Privacy Breaches Make Headlines – The Value of Encryption

Healthcare data breaches are on the rise. The Ponemon Institute reports in its 2011 Benchmark Study on Patient Privacy that the frequency of reported data breaches has increased 32% from 2010. Theft and loss of electronic devices is the leading cause of data breaches. Widespread use of unsecured mobile devices along with vendor and employee mistakes have compromised patient privacy and are contributing to medical identity theft. The most notable privacy breaches for the fourth quarter of 2011 all involved electronic devices:

<table>
<thead>
<tr>
<th>Who &amp; What</th>
<th># Affected Individuals</th>
<th>Data Exposed</th>
<th>Outcome To Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRICARE: Unencrypted backup computer tapes were stolen from the vehicle of an employee of Science Applications International Corp. (SAIC), a contractor for TRICARE. TRICARE provides health benefits for military personnel and retirees.</td>
<td>4.9 Million</td>
<td>Name, SSN, DOB, phone, address, health information</td>
<td>Patient and agency notification; call center; media coverage; website statement; credit monitoring and restoration services; questionig by federal authorities; $4.9B class action lawsuits against DoD and SAIC</td>
</tr>
<tr>
<td>Sutter: An unencrypted desktop computer was stolen from the administrative offices of Sutter Health affiliate Sutter Medical Foundation.</td>
<td>4.2 Million</td>
<td>Name, DOB, MRN, address, email address, phone, health insurance plan (for 3.3 million) In addition to the above, date of service, health information (for an additional 943,000)</td>
<td>Patient and agency notification; call center; media coverage; website statement; $4.2B class action lawsuits against Sutter Medical Foundation and Sutter Health</td>
</tr>
<tr>
<td>UCLA: An external hard drive was stolen from a physician’s home. Although the drive was encrypted, a piece of paper with the password was sitting nearby and was also taken, thereby rendering the encryption useless.</td>
<td>16,288</td>
<td>Name, DOB, MRN, address, health information</td>
<td>Patient and agency notification; media coverage; website statement; identity theft and restoration services</td>
</tr>
</tbody>
</table>

As these incidents show, a single breach of electronic patient information can be devastating. The Ponemon Institute reported that the average economic impact of a data breach is $2.2 Million. Encryption is the only federally recognized method for securing electronic patient information and therefore is the gold standard for protection of patient data residing on electronic devices or moving through hyperspace. This should give you pause to stop and think – are all your electronic devices encrypted? If not, contact the UCSF IT Service Desk to obtain instruction for encrypting your devices.

OCR HIPAA Audits are Underway

In June, The Office for Civil Rights awarded a $9.2 million contract to KPMG to conduct HIPAA audits in an effort to meet the requirement of the American Recovery and Reinvestment Act of 2009. On November 4, the program launched with audit notification letters being mailed to the first five entities chosen for audit. Up to 150 covered entities and business associates will be audited during the pilot phase of the program, which runs from November 2011 – April 2012.
Secure Email Features You Should Know

Federal law and University policy requires that you secure electronic messages containing protected health information. UCSF’s secure email solution ensures confidentiality by placing the message on an encrypted server that requires login for the recipient to view. Instructions for using secure email can be found on the ITS website: http://its.ucsf.edu/main/171-DSY.html. Below are some helpful system features that you may be unaware of:

- **Trigger Words:** The secure email system is activated by you when you enter specific trigger words at the beginning of the subject line. Triggers include “ePHI:”, “PHI:”, and “Secure:”. The colons are critical; capitalization is not. Trigger words are stripped from the subject line when the recipient receives the message and are not automatically added back to the subject line when the recipient replies. Thus, each time you reply to an external message, or forward a message externally, you must re-activate the secure email system by adding a trigger word to the subject line. This applies even when the email string had been previously secured, as each message is secured individually.

- **Your Secure Email Box:** Every system user is provided with their own secure mailbox for managing secure messages they’ve sent and received. This mailbox is accessible at https://smmcb01.ucsfmedicalcenter.org/messenger. Once you log in, you will be able to view your Inbox and Sent Items. Here, you can see the date messages were sent, their expiration date, and tracking details. A tracking status of “sent” means that the message has been successfully sent to the recipient; “received” means that the recipient has successfully logged into their secure mailbox and retrieved (viewed) the message; “recalled” means that the sender has successfully recalled a message (more on this below).

- **Recalling a Sent Message:** Secure messages inadvertently sent to the wrong individual or with the wrong attachments can be recalled. Simply login to your secure mailbox, open the sent message, and click the “Recall” button. Before recalling a message, check the tracking status to ensure it has not yet been viewed by the Recipient. Recalling a message deletes the message entirely from the Recipient’s secure mailbox, such that the Recipient is unable to retrieve it. This functionality can be a lifesaver in preventing privacy breaches. Contact the Privacy Office for guidance if you’ve sent an email to the wrong individual.

For answers to questions regarding secure email functionality, contact the UCSF IT Service Desk.

**UCSF Launches Telehealth Network**

The UCSF Telehealth team has recently rolled out the UCSF Telehealth network which when combined with secure end-points allows for live video consultations between health professionals and patients. This group supports UCSF-wide telehealth programs and initiatives. Telehealth includes videoconferencing, transmission of still images, e-health including patient portals, remote monitoring of vital signs, continuing medical education, encounter management and mobile health applications. This team works closely with Security, Privacy, Risk and Legal to ensure all UCSF Telehealth programs are secure, compliant and following best practices. We offer consulting, training and support for:

---

For more information visit http://hipaa.ucsf.edu or email the Privacy Office at privacy@ucsf.edu
Recent Social Media Privacy Breaches

- Tri-City Medical Center: 5 RNs were fired for discussing patients on Facebook
- Westerly Hospital: An MD was fired, fined, and reprimanded by the state medical board for posting information online about a trauma patient, even though the posting did not include the patient's name.

Navigating Social Media Responsibly

As healthcare workers, we’re often bombarded with confidential information every day. And the patients we care for trust that we'll protect their information. With the advent of new technologies and pervasive social media, it’s more important than ever to be aware of who our audience is and what information we’re sharing with them.

Even subtle information sharing carries the risk of unauthorized disclosure of information. While posting a photo of a patient without consent is a clear no-no, consider an informal blog post discussing an interesting case, where no names are mentioned. We must remember that 1 of the 18 HIPAA identifiers includes “any other unique” information. A rare disease or discussion of a patient’s particular situation could lead to the identification of the patient. Likewise, a breach can occur when seemingly de-identified information is combined with publicly available information, resulting in identification of the patient.

UCSF recognizes the value of social media to connect with audiences worldwide; to encourage patients to become active participants in their own healthcare; and to foster collaboration, innovation, and thought leadership. In order to ensure consistent and accurate representation of the University, and to remind users of their responsibility to adhere to applicable policies and laws, UCSF has developed social media guidelines and best practices. You’ll also find a social media overview, a bevy of resources, and links to UCSF’s social media pages at http://www.ucsf.edu/about/social-media-overview.

Cross Before You Toss?

It’s all too easy to grab that extra fax and toss it in the garbage. But did it contain PHI? If so, it must be disposed of properly into a secure shredding bin. If you need a bin, ask your Manager to order one from Environmental Services. What about a patient label on an empty IV bag?

You might be tempted to use a Sharpie to cross out PHI before tossing the bag into the garbage. However, this is not sufficient, as patient information may still be visible through the permanent ink overlay. Instead, use a black-out label. These labels are designed to completely cover the original label and conceal any PHI from both sides. They’re easy to use, and take just a moment to peel and stick. Material Services maintains an inventory of black-out labels in various sizes and styles. Ask your Manager for a sheet or roll and carry them with you.

Provider Notes: How to Protect Yourself and Your Patients

Provider notes, logs, and worksheets are a critical tool used daily by doctors, residents, nurses, and other care providers to organize their time and efforts, to keep track of patients, to note particular patient needs or concerns, and to remind themselves of “to-dos”, among other things. Often times, these notes are quickly handwritten on a sheet of paper that can be carried in their pocket while working a shift or making rounds. However, due to the inherent sensitivity of the information they contain, they present a risk for breach of privacy should they be lost, stolen, or accidentally thrown in the trash bin instead of shredded. Below are some simple guidelines designed to help protect providers and the patients they care for.

For more information visit http://hipaa.ucsf.edu or email the Privacy Office at privacy@ucsf.edu
- Write down only the minimum necessary (i.e. avoid additional identifiers such as age, sex, MRN, and detailed medical information)
- Use only first and last initial to identify patients
- If there is a need to distinguish between two patients with the same initials, use additional letters of the first name or full first name, but avoid using full last name. If necessary to further distinguish, consider room numbers or the last 4 of the MRN.
- Avoid including your name or your colleague’s name
- Ensure paper is blank (do not use letterhead or scrap paper which may have the name of the facility, clinic, provider, or other information already printed on it). If using a prepared template, review it to ensure it does not prompt for patient or provider names and limits information to the minimum necessary.
- Consider using brightly colored paper to help prevent loss
- Keep your notes on you at all times; avoid putting them down while doing something else as you may forget to pick them up again
- Consider carrying notes in a closed folder or envelope, or writing them in a notepad, notebook, or binder (as opposed to carrying loose sheets of paper) so that they aren’t so easily viewed by others, forgotten, misplaced, or lost. However, if using a notebook, remember to remove and shred pages as soon as they are no longer needed, so information does not accrue over time in the binder.
- Never remove notes from the facility
- Make it standard procedure to shred the worksheets as soon as they are no longer needed (implementing this as an end-of-shift or end-of-day procedure is best practice)

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 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.