Importance of Timely Privacy Incident Reporting

We all know that the unauthorized access, use or disclosure of patient information can have a harmful impact on our patients, their care, and on UCSF. Privacy incidents involving patients’ health data affect their trust and relationship with UCSF. There are also State and Federal laws that may be violated due to a privacy incident, and UCSF (and in some cases, the responsible staff) may be held accountable.

While we as a community do our very best to avoid privacy incidents involving patient information through our vigilance and training, we also understand that privacy incidents happen. Per State law, UCSF has only 15 days from the date of the initial notice of a privacy incident to mitigate any harm to the patient, investigate the root cause of the incident, initiate staff remediation, and ensure that the patient and the California Department of Public Health (CDPH) State are notified.

Delays in notification will result in fines levied against UCSF by the State ($100/day for each day beyond the deadline), potential reputational harm to UCSF, and increased risk to the affected patient(s).

Therefore, if a privacy incident occurs, it is critical that the Privacy Office is notified as soon as possible so that prompt action can be taken to initiate the investigation and mitigation process. If you are aware of or suspect any inappropriate use or disclosure of PHI, please report the privacy incident to your supervisor or to the Privacy Office at 415-353-2750 or at privacy@ucsf.edu. Please refer to the UCSF Privacy Investigation Policy: 200-30 for additional information.

The General Data Protection Regulation (GDPR) Is Here

Have you heard? The European Union General Data Protection Regulation (GDPR) went into effect on May 25, 2018. The GDPR seeks to protect individual data privacy and applies to a broad range of data elements collected about “natural persons.” It addresses multiple issues, such as the rights of data subjects, consent, and purpose of use.

UCSF must comply with the GDPR to the degree that the university collects, processes, and stewards data about people protected under the GDPR. Guidance information from the Privacy Office will be forthcoming and will include advisory documents from UCOP, inventory tools, and planned dates for information sessions on GDPR. Visit https://hipaa.ucsf.edu/gdpr for more information.

Kudos Korner: Urology Faculty Practice

The Privacy Office would like to recognize Chris Brieze (Practice Manager, Urology Faculty Practice) for being a Privacy Advocate by providing detailed privacy educational materials and training to his staff. Thank you, Chris, for disseminating best practices on protecting patient privacy.

Looking for some tips to share with staff during a huddle or team meeting? Check out the Resources section of the Privacy Office website for tip sheets, FAQs, and past editions of the Privacy Beat: http://hipaa.ucsf.edu/workforce-resources-and-guidance.
De-Identification Validation Service

The IT Enterprise Information & Analytics (IEIA) and Clinical & Translational Sciences Institute (CTSI) departments have partnered with the UCSF Privacy Office to start a new service offering data de-identification validation testing. The goal of this service is to help the UCSF Community obtain certification that their de-identified patient data sets have been de-identified in accordance with HIPAA regulations.

Through this new service, you will:

- Collaborate with the CTSI Consultation Services Data Management team to evaluate the characteristics of your data set, such as size, complexity, data type, data sharing plans, etc. to help you identify the best resource to perform the data de-identification validation testing for your data set.
- Partner with a subject matter expert on the data de-identification validation testing of your data set to probe, profile, and review your data set to determine whether all Protected Health Information (PHI) has been removed from the data set in accordance with the HIPAA Safe Harbor standard during the initial pilot of this service. These validation testing services will be provided by both the Academic Research Systems team and external consulting and privacy analytics firms on a fee-for-service basis.

To submit a data de-identification validation request, please visit http://accelerate.ucsf.edu/consult/data.

To learn more about this service, please visit https://data.ucsf.edu/data-assets/de-identification.

Protect Your Password

As a global leader in health sciences, UCSF is often the target of sophisticated cyberattacks, and strong passwords are essential to securing you, your data, and UCSF. Strengthening your passwords and password management practices is one way you can actively help create a more secure work environment at UCSF. Following these best practices will ensure you have a strong password for every account.

- Instead of just a word, use a phrase or sentence at least 12 characters long
- Strive for complexity - use a combination of upper and lowercase letters, numbers, and symbols
- Make it something known only to you (not publicly available information) but still easy to remember
- Use separate, unique passwords/passphrases for each of your accounts

Please visit www.it.ucsf.edu/password for additional password security tips.

Privacy Quiz Winner

Congratulations to the winner of our Winter 2018 Privacy Quiz, Jill Grochowski of the UCSF Department of Cytology. We hope you enjoy your gift card.

Updated HIPAA Business Associate Policy: UCSF Campus Policy 200-28

In March, UCSF’s Campus Policy on HIPAA Business Associates was updated to include the following revisions:

- Added reference to HITECH Act (Health Information Technology for Economic and Clinical Health)
- Updated definition of Protected Health Information (PHI)
- Aligned formatting and flow to more closely mirror the UCSF Medical Center Policy 1.02.15: HIPAA Business Associates (Updated September 2017)

A Business Associate Agreement (BAA) is required whenever another person or entity outside of UCSF’s workforce performs functions or activities, or provides services to, UCSF that would involve access to PHI.

Are you thinking about working with a vendor to process or store UCSF PHI? Do you want to purchase a tool or software for your research study that would require uploading PHI? Help protect our patients’ data and avoid HIPAA violations by ensuring a BAA is in place for these activities. For more information, visit the Supply Chain Management website (https://supplychain.ucsf.edu/hipaa) or contact the Privacy Office (privacy@ucsf.edu).