UC DAVIS HEALTH | Compliance Connection

Summer 2024, vol. 4

ENCOURAGING AND REINFORCING PATIENT PRIVACY IS EVERYONE'S RESPONSIBILITY

Do you have a responsibility to ensure patient privacy at UC Davis Health? Hopefully, your immediate response was a confident and enthusiastic "Yes!" From the time of hire as a new employee, employees learn about our Privacy Program. In addition, on an annual basis all employees must take Privacy and Security training in the online learning management system (LMS).

This training module assists employees in their understanding of state privacy laws and the Health Insurance Portability and Accountability Act (HIPAA) which requires us to ensure our workforce understands the importance of complying with these laws and the consequences of failing to do so. This training provides foundational awareness of the importance of your role and your responsibilities in securing our patients' medical information. In addition to training, promoting a culture of privacy at UCDH is essential to safeguarding our patients' personal information.

How do we build that culture within our departments? Working within a healthcare environment requires us to interact with sensitive Protected Health Information (PHI) on a daily basis. Together, we can accomplish a culture of privacy within our departments by encouraging, reinforcing, and discussing compliant behaviors such as:

- Never sharing or using another employee's password;
- Properly logging out of your workstation, especially if you use a shared workspace;
- Using the minimum necessary information when discussing or accessing patient information;
- Utilizing secure Shred-it bins when disposing of PHI;
- Properly securing devices that contain sensitive information; and
- Ensuring all access to PHI is for the purpose of performing your assigned work-related tasks associated with the treatment, payment for treatment, or healthcare operations related to the patient in question.

We encourage consistent discussions and reminders that reinforce these behaviors in your department. It is important that all staff understand the need to report potential privacy violations immediately. While we aim to mitigate any privacy concerns through training and creating a work environment that fosters a culture of privacy, we do have appropriate internal steps to address privacy concerns when they arise.

What are the consequences of noncompliance? When privacy concerns are raised to our office, we review and investigate these concerns. When conducting investigations into potentially unauthorized access to or a breach of a patient's medical information, we are often given these common reasons for the access or breach:

- "I was bored;"
- "My coworker asked me to access the record even though I am not directly involved in their care;"
- "I used it to obtain the contact information of someone I know;"
- "I did not know that it was against policy to look up my family members' records;" or
- "I thought I could look at my own record."

These explanations typically accompany findings of policy or privacy violations. Such findings may adversely impact your employment via the resulting corrective action, up to, and including termination. Furthermore, both you and UC Davis Health can potentially be fined for breaches of patient privacy. For supervisors, identified privacy concerns within your area should prompt reeducation efforts within your unit, not just for an employee deemed responsible for an incident, but for staff broadly. This helps to reinforce a culture of patient privacy in the workplace and identify areas of future improvement.

UC DAVIS HEALTH | Compliance Connection

THE IMPORTANCE OF USING ONLY APPROVED APPLICATIONS FOR WORK PURPOSES

At UC Davis Health, the need to effectively meet University goals is enhanced by the use of technology in the form of digital systems, tools, and applications. While the availability of a diverse range of technology can enhance productivity and efficiency, it also poses significant risks to the University, patients, and the workforce if improperly utilized. Ensuring that you, the workforce, use only approved applications for work purposes is crucial for maintaining security and privacy, compliance, and overall organizational productivity.

Enhancing Security and Privacy
Only enterprise-approved applications must be used. One of the primary reasons for this is to enhance the security and privacy of data. Approved applications have undergone rigorous vetting processes to identify and mitigate potential security vulnerabilities. This vetting process helps protect UC Davis Health from various cyber threats, such as malware, phishing attacks, and data breaches. By limiting technology use to only those that are approved, UC Davis Health can ensure that all data is managed within secure environments, reducing the risk of unauthorized access and data events.

Ensuring Compliance
As a regulated entity, UC Davis Health must adhere to many different sets of regulations and laws, such as the Health Insurance Portability and Accountability Act (HIPAA), the Confidentiality of Medical Information Act (CMIA), and the Information Practices Act (IPA), amongst others. These rules impose strict requirements on how data is managed and protected. Approved technology is chosen based on its ability to meet these varied regulatory standards. Using only approved technology ensures that UC Davis Health remains compliant with applicable laws and regulations, thereby at a minimum avoiding aggrieved patients, reputational harm, hefty fines, and legal consequences.

Promoting Productivity
While security and compliance are critical, using approved applications also promotes productivity. Standardizing the technology used at UC Davis Health reduces potential compatibility issues and ensures workflows make sense. You can collaborate more effectively when using the same set of tools, which are often integrated with other systems at UC Davis Health. Moreover, Innovation Technology (IT) teams can provide better support and maintenance for a standardized set of applications, leading to quicker resolution of issues and minimizing downtime.

Conclusion
In conclusion, the use of only approved technology for work purposes is vital at UC Davis Health. Doing so safeguards against security threats, ensures compliance with regulatory and legal requirements, and enhances overall productivity. This approach not only protects UC Davis Health assets but also supports a streamlined workflow, ultimately contributing to organizational success.

UC DAVIS HEALTH

Compliance Connection

RESEARCH COMPLIANCE TEAM TO CONDUCT AUDITS OF ONCORE CLINICAL TRIAL MANAGEMENT SYSTEM

The OnCore Clinical Trial Management System (CTMS) is an enterprise-wide technology for broadly managing clinical trials and other studies, to include study budgets and sponsor invoices, Medicare coverage analysis and billing grids, regulatory documents and regulatory reviews, subject management, and more. Additionally, OnCore interfaces with Epic to provide real-time updates to study information and research subject status information in Epic.

Phased implementation of OnCore occurred between 2021 and 2023, reaching full implementation at UC Davis Health in December 2023. As a result, the Clinical Trials Data Bridge (Bridge), a REDCap Database utilized at UC Davis Health since 2013 to create clinical trial records for upload to Epic, was retired in early 2024.

UC Davis Health Policy 2317, Documentation of Research Patient Status in the Electronic Medical Record, was updated in August 2023 to reflect workflow changes that resulted from the implementation of OnCore and the retirement of the Bridge. Following the policy updates, Compliance initiated audits that evaluated OnCore resources available to end users. Additionally, routine audits performed by the Research Compliance Program assess compliance with OnCore workflows described in UC Davis Health policies.

The UC Davis Health CTMS Operations Office distributed an advisory on July 29, 2024, instructing end-users to ensure subject management documentation is up to date and to ensure the documentation in OnCore aligns with information in Epic. The advisory was broadly distributed via the Clinical and Translational Science Center listserv, assigning a deadline of September 30, 2024, to complete the task. Compliance will initiate auditing and monitoring activities to assess policy compliance for OnCore use starting in October 2024.

Extra, Extra Read All About It!
Ethics & Compliance Week 2024 is coming!

Compliance is looking forward to celebrating Ethics & Compliance Week, November 3-9, 2024. Look for our Compliance staff throughout the UC Davis Health campus during the week. Get your ethics and compliance questions answered and meet the teams that are available to guide you on your ethics and compliance questions! Mark your calendars and stay tuned for more information.

Need to Reach out to Your Compliance Team?

Phone: 916-734-8808 **Fax:** 916-734-0222
Confidential Hotline: 1-800-403-4744

Compliance Help: hs-compliancehelp@ucdavis.edu
Research: hs-researchcompliance@ucdavis.edu
Rev Cycle: hs-codingbillingcompliance@ucdavis.edu
Privacy Team: hs-privacyprogram@ucdavis.edu
Website: http://health.ucdavis.edu/compliance