How does the HIPAA Privacy Rule Apply When Reporting to Avert Threats to Health/Safety?

In the wake of recent mass shootings in our nation, the Department of Health and Human Services recently released an important reminder that, “The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule does not prevent your ability to disclose necessary information about a patient to law enforcement, family members of the patient, or other persons, when you believe the patient presents a serious danger to himself or other people.”

To review the complete guidance, please visit: http://www.hhs.gov/ocr/office/letteronationhcp.pdf

Privacy Breaches Make Headlines: Kaiser Patient Files Stored in Private Home

Kaiser Permanente recently made headlines during a federal and state investigation revolving around confidential patient files stored in a private home. According to the Los Angeles Times, a small home business was hired by Kaiser to store confidential hospital files. The number of files stored by the home business, Sure File, reached nearly 300,000 and included protected health information (PHI) of thousands of patients.

Sure File held files for approximately seven months with no contract in place. In addition to storing records in a shared warehouse space, PHI for thousands of Kaiser patients was also stored on home computers. Kaiser claims that Sure File left several hard drives containing PHI in their home garage, with an open door. In December 2012, the California Department of Public Health determined that Kaiser had “failed to safeguard all patients’ medical records.”

While federal and state officials continue to investigate the matter, Kaiser is suing the business owners. However, a state judge recently denied Kaiser’s request to access Sure File’s personal computers and email accounts.

How can you avoid similar situations at UCSF? Follow established policies and practices. At UCSF, all vendors must go through the procurement process. If PHI is involved, the Procurement Office obtains the Business Associate Agreement, which holds the vendor responsible to protect the PHI. Additionally, IT performs a Security Risk Assessment, which identifies any gaps in the security of the data while in transit and at rest.

For additional guidance, please visit the Business Contracts BAA sections at: http://sc/forms_policies
Information Security Corner:

Pagers: If You Use a Pager, What You Need to Know...

Did you know that texting is not secure? In our increasingly busy lives, quick and easy methods for communicating have become the norm. Use of text pages and text messages to send patient and provider queries or updates is not uncommon. These communications are not secure and could result in sensitive information falling into the wrong hands through interception. Such communications are often relied on to achieve the improved patient care UCSF seeks as a world class health care organization. However, only a fraction of personnel realize the underlying risks these mobile devices present.

Text messages sent from mobile devices (such as pagers, phones, and tablets) are sent in the form of radio frequency waves that anyone can read with the right tools. Carefully crafted equipment could capture the information and use it maliciously.

"PHI isn’t exactly worth its weight in gold, but it gives a secondary precious metal such as silver a run for its money. Experts generally agree that the sale of a single patient record will net around $50. That compares to just $1 for a viable Social Security number" (AIS Health Staff, 2012).

There are instances where PHI must be sent in plain text for purposes such as patient care. Below are some helpful guidelines to follow:

- Report a lost, stolen, or misplaced pager immediately to the UC Police
- Delete the message as soon as possible (these are stored in plain text on the pager)
- Limit the use of patient identifiers (e.g. instead of first and last name, use initials only)
- Do not identify the message as coming from or to UCSF
- You may use the room number
- You may provide some health information

For example: “Pt RW in room 1422 has a BP of 85/45. Rob, 3-1234”

These are recommendations and may not be practical in all circumstances. Patient care and safety comes first, but please remember that patient privacy is also critical.

Reference: AIS Health Staff. (2012). A driver of some privacy breaches, the market for stolen PHI is strong. AIS Health, 12(11), Retrieved from http://aishealth.com/archive/hipaa11112-04
Mobile Devices and Apps: Is Your App Secure??

Did you know that only a few apps have been approved by UCSF for use with protected health information (PHI)?

Reference apps, such as Medscape and Epocrates, don’t present a risk, and may be used freely. Haiku and Canto for the iPhone and iPad, respectively, are approved for handling PHI on mobile devices. All other apps require approval by IT Security, who help ensure the app is safe and data is protected appropriately. While numerous regulations and policies govern PHI, we also have a duty to protect the privacy of our patients’ information. If you are interested in using an app that uses PHI, contact the appropriate IT department (e.g., Campus ITS or Medical Center IT Security).

As a reminder, UCSF policy requires that smartphones and tablets used for UCSF and UCSF Medical Center business must be connected to the UCSF email system, which enables the required security controls. Contact the Service Desk at 514-4100 or see http://it.ucsf.edu/services/email-mobile-access for detailed instructions.

APeX Faxing: How to Avoid Privacy Breaches

As part of the APeX rollout, clinical documentation is now being faxed electronically via APeX RightFax. This means less snail mail and manual faxing, and that providers receive their patient’s health information immediately.

Did you know?

Below is just a sampling of the documents being faxed today:

- Consult Letters
- Progress Notes
- Notifications of Admission and Discharge
- Discharge Summaries
- Operative Reports

It’s more important than ever to ensure that provider contact information listed in the patient’s record is accurate, as correspondence is auto-faxed to those providers, including the PCP and referring provider listed in the patient’s Care Team. Faxes sent to the incorrect provider are reviewed by the Privacy Office and the affected Department, which may result in a privacy breach notification to the affected patient(s), California Department of Public Health (CDPH), and/or the Department of Health and Human Services (DHHS).

Tips to ensure that provider information is entered accurately:

1. Review complete provider information with the patient at scheduling, rescheduling, check-in and/or admission. Update the information if the provider has changed or the information is inaccurate.

2. When selecting providers in APeX, be sure to verify:
   a. Full name (including first, last, and middle)
   b. Specialty (does it match the patient and their encounter?)
   c. Address (including the street, city, and state)
   d. Phone number
   e. Fax number (area codes can provide a quick tip-off)

Comparing these details against the paper Referral or Order, or reviewing them with the patient improves accuracy and prevents misdirected faxes because: 1) the correct provider is selected, especially in cases where the provider has a common name or one similar to another provider or UCSF workforce member; and 2) the fax is sent to the provider at his/her correct location when a provider has recently moved or has multiple practice locations.

3. When searching for providers in APeX, remember that “less is more”. Use minimal letters in your search string, which will bring up a more complete list of possible matches, with detailed contact information that will help to distinguish between similar and same name providers.

For more information visit http://hipaa.ucsf.edu or email the Privacy Office at privacy@ucsf.edu
4. If the patient does not have a PCP or referring provider, enter “NO, PCP” or “NO, REFERRING”. Do not type “No”, “None”, or “Self”, as these search strings default to external providers, such as Dr. No. Take a moment to verify that you’ve selected the correct provider before signing and sending the letter.

5. Note that the Referring Provider fields will not accept the name of a UCSF Resident or Fellow. You must instead enter the name of the Attending. Because the field doesn’t accept Residents, your search for a Resident’s name may default to an external provider. Use caution when filling out this field.

6. When routing letters in APeX, you may rely on the fact that members of the Care Team have been verified by front line staff, and that addressing letters to members of the Care Team will help to avoid blunders. Make use of the PCP and Referring Provider buttons, which pull recipients from the Care Team and Appointments. Avoid the “Previous”, “All Referring” or “Last” recipient buttons in APeX, unless you verify each recipient for accuracy prior to sending the letter.

Remember: If you become aware of or suspect a misdirected fax, report the incident to the Privacy Office immediately at (415) 353-2750.

Human Research Protection Tip Center

Did you know…?

✦ The UCSF Subject Authorization for Release of PHI for Research is available in 20 languages?
✦ The Experimental Subject’s Bill of Rights is available in 27 languages?

Use these forms when consenting non-English speaking subjects, and remember to check the HRPP website for the most recent guidance here: http://www.research.ucsf.edu/chr/Guide/chrG_SpSpeakWrite.asp

Accounting of Disclosures: Guidance and Process

Under HIPAA, there are limited circumstances whereby identifiable patient health information may be released without patient authorization, such as when mandated by state and federal law. As patients have a right to receive a written accounting of these types of disclosures for the six years prior to the date of their request, these disclosures must be tracked by UCSF in order to provide these reports to patients.

UCSF uses APeX Quick Disclosure and eDisclose to track the releases of these types of releases, including disclosures to public health agencies for purposes of reporting communicable diseases, cancer/tumor registries, victims of abuse, neglect, or violence, and other disclosures required by law. However, HIPAA excludes certain types of disclosures from the accounting of disclosure requirement, such as releases for the purposes of treatment, payment, healthcare operations or disclosures authorized by the patient. If you release patient information, you may be required to account for the disclosure in Quick Disclosure. Note that if you obtain patient authorization for the disclosure or if the information to be released is de-identified, then you do not need to do an accounting for the disclosure. For more detailed guidance (including which disclosures need to be accounted for, and how), please visit the accounting of disclosures section of the APeX Knowledge Bank at the following link: http://myapex.ucsf.edu/kb/HIM_Resources.htm

Privacy Reminders

Report Lost or Stolen Property to UCPD: If you are alerted to lost or stolen UCSF information or devices, immediately report the incident to the UCSF PD at (415) 476-1414. This includes “paper copy” forms such as binders, files, films, x-rays, folders, or photos in addition to electronic devices such as laptops and iPads.

Safeguard Mobile Devices from Theft: One of the hazards of smartphones and tablets is that they are popular targets for thieves. While they have a high resale value and are expensive for the victim to replace, the greatest cost comes if a lost or stolen device contains PHI. The financial and reputational cost to UCSF, and to the individual user, can be staggering. Find out how to protect yourself and UCSF by visiting http://tiny.ucsf.edu/losttheft.

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