STORAGE OF ELECTRONIC PATIENT INFORMATION ON PERSONAL DEVICES

COMPLIANCE AND PRIVACY SERVICES **FEBRUARY 2025**

APPLICABLE POLICIES

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

BYOD (Bring Your Own Device)

Personal devices allow UC Davis Health (UCDH) workforce members to access information, including electronic patient information, wherever they are and whenever they need it. This access to information offers an enormous opportunity to improve academic, research and clinical outcomes, as well as to drive higher patient satisfaction with the services we offer as a healthcare provider. Surveys of workers in the healthcare industry have shown that as mobile technology matures, users increasingly want to use both organization-issued and personally owned devices to access enterprise data to perform work-related activities. This guidance will highlight some of the risks associated with storing enterprise data and specifically electronic patient information on personal devices so that UCDH users can take some affirmative steps to mitigate these risks.

Potential Risks

Some of the risks associated with storing electronic patient information on personal devices include:

- Due to their small size and portability, personal devices are at a greater risk of being lost or stolen. A lost or stolen personal device containing unsecured data could result in a breach requiring notification under HIPAA and state laws.
- Your personal device may have default settings that enable unsecure connectivity to Wi-Fi, Bluetooth, cloud storage or file sharing network services.
- Data may be accidentally pasted or uploaded to cloud apps that are not UCDH-approved and not covered by a Business Associate Agreement (BAA), potentially resulting in a reportable breach.
- Depending on your use, your personal device could become infected with viruses and malware. For example, a seemingly innocuous mobile application or game could access your contacts, pictures, or other information and send such data to a third-party without your knowledge.
- Personal devices may be accessed by household members, family and friends which could allow unauthorized access to the data.

Data may be accidentally pasted or uploaded to cloud apps that are not UCDH-approved

Best Practices

Best Practices for securing PHI on personal devices include the following:

- Avoid storing electronic patient information on personal devices. This data may be accessed using a personal device. However, it is strongly encouraged that prior to accessing this data the personal device be enrolled in the UCDH BYOD (Bring Your Own Device) Program. This program uses security technologies like Workspace One to maintain a separation of work apps and data from personal apps and data. This separation protects electronic patient information from accidental mishandling and also protects your personal privacy by preventing your personal apps and data from potentially being considered University property and/or becoming part of a privacy investigation.

> UC Davis Health BYOD (Bring Your Own Device) Program uses security technologies to maintain a separation of work apps and data from personal apps and data.

- When working with electronic patient information on a personal device, it is best practice to avoid storing data directly on the device. Instead, when necessary to save the data, it should be stored in a UCDH-approved storage solution (e.g., OneDrive, SharePoint) or other UCDH-approved third-party application.
- Never use electronic patient information with a personally owned/licensed cloud app or a privacy violation may occur. HIPAA requires a Business Associate Agreement (BAA) to be completed prior to using this data in this manner. At UCDH, only the applicable Purchasing team(s) are authorized to enter into such an agreement.
- Require authentication (e.g., biometric, pin, etc.) to use or unlock mobile devices.
- Regularly install security patches and updates.
- Install or enable encryption, anti-virus/anti-malware software, and remote wipe capabilities on all devices.
- Use only secure Wi-Fi connections prior to accessing the data.
- Use a virtual private network (VPN) with all devices prior to accessing the data.
- Reduce risks posed by third-party apps by carefully reviewing the Terms and Conditions to determine what information the app will have access to (e.g., your contacts, pictures, etc.), if your data will be sent to the third-party, and if patient data might be accidentally mishandled by your using it.
- Always secure your personal device. Do not allow access by household members, family or friends.
- Immediately report lost or stolen personal devices to the IT helpdesk, and Compliance and Privacy Services.

Remember

Ensuring the security of patient information is a responsibility we all share. Storing sensitive data on personal devices—even with the best intentions—can create unnecessary risks. By following best practices, we help protect patient privacy, maintain trust, and support the integrity of UC Davis Health.

Questions?

For more information, please review UCDH policy 1313, Protected Health Information or Personal Information on Mobile Devices and Personal Computers. Please also contact Compliance and Privacy Services by email or telephone at:
hs-privacyprogram@ucdavis.edu or 916-734-8808

You may also reach the IT Help Desk at 916-734-4357.