Division of
Information Technology

Texas A&M University

Electronic Protected Health Information MOBILE DEVICE MANAGEMENT Control

Table of Contents

Purpose

The purpose is to ensure units have Electronic Protected Health Information (ePHI) procedures to protect mobile devices containing ePHI with adequate security in case of loss, theft, or tampering.

Scope

This policy applies to TAMU in its entirety, including all systems that process ePHI.
HIPPA Safeguards: 45.CFR.164.308 (a)(1) Periodic Review; 45.CFR.164.308 (a)(3) Authorized Access; 45.CFR.164.308 (a)(5) Passwords; 45.CFR.164.310(b) Security Controls; 45.CFR.164.312(a)(1) Technical Access Safeguards; 45.CFR.164.312(b) System Monitoring.

Roles and Responsibilities

TAMU units acting as Health Care Components, either as a Covered Entity or Business Associate, will clearly identify and document:

- Mobile information assets (for example; laptops, tablets, pads, smartphones, IoT devices) that either directly store or transmit ePHI.
- Mobile information assets have access and password/passcode management that either directly or indirectly store or transmit ePHI.

- Mobile information assets have both time-duration and failed-attempts lock screen settings enabled.
- Mobile information assets have encryption activated that meets the TAMU HIPAA Encryption and Decryption Control, https://cio.tamu.edu/policy/it-policy/hipaa/pdfs/EncryptionAndDecryptionControl.pdf
- Unit procedures to 1) know the last time the mobile information asset was on the TAMU network and 2) periodically to audit device presence on the TAMU network no less than every ninety (90) days for non-reporting assets.
- Unit procedure to remotely wipe and delete all data in case of a report of theft or loss.
- Compliance with TAMU System Regulation 29.01.03, http://policies.tamus.edu/29-01-03.pdf , requiring multi-factor Authentication (MFA) for any systems containing confidential information.

Security Control

Mobile devices storing and/or transmitting ePHI must be both encrypted and centrally managed, preferably by mobile device management software (MDM). The MDM should either establish or validate technical safeguards such as updated software and malware protections. Mobile devices are often lost, stolen, or even tampered with if left in an unsecured physical location. Upon reported incidents involving a mobile device the MDM there should be the tool to track the device. It is recommend to consider enabling location tracking of devices at periodic intervals through MDM to detect unexpected locations and potential unreported mobile device loss.

All TAMU mobile information assets containing ePHI must have unique authentication granting access to ePHI. Password/passcode management must be part of the authentication. https://cio.tamu.edu/policy/it-policy/hipaa/pdfs/HIPAA%20Role-based%20Access.pdf

Procedure(s)

Units with ePHI on mobile devices must utilize:

- Unit procedures around mobile device management.
- If available, MDM configuration policies must be set to ensure compliance with all TAMU security requirements.
- In the absence of an MDM, unit procedures must clearly document the methods used for mobile device ePHI protection.
- accurate and timely accounting and auditing of device presence on the network beyond an annual inventory.

Contact and Questions

Please send all inquiries to: *ra@tamu.edu*