UC DAVIS HEALTH COMPLIANCE AND PRIVACY SERVICES NEWSLETTER

Volume 1, November 2023

COMPLIANCE HOT TOPICS

● UC Davis Health is pleased to announce the inaugural annual celebration of Ethics and Compliance Week, November 6 – 9, 2023. Details available here.

● Revised Code of Conduct – UC Davis Health released an updated Code of Conduct in August 2023 – Read it here!

Melinda Mendoza
Chief Compliance
and Privacy Officer

Safeguarding PHI from Hackers – Push Phishing

A Message from Your Privacy Compliance Team

The UC Davis Health network is a vital resource for treating patients and depended upon by thousands of care providers for life-saving services. The network is also a prized target for hackers. Healthcare records are more valuable on the black market than other types of data making our network a profitable target for hackers. There are many tactics used by hackers to try to infiltrate networks. One emerging tactic that hackers employ is called "push phishing," which can occur if a UC Davis Health workforce member's system credentials (username/password) have been compromised. The hackers then attempt to use the credentials to log in to the network and hope that the workforce member will simply approve an invalid Duo push request that is received. These push phishing attacks may be timed to arrive at the beginning of the day, end of the day, or when the workforce member has a lot of meetings so that fatigue and/or distraction may lower the ability to detect the invalid push request.

To guard against this, ask yourself the following questions if you receive a Duo push request that is unexpected or irregular:

1. **Did I just attempt to access a UC Davis Health application when the Duo push arrived?**
2. **Where is the Duo push request coming from? Check the location details provided with the push in the Duo Mobile application.**
3. **Is there anything unusual about the resource or application I am trying to access?**

With a goal of always securing confidential information, the DUO service is making updates in November 2023 to the push prompt screen and to cover ServiceNow.

Research Compliance Program Education and Outreach

A Message from Your Research Compliance Team

The **Research Billing Academy** restarts after a summer break. Upcoming educational events include a series on managing charges generated from conduct of research in the clinical setting. The Research Compliance Team will partner with Epic and OnCore staff to demystify research billing workflows, maximize the benefits from the OnCore-Epic integration, and fast-track expansion of your research billing subject matter expertise.

Virtual and in-person outreach events targeted toward **data security and data sharing** will occur during Ethics and Compliance week. Bring your questions and drop in for a chat with subject matter experts from Compliance and Privacy Services, the Data Center of Excellence, and the Clinical and Translational Science Center.

> **Tip**: Ensure signed consent and authorization are obtained before entering **protocol-directed orders** in Epic. A waiver of authorization for recruitment does not cover access to PHI for performing (or preparing for) study activities.

Drop us an email at HS-ResearchCompliance with your questions, concerns, and ideas or requests for education. We are available to present at your team or department meetings.

Compliance Policy Updates

- 2302, Clinical Database Access – The 8/2023 policy update combined Epic Clarity and Caboodle user access standards and requirements. The update also added an exception from standard filtering of sensitive groups' data with explicit Institutional Review Board approval.

- 2317, Documentation of Research Patient Status in the Electronic Medical Record – The 8/2023 policy update aligned the policy with the OnCore Clinical Trial Management System (CTMS) implementation practices and assists in facilitating new OnCore billing functionality. All research studies subject to the policy are now required to be entered into OnCore for deployed departments. New documentation and study linking requirements are required to further support CTMS implementation and functionality.

Compliance wants to hear from you! Please send us any topics you would like for us to focus on in our next issue.

Contact Us:
UC Davis Health, Compliance and Privacy Services
2335 Stockton Blvd.
Sacramento, CA 95817
916-734-8808
HS-compliance@ucdavis.edu
https://health.ucdavis.edu/compliance/