UC DAVIS HEALTH | Compliance and Privacy Services

TELEWORK/TELECOMMUTE GUIDELINES

It is the legal and ethical responsibility of all UC Davis Health workforce members to protect the privacy, confidentiality, and security of all patient, proprietary, and/or other confidential information relating to the University and its business.

The following information is provided to assist you with protecting all types of confidential information when working from a remote location:

Workspace considerations:

- Patient, proprietary, and other confidential information should not be taken home/off-site whenever possible. However, if it is necessary to take documents home, only the minimum necessary documents may be removed. The confidentiality of paper documents should be maintained outside the workplace.
- Designated home/off-site workspaces should be set up in a secure environment to maintain confidentiality.
- Work-related conversations must be undertaken in a confidential manner to prevent unauthorized disclosure to anyone.
- Any and all patient information must always be secured. Paper documents should be stored confidentially – they should not be left out at home or visible to unauthorized people. Any electronic sessions or devices should be logged off and/or stored when not in use.
- Control of devices. Do not leave laptops, mobile devices, and/or documentation unattended anywhere, not even your car!

Technology and resources:

- Any equipment, software, data, supplies, and/or furniture provided by the University is limited to use by authorized persons and for University business only. Do not let anyone else use these resources for any purpose (e.g. family or friends.)
- Only use University-issued laptops and/or mobile devices (e.g., cellphones, tablets, etc.) to conduct business *unless* they are not available or have not been issued to you and remote work has been approved by your supervisor.
- If using non-University devices (e.g., a laptop, cellphone, tablet, etc.), please refer to Policy and Procedure 1313- *Protected Health Information or Personal Information on Mobile Devices and Personal Computers* to comply with security requirements and this link for set-up options: https://health.ucdavis.edu/remoteaccess/.

UCDAVIS HEALTH | Compliance and Privacy Services

Network connections:

- It is best practice to not connect to a public, wireless network. If it is necessary to connect in a public location, the University VPN service should be used for remote access.
- Remain vigilant when checking email, especially on mobile devices. There are criminals trying to take advantage of the current COVID-19 situation to trick people into clicking on false links or opening false documents. If you receive a questionable communication, please promptly forward the email to abuse@ucdavis.edu for a security review.

Storage:

- Only store patient, proprietary, and other confidential information on a UC-devices, OneDrive account, or unit-approved University network location.
    - You should confirm with IT and/or your management before you use any free tools that you may use for personal reasons like Dropbox, Google Drive, Google Docs, etc. before using them to store University information.
- If using mobile devices, automatic backup to cloud storage locations should be disabled if these devices are used to view documents that contain patient, proprietary, and/or other confidential information.
- Patient, proprietary, and/or other confidential information must not be stored on external media – like USB drives, disks, etc. – that are not approved by the University.

Destruction:

- Patient, proprietary, and/or other confidential information saved on laptops and/or mobile devices must be permanently deleted when the information is no longer needed.
- Disposal of confidential information must only occur in approved shredding containers. When working remotely, it is not appropriate to place confidential information in the trash. Confidential documents should be retained in a safe place until you are able to return them to UC to a confidential/shredding location.

Resources – If you need help, please do not hesitate to reach out:

Compliance and Privacy Services Department
Phone: 916-734-8808
Hs-privacyprogram@ucdavis.edu
https://health.ucdavis.edu/compliance/