SAFEGUARDING PROTECTED HEALTH INFORMATION (PHI)/MEDICAL INFORMATION IN A REMOTE ENVIRONMENT

COMPLIANCE AND PRIVACY SERVICES **SEPTEMBER 2023**

APPLICABLE POLICIES

Policy and Procedure (P&P) 1302, Protected Health Information, Personal Information Breach Notification

P&P 1313, Protected Health Information or Personal Information on Mobile Devices and Personal Computers

P&P 1314, E-mail Use for UC Davis Health Personnel (Employees, Faculty, Staff)

P&P 2442, E-Mail Communication that Contains Protected Health Information or Personal Information

P&P 2450, Disclosing the Minimum Necessary Protected Health Information

P&P 2902, Confidentiality

Contains active links. Distribution via email is preferred. Print as necessary.

While working remotely, all workforce members are responsible for ensuring the protection of all confidential information pursuant to applicable federal and state privacy laws. This includes information that may be stored electronically, in printed materials, or verbally discussed. UC Davis Health also maintains policies to protect confidential information, such as PHI, from unauthorized access, use, and/or disclosure. Such policies do not change when an employee works from home or anywhere else remotely.

Safeguarding PHI: Network Connection

The UC Davis Health data networks are vital resources for treating patients and depended upon by thousands of care providers for life-saving services. Access must only be made through standard, approved methods and apps, such as the UC Davis Health Virtual Private Network (VPN) via the Cisco AnyConnect application, or applications like Citrix and Zoom, vetted, assessed, approved formally, and installed by Innovation Technology. These approved secure remote access technologies are standards backed by policy and protect the confidentiality of data and prevent the interception of data. Multifactor authentication (MFA) is also required and confirms a workforce member's identity with something you have like a cell phone, something you know like a PIN, or something like a fingerprint. MFA can go a long way in keeping applications, e-mail, cloud storage and VPN accounts secure**.** Additional information about remote setup and connectivity can be found at https://health.ucdavis.edu/remoteaccess/. You may also contact the Innovation Technology (IT) Helpdesk for support by calling 916-734-4357.

Safeguarding PHI: Electronic Transmissions

The official UC Davis Health Outlook email system (example@ucdavis.edu) must be used for all work-related activities associated with your assigned duties. UC Davis Health workforce members are prohibited from forwarding work emails to their personal email account(s) for any reason, including the avoidance of work challenges like slow network connectivity or the inability to print. If you experience these challenges, please contact the IT Helpdesk for support by calling 916-734-4357.

Safeguarding PHI: Documents, Mobile Devices, and Computers

Documents, mobile devices, and computers must be controlled by UC Davis Health workforce members and secured at all times. Physical space in the remote setting should be in an area that is dedicated to work and not used for anything else. Household members, family members, or anyone else that is not a UC Davis Health workforce member with a work need should not have access to UC Davis Health documents, mobile devices, or computers in the remote environment.

Actions to Take When a Known or Suspected Breach Has Occurred

In the event the confidentiality or integrity of patient information has been compromised, or a suspected incident has occurred, all UC Davis Heath workforce members must **immediately** notify the Compliance and Privacy Services Department by phone, email, or RL Datix, **and** notify their immediate supervisor.

Three ways to report privacy incidents:

☎ 916-734-8808

✉ hs-privacyprogram@ucdavis.edu

Submit an Incident Report via RL Datix by typing "*incident*" in your browser address bar or log in via Citrix.

! Select "Confidentiality/Healthcare Information" category when completing the report.

What Information Should You Report?

The following **ten items** should be provided when reporting a known or suspected breach:

1. The date the incident occurred.
2. The date the incident was detected/discovered.
3. How the incident occurred.
4. How the incident was detected/discovered.
5. The name(s) of the patient(s) whose information was disclosed (affected patient).
6. The name(s) of the recipient(s) of the disclosed information (unauthorized recipient).
7. The specific information disclosed (if possible and applicable, please provide a copy).
8. Actions taken to mitigate harm.
9. The name(s) of the individual(s) responsible for the incident.
10. The department contact for follow-up questions.

Immediately provide as much information as possible. Do not delay reporting if some information is missing.

Best Practices Overview

- Maintain control of data by ensuring documents and devices that contain PHI are secured when not in use. Failure to maintain accountability of PHI can lead to loss, theft, or misuse, resulting in a violation of patient privacy laws and UC Davis Health policy.
- Secure remote workspace so that PHI can be properly safeguarded from unauthorized access.
- Never leave PHI in view of unauthorized individuals; PHI should always be secured, and computers should remain locked when not in use.
- Do not print PHI to a home printer without authorization from your management. Home computers, printers, faxes, and copiers all contain internal storage; the information stored within the internal storage is vulnerable and could lead to a privacy violation.
- Encryption must be used when emailing PHI to any non-UC Davis Heath email account. UC Davis Health cannot protect information once it is removed from our network. Sending unencrypted PHI to a non-UC Davis Health account is a violation of UC Davis Health policy and may result in a privacy breach.
- The official UC Davis Health Outlook email system (example@ucdavis.edu) must be used for all work-related activities associated with business.
- Auto-forwarding email messages from the UC Davis Health Outlook email system to any non-UC Davis Health email account (e.g., Gmail, Yahoo, Hotmail, etc.) is a violation of UC Davis Health Policy and may result in a privacy breach.

Questions?

We encourage you to reach out to our team with any compliance or patient privacy related inquiries or concerns.

☎ 916-734-8808

✉ hs-privacyprogram@ucdavis.edu