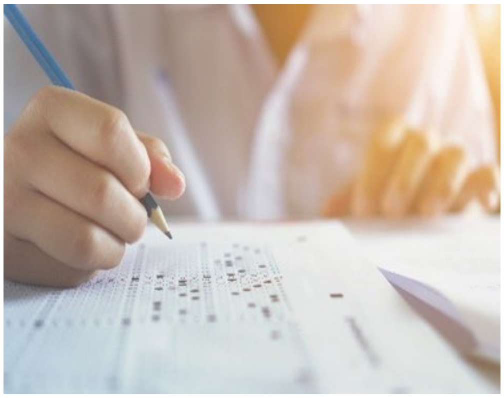
UC DAVIS HEALTH

Winter 2024

Compliance Connection

UC Davis Health Staff Appraisals: Mandatory



At UC Davis Health, as part of our ongoing commitment to professional growth, maintaining industry standards, and ensuring a safe and productive work environment, all employees are required to complete annual and bi-annual training.

Mandatory training includes: Privacy & Security Training, UC Abusive Conduct in the Workplace, UC General Compliance Briefing, UC Preventing Harassment and Discrimination, UC Cyber Security Awareness Fundamentals, Mandatory Annual Training ("MAT"), and Workplace Violence Prevention in Healthcare. Each UC Davis Health employees' staff appraisal requires that UC Davis Health Managers and Supervisors confirm each employee's completion of the mandatory trainings as part of the employee's appraisal.

UC Davis Health Policy 1007 states, "[s]upervisors and managers are responsible for ensuring their direct reports complete mandatory educational programs and training. Supervisors and managers who fail to do so will be held accountable and are subject to appropriate action."

In anticipation of the 2024 Annual Performance Appraisals, please take time to review the status of your staffs' mandatory training completions. You can do this by following these simple steps in the UC Learning Management System (LMS):

Exception Reports
Navigate to My Team > Manager Dashboard

● Locate the employee tile and click the number Incomplete. Your direct reports will auto-populate where you can see each employee's training status.

Advanced Reporting

- Navigate to Self > Reporting > Advanced Reporting

● Expand the folders to UCD Health and select the reports.

Each report can be exported and filtered by the designated manager's name for ease of identifying staff training compliance. Continued training ensures that UC Davis Health continues to provide the best possible care for our patients and the community. For additional information on accessing the LMS Manager Dashboard you can visit: Manager Role: Manager Dashboard (youtube.com).

Regulatory Corner

Generative AI
Generative artificial intelligence (AI) products like Chat GPT, Microsoft Copilot, and Bard offer use of cutting-edge large language model technology to create new content such as text, images, and videos by emulating patterns in existing data. While it is exciting to explore the potential of this new AI technology, when providing data to generative AI tools, caution is advised as many tools are untested and unregulated. The UC Davis Health Compliance Department recently published Guidelines for Using Generative AI. This guidance provides guidelines for using this new technology in the workplace and in the healthcare setting, including prohibitions on entering personal, confidential, or sensitive data unless a tool has been formally approved by the necessary UC Davis Health bodies. Considerations include:

- Never enter PHI into generative AI sites or applications, unless they have been explicitly approved by the institution for PHI.

Research

Did you know that research procedures may be ordered in Epic only after the research subject has signed the research informed consent form and the UC Davis Health HIPAA authorization form?

Researchers must have the patient's permission to access the medical record for research before entering orders required only for purposes of a research protocol. Patient permission is obtained when the patient or representative signs the research informed consent form and the UC Davis Health HIPAA authorization form.

Items and services necessary for the direct clinical management of a patient's health condition may be ordered as needed by the provider independent of any study being considered for the patient.

Study teams are encouraged to consult the IRB about engaging in remote informed consent if it is necessary to place orders and/or schedule procedures in Epic before inviting the potential research subject to meet the study team on site.

The standards described above ensure compliance with HIPAA, the Common Rule, and proper billing practices. UC Davis Health Policy 2317, Documentation of Research Patient Status in the Electronic Medical Record, maps out the workflow for researchers as follows:

III.C. 2. Each research subject must be linked to the study in the EMR in accordance with the following timeliness standards:

a. The subject must be linked to the study after the study's informed consent form (ICF) to participate in the research study is completed and signed,

b. The subject must be linked to the study before protocol-directed orders are entered in the EMR, and

c. The subject must be linked to the study before protocol-directed encounters are completed.

The Research Billing Academy is published in the UC Davis Clinical Research Guidebook.

A course catalog of available Research Billing Academy courses has been published in the Clinical Research Guidebook. Course recordings and PowerPoint slides for four Core Courses and six Intermediate Courses are available for review. Additional Research Billing Academy content is in development.

Introducing HS-ResearchBillingHelp@ucdavis.edu.

Have a question about billing or related functions and not sure who to contact? We're here to help.

Subject matter experts from OnCore IT, OnCore Operations, Epic Research, Patient Financial Services, and Compliance have established a shared email inbox for your billing-related questions. Emails received will be triaged and sent to the expert who can most readily assist you. We are looking forward to hearing from you.

Questions about this content or other research topics can be addressed to HS-ResearchCompliance@ucdavis.edu

Regulatory Corner con't.

- Output from these tools may not always be accurate.
- Be cautious of output which may contain potential biases - particularly those that may perpetuate social and health disparities.
- No-cost or low-cost generative AI tools should be approached with care, as they often come with terms and conditions that users need to review and comply with to ensure responsible and ethical usage. Workforce members could be held personally liable for violation of these terms.

For more details, please see the Guidelines for Using Generative AI in the Quick Links section of the Compliance and Privacy Services website: https://health.ucdavis.edu/compliance/about/ (Kerberos account needed.)

Open Payments

Did you know, the Physician Payments Sunshine Act is a national transparency program which collects and makes public financial relationship information between physicians, teaching hospitals and the manufacturers of drugs, medical devices, and biologics? This information is published on the CMS Open Payments database.

Last fall, the Medical Board of California sent reminder notices to physicians about their obligations under these rules to notify patients about the Open Payments database. These obligations including providing notice to patients in written or electronic form, via posted notice, and on a public website. UC Davis Health provides these notices on behalf of the physician workforce, including providing a link to the searchable federal database on our website: Public Reporting | UC Davis Health.

Investigation Trends

Hot Topics – Policy Reminders

Badge/Card-key Use

Your UC Davis Health issued identification badge doesn't just include your most flattering photo, your name, and information about your role here. It also includes a card-key, which may allow you access to various buildings and restricted areas within those building. This card-key must be used responsibly, especially when accessing patient care areas. When conducting personal visits with family members or friends being treated in the hospital, staff must follow visitor policies and may not use their card-keys to access secured patient care areas. Unless you have a work-related reason for being in a locked area, you may not use your card-key to gain access. See Policies 3311, Cardkey Security Access, and 2878, Patients' Visitors, for more information.

Access to Family Member Medical Records

Your UC Davis Health-issued EMR credentials allow access to sensitive medical information and must only be used to access patient information for a work-related reason. Many employees have family members who are UC Davis Health patients and are involved in these family members' care in a personal capacity. While there are rules in place outlining who is entitled to a patient's medical information and when this information can be shared, there are also UC Davis Health policies governing permitted access to patient records. These policies prohibit accessing the records of family members unless it is for the sole purpose of performing your assigned duties. An appropriate way to access your family member's record is via MyChart. If you would like information about obtaining access, please visit: health.ucdavis.edu/login and select the "Access Family's Record" link. See Policy 2454, Employee Access to Protected Health Information and Personal Information, for more information about permissible access to patient medical records.

UCDAVIS
HEALTH

For more information,
Contact Compliance and Privacy Services
916-734-8808
hs-compliancehelp@ucdavis.edu

Securing Protected Health Information (PHI) and Personal Information (PI) When Using Email

With the high daily volume of email communications transmitted at UC Davis Health there are potential risks involved when electronically transmitting emails that contain PHI and/or PI. Below are a few risks that can affect you as a workforce member, the UC Davis Health organization, and most importantly our patients.

- Utilizing the auto-fill list function in the UC Davis Health Outlook email system and accidentally selecting the incorrect recipient.
- Manually entering the incorrect recipient email address within UC Davis Health's Outlook email system.
- When transmitting an email to external recipients, failure to enter the proper encryption verbiage of #secure# in the subject line or anywhere within the body of the email or entering the incorrect encryption phrase in attempt to enable the encryption (e.g., #encrypt#).
- Attaching a file containing PHI and/or PI when replying or forwarding an email to unintended UC Davis Health or non-UC Davis Health recipients.

Here are some useful tips that should help minimize the above listed risks:

- Double check the email address of the intended recipient and thoroughly review the attached files for correctness.
- When in doubt, review the email with your respective leadership for guidance prior to sending.
- To enable encryption properly when sending emails to non-UC Davis Health recipients, enter the encryption phrase of #secure# in the subject line or anywhere in the body of the email.
- For workforce members that send external emails often, an email template to include the correct encryption verbiage of #secure# can be created in the UC Davis Health Outlook email system.
- In the event an email was sent to an incorrect recipient, immediately attempt to recall the message and immediately report the incident to Compliance and Privacy Services at hs-privacyprogram@ucdavis.edu