.edu/EIS/13256-DSY.html, and/or reference UCSF Medical Center Policy 5.01.04 (Information Security and Confidentiality), and Medical Center / School of Medicine / School of Nursing Device and Media Controls Procedure.

Faxing Confidential Information

Did you know that inadvertently faxing confidential patient information to the wrong party is one of the most prevalent privacy errors? Below are a few simple tips to prevent this commonplace error:

- Pre-program commonly used numbers. Verify the numbers every 6 months. Otherwise, confirm the number prior to sending, and confirm that you’ve keyed it in correctly.
- Double-check each page you plan to send
- Use a cover sheet with a confidentiality statement and complete contact information for both parties
- Send only the minimum necessary information
- Contact recipient to advise of incoming fax or to confirm receipt afterwards
- Keep fax machines in secure locations
- Do not leave documents unattended at the machine
- Obtain and retain fax confirmation sheets or logs
- Where possible, designate one person to be responsible for faxing
- Separate the duties of faxing from other work to allow the sender to focus on the task at hand
- Consider a written faxing procedure that is reviewed with staff annually

What’s New?

Have a look at our recently updated educational materials and forms:

- UCSF Privacy and Confidentiality Handbook (Revised 2011)
  This Handbook provides a general introduction to privacy and security, and is meant to provide a basic understanding of HIPAA, California privacy and security laws, and related UC policies. If it’s been a while since you or your team has read it, now’s a great time for a refresher!
What’s New?
Cont’d from page 3

- **Confidentiality Statement**
  This statement serves to remind workforce members of their confidentiality obligations. It is required to be read and signed upon hire. Signed statements should be retained as documentation in the personnel file.

- **HIPAA 101**
  This presentation provides an overview of HIPAA privacy laws and regulations, how they affect you and your job, ways to protect patient confidentiality, your responsibilities as a workforce member, and how to report breaches.

- **Advanced HIPAA for Fundraising (Now in LMS!)**
  This presentation is mandatory for UCSF workforce members who are involved in fundraising and development. The training provides the viewer with an increased understanding of their responsibilities for maintaining patient privacy and confidentiality in relation to fundraising activities.

The Privacy Office Website

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](http://hipaa.ucsf.edu) for a host of resources and information. Find training guides, policies and procedures, forms, research and IT Security guidance, HIPAA FAQs, the Privacy and Confidentiality Handbook, the Notice of Privacy Practices, UCSF privacy news and newsletters, resources and links, and contact information, all designed to help you protect our patients’ medical, personal, and sensitive information.