Social Media and Confidentiality: How to #Hashtag and Snap, Compliantly

Are you active on social media platforms? Think twice before Tweeting, Snapchatting or Instagramming content that references your work at UCSF. Without the use of appropriate safeguards, posting on social media poses potential risks to the private information of patients, workforce members and staff alike. Below are best practice guidelines for creating social media posts that are compliant with UCSF policy and state and federal privacy and consent laws.

Do not post photos, videos or information about others without their consent, including students, colleagues, visitors or patients.

Social media networks are expansive – you might not know who in your network knows who. Even if you do not disclose a person’s name in a post, if there is enough information that at least one person could identify the subject of the post, it could be a violation of that person’s privacy and a potential violation of HIPAA.

Keep in mind that even if you try to “de-identify” information about an individual in the content of your post, colleagues or friends who respond to your post in the comments might contribute additional facts or identifiers that would allow the subject of the post to be re-identified.

Posting photos of documents, work schedules and even workspaces could expose private or confidential information. Be mindful of what is depicted in your photos and take care to double-check if you might have captured something in the background that has protected health information (PHI) or other confidential data.

For best practices on posting on a personal social media account, visit https://www.ucsf.edu/about/social-media-best-practices.

For guidelines on posting on a UCSF-hosted or branded social media account, visit https://www.ucsf.edu/about/social-media-guidelines.

---

Proactive Monitoring of EHR—Discouraging the Use of APeX for Snooping or Other Non-TPO Actions

As responsible stewards of UCSF data, we know the Health Insurance Portability and Accountability Act (HIPAA) and the California Medical Information Act (CMIA) require us to protect the privacy and security of patient health information (PHI) and to adhere to the “minimum necessary” standard for use and disclosure of PHI.

One of the ways the UCSF Privacy Office protects PHI is by monitoring for and discouraging unauthorized access to patient information stored in clinical systems such as APeX. Unauthorized access includes the inappropriate review or viewing of patient medical information without a direct need for diagnosis, treatment, or other lawful use.

An example of such access may be “snooping” on your co-workers’ or neighbors’ patient records. APeX and other clinical systems produce audit logs for any access into patient records which may be monitored and flagged for potentially inappropriate access. These flagged incidents are reviewed by the Privacy Office to determine whether a violation has occurred.

Privacy violations carry penalties under federal and state laws as well as UC policies, and may lead to disciplinary action. When in doubt, it’s always helpful to ask yourself if your access to clinical records is the “minimum necessary” to perform your work!
Are You Transmitting PHI Without a BAA?

It is a legal requirement of HIPAA regulations that a Business Associate Agreement (BAA) be in place between two parties transmitting Protected Health Information (PHI) for purposes other than treatment. The Covered Entity (UCSF) and the Business Associate (3rd party vendor) must agree to and sign the BAA before transmitting any PHI.

At UCSF, we are always on the cutting edge of technology and exciting new innovations. Sometimes it is tempting to begin transmitting data/PHI before a BAA is in place. Don’t fall prey to this temptation as it creates an unnecessary risk for UCSF!

We could be subject to costly fines, penalties, reporting obligations, or reputational damage, should PHI be transmitted without an executed BAA. As an example, Advanced Care Hospitalists PL (ACH) has agreed to pay $500,000 to the Office of Civil Rights at the U.S. Department of Health and Human Services (HHS) for an alleged violation of HIPAA. OCR found that ACH impropriously disclosed the PHI of 9,255 of its patients to a third party vendor for billing processing services without the protections of a BAA in place. The PHI was later found on the vendor’s website. Additional information about this case can be found here.

If you are unsure whether a BAA has been executed or if a BAA is required, contact your appropriate UCSF Procurement Office. Be Safe. Avoid Fines. Ensure a BAA is in place.

Protect UCSF Data on Removable Storage Devices Using Dell Data Protection Encryption

That free USB drive in your pocket could be a very expensive thing to lose! The loss of unencrypted UCSF data can expose you and UCSF to costly fines, intellectual property theft, and could result in a loss of public trust in UCSF.

While UC policy requires encrypting any sensitive or restricted data on external storage devices, UCSF strongly recommends that Campus and Medical Center users encrypt all UCSF data as a default, regardless of sensitivity. The benefits of encrypting all UCSF data is that you don’t need to consult rules about data categories and you can reduce the potential risk of a data breach. In addition, Medical Center users have been using mandatory external drive encryption for two years without any major disruptions or issues.

Even if you do not work with electronic Protected Health Information (ePHI), there are other types of sensitive or restricted data that should be kept from unauthorized persons. This includes, but is not limited to, contracts, payroll information, unpublished research data, building or network diagrams, etc.

See https://it.ucsf.edu/policies/dataclassification for additional information on classes of data at UCSF.

UCSF Privacy strongly recommends that all UCSF data be encrypted, regardless of sensitivity.

Thankfully, you can easily secure data on external drives by encrypting it with Dell Data Protection Encryption (DDPE) Removable Storage Encryption. You can also use any of the hardware-encrypted removable drives listed here: http://tiny.ucsf.edu/securityproducts.

When you enable Removable Storage Encryption on a device like a USB hard drive or flash drive, DDPE encrypts new files that are copied from a UCSF computer to the drive. You can read and write encrypted data on the drive from any computer, even if it does not have DDPE installed. DDPE Removable Storage Encryption is file-based encryption and is compatible with both Windows and macOS, so you can read and write encrypted data from both platforms.

For more information, please visit: https://it.ucsf.edu/services/removable-storage-encryption.

Prezi Incident

Written by Tom Poon, Interim Chief Privacy Officer and Patrick Phelan, Chief Information Security Officer

Recently, a UCSF patient discovered their protected health information (PHI) on the internet for all to see. A former UCSF resident used an online presentation tool called Prezi and inadvertently made the presentation publicly available.

While there are many useful free or low-cost cloud services, it is not appropriate to use them with restricted or confidential UCSF data (e.g., patient health information, student information, etc.). When you agree to the service provider’s terms of use, you are putting UCSF data in the service provider’s hands without the necessary UCSF contractual assurances or a federally required HIPAA Business Associate Agreement. If you agree to the terms of a “click-through agreement” without consulting the appropriate internal department(s), you may be held personally responsible for the terms of the agreement. The fines levied for inappropriate disclosures of patient health information can be as high as $1.5 million per incident. Continued on Page 3.
Prezi Incident (cont’d)

If you are using Prezi or a similar service, discontinue its use and remove any UCSF data from the service immediately. Instead, use UCSF-sanctioned services/software like Box, PowerPoint, or Keynote. When dealing with patient health information, follow HIPAA’s “minimum necessary” requirement.

Minimum necessary means limiting the use or disclosure of, and requests for, protected health information to the minimum necessary to accomplish the intended purpose (i.e., remove names, MRNs, and other identifiers that are not needed).

We understand the appeal of free and low-cost cloud services, but the risks to UCSF data and the privacy of our student and patients’ health information outweigh the perceived benefits of such services.

Delegated Signature Authority

There has been a recent increase in UCSF employees without Delegated Signature Authority entering into contracts on behalf of UCSF. This can put UCSF at risk.

**What is Delegated Signature Authority?** The Board of Regents of the University of California gives decision-making authority to the UC President via the Standing Orders of the Regents. The UC Presidential Delegations of Authority (which includes Delegated Signature Authority) are maintained at the Office of the President. The President may re-delegate some of his/her authority to Chancellors and other UC officers through UC policy, Business and Finance Bulletins, or letters of delegation.

As with other Presidential Delegations of Authority, UCOP delegations of authority specify to whom authority has been delegated and the scope of the authority. The President delegates authority to a direct report, who then (if allowed) may re-delegate that authority to a direct report, and so on. The same principle applies for delegation of signature authority and with applicable laws, regulations, and University policies. See [https://www.ucop.edu/business-resource-center/policies-and-guidance/guidelines/delegations-of-authority.html](https://www.ucop.edu/business-resource-center/policies-and-guidance/guidelines/delegations-of-authority.html)

**What happens if I sign a contract and I don’t have Delegated Signature Authority?** If the contract is not properly executed, it is not considered to be valid and may be voidable. This may further delay your project or purchase. You may have executed a contract on behalf of the University with terms that we may not be able to meet or that we cannot accept. This puts the University at unnecessary risk with the potential need to expend additional time/fees for legal representation. If the individual who has not been delegated purchasing authority makes an unauthorized purchase for goods or services, they shall be responsible for payment of the charges incurred (BUS 43: [https://policy.ucop.edu/doc/3220485/BFB-BUS-43](https://policy.ucop.edu/doc/3220485/BFB-BUS-43)).

To save yourself time in the long run and to decrease risk, please work with your appropriate UCSF Procurement Office or Contract Office to ensure contracts and purchases are executed properly.

The UCSF Office of Legal Affairs is setting up a task force to address and record the delegation of signature authority, so check back in the future for updates.

National Cybersecurity Awareness Month:
Enterprise Outreach

October was National Cybersecurity Awareness Month. The UCSF IT Security and Privacy Awareness Training Team (ITSPATT), led by Esther Silver, was at BCHO, Parnassus, Mission Bay and ZSFGH. Staff and students won many prizes and lots of candy by completing a short quiz on cybersecurity and privacy topics. The U.S. Dept. of Homeland Security led program is designed to help us *Stay Safe Online*.

During the holiday season, the ITSPATT team would like you to stay safe while online shopping. For details visit [https://it.ucsf.edu/news/don%20%E2%80%99t-get-more-you-bargained-holiday-season](https://it.ucsf.edu/news/don%20%E2%80%99t-get-more-you-bargained-holiday-season).

Left to right: Nelson Lee, Owen Buckvar, Esther Silver, Christopher Yip, Qian Dong Li