Augusta University Medical Center Policy Library

Mobile Device Policy

Policy Owner: Information Technology Support and Services

POLICY STATEMENT

Augusta University Medical Center (AUMC) discourages the storage of electronic Protected Health Information (ePHI) as well as other forms of regulated information on mobile computing devices. The Institution recognizes that incidental storage may occur through normal business activities; therefore, all mobile devices, regardless of ownership, used for official business must adhere to the controls outlined in this policy.

AFFECTED STAKEHOLDERS

Indicate all entities and persons within the Enterprise that are affected by this policy:

☒ Administrative Services
☒ Hired Staff
☒ Housestaff/Residents & Clinical Fellows
☒ Leased staff
☒ Medical Staff (includes Physicians, PAs, APNs)
☒ Patient Care Services (Nursing, PCT's, Unit Clerks)
☒ Professional Services (Laboratory, Radiology, Respiratory, Pharmacy; etc.)
☒ Vendors/Contractors
☐ Other:

DEFINITIONS

Encryption: Process for transforming information to make it unreadable to anyone except those possessing appropriate credentials to authorize access in accordance with FIPS/NIST standards. Encryption solutions can be obtained and implemented with the assistance of IT Services.

Endpoint Protection: Mobile device protection that can include solutions such as anti-virus/malware protection, pro-active threat protection and network threat protection and/or intrusion prevention system.

FIPS: Federal Information Processing Standards

Incidental Storage: can include, but is not limited to storing your AUMC email on a mobile device in which your email contains regulated data such as PHI.

Mobile Device: Any computing or data storage device that is easily transported. For the purpose of this policy a mobile device includes, but is not limited to: handheld computers, smartphones, laptops, tablet computers, USB flash drives, and portable hard drives.

NIST: National Institute of Standards and Technology

Office of Compliance and Enterprise Risk Management Use Only
Policy No.: 392
Policy Sponsor: Chief Information Officer
Originally Issued: Not Set2
Last Revision: 04/24/2017
Last Review: 08/11/2017
Next Review: 11/04/2019

Personally Identifiable Information (PII) Any one or more of the following data elements in combination with an individual's first name or last name or first initial and last name, when either the name or the data elements are not encrypted or redacted:

- Social security number;
- Driver´s license number or state identification card number;
- Account number, credit card number, or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes, or passwords;
- Account passwords or personal identification numbers or other access codes; or
- Any of the above, bulleted items when not in connection with the individual´s first name or first initial and last name, if the information compromised would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised.

The term personally identifiable does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records."

Protected Health Information (PHI): PHI means individually identifiable health information that is:

(1) Except as provided in paragraph (2) of this definition, that is:
(i) Transmitted by electronic media;
(ii) Maintained in electronic media; or
(iii) Transmitted or maintained in any other form or medium.

(2) Protected health information excludes individually identifiable health information:
(i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;
(ii) In records described at 20 U.S.C. 1232g(a)(4)(B)(iv);
(iii) In employment records held by a covered entity in its role as employer; and
(iv) Regarding a person who has been deceased for more than 50 years.

Regulated Information: Any data regulated by federal, state, and/or local statutes or policy. This includes, but is not exclusive to, protected health information (PHI) and personally identifiable information (PII) about patients, students, faculty, staff, business partners and others, who provide such information to AUMC, that could be used for identity theft, or data deemed business sensitive such that unauthorized disclosure could have negative impact on operational, financial, or reputational business relations.

Remote Wipe: Process in which data can be remotely deleted from a mobile device in accordance with NIST standards.

Restricted Data is not legally protected, but should not be made public and should only be disclosed under limited circumstances. Users must be granted specific authorization to access since the data's unauthorized disclosure, alteration, or destruction may cause perceivable damage to the institution.

The following are examples of restricted data elements:

- Non-directory information identifiable to an individual (including students, staff, faculty, trustees, donors, and alumni), including but not limited to, dates of birth, driver's license numbers, employee and student id numbers, license plate numbers and compensation information.
- The institution's proprietary information, including but not limited, to intellectual research findings, intellectual property, financial data, and donor and funding sources.

Smart Phone: Any phone that, in addition to basic voice communications, offers advanced computing ability, data storage, email, and/or Internet connectivity.

Rooting or Jailbreaking: Installing software or exploiting an operating system (OS) flaw that bypasses the security lockouts enforced by institutional policy and/or the manufacturer on a mobile device.

PROCESS & PROCEDURES

Provisions

1. AUMC has the right to approve or deny the use of a personal device in the workplace.
2. AUMC is not liable for loss, damage or theft of any personal devices.
3. Employees are responsible for reporting loss or theft any device to the help desk so that all hospital information and applications can be remotely wiped from the device.
4. AUMC is not responsible for technical support of an employee's personal device outside of approved applications by the hospital. Employees are responsible for maintaining and supporting their own devices, as well as incurring any costs associated with the support of these devices.
5. AUMC provides WiFi in the facility for use of AUMC applications on personal devices. AUMC will pay for the license cost to use approved applications. It is up to the employee to ensure they are connected to WiFi when using these applications. AUMC will not reimburse employees for data usage on personal devices.
6. AUMC may choose to revoke access to Imprivata Cortext® or other hospital applications from an employee's personal device if deemed appropriate.
7. All mobile computers and devices, regardless of ownership, used to conduct the business of the enterprise must meet the security standards outlined in this policy. The institution requires all users to utilize appropriate enterprise designated systems for the storage of regulated information

(i.e., Synchronicity (PowerChart) is the system of record for the electronic medical record, the "R" drive is the network storage location for research data).

8. All mobile devices used to transmit or store institutional restricted and/or regulated information must be either owned by the institution or have implemented the security controls owned and managed by the institution.

9. All employees are responsible for the protection of institutionally owned data, PHI, PII and other forms of regulated data contained on mobile devices in their custody and/or used to connect to the enterprise network. Security of data maintained, stored, or transmitted is subject to the provisions of local, State, Federal statutes and regulations, and the provisions of the institution's privacy and security policies.

General Technical Requirements

1. Endpoint Protection: Any system used to connect to the enterprise network or other business entity on behalf of AUMC, regardless of location or ownership must have safeguards installed to prevent malware infection or unauthorized access to the enterprise network or data.

2. Mobile devices connecting to enterprise systems or used for official business must:
   - be password protected in accordance with institution policies and standards
   - use institution issued and installed data encryption software to prevent unauthorized disclosure
   - as applicable, have personal firewalls installed and active
   - never be left unattended and remain in positive control of the custodian at all times
   - be permanently destroyed when no longer required when the system has reached end of life
   - wipe, according to NIST standards, the device before ownership is transferred

3. Security Software: No action should be taken to disable security software or configurations designed to protect the device from compromise. This includes removal of anti-malware software or disabling firewalls on a laptop and rooting or jail-breaking a phone or tablet.

Device Specific Requirements

1. **Laptops:** Laptops storing institutionally-owned restricted and/or regulated data must be owned by the institution and employ enterprise approved security software to include endpoint protection and encryption.

   Do not store institutional restricted and regulated information on unapproved cloud-based storage offerings such as, but not limited to, Apple iCloud, Dropbox, Google Docs, Google Drive, etc. to prevent data leakage to third parties that the institution does not have data agreements with. Contact the ITS Service Desk or the Information Security Office for information on approved cloud storage providers.

2. **Smart Phones and Tablets**. All smart phones and tablets, regardless of ownership, used to connect to enterprise information systems (including email) must adhere to:
   1. Register device with the institution by requesting access to AUMC email
   2. Minimum device unlock passcode/password length of 4 characters
   3. Configured to a timeout of no greater than 10 minutes of inactivity
   4. Enable encryption

   All smart phones and tablets, regardless of ownership, that store institutionally-owned restricted and/or regulated information, must have all unapproved cloud synchronization services, such as, but not limited to, Apple iCloud, DropBox, Google, etc., disabled to prevent data leakage to third

parties that the institution does not have data agreements with. An example would be taking a patient identifying photograph on an iPhone that is synchronizing the picture to iCloud. Contact the IT Help Desk or the Information Security Office for information on approved cloud storage providers.

Note: The institution reserves the right to wipe any mobile device used to connect to enterprise systems. This is especially relevant to devices connecting to the enterprise email system or other systems which download data to the device's onboard data storage.

3. **Flash (e.g. SD Cards/Thumb) Drives and Portable Hard Drives:** All flash and portable hard drives storing institutionally-owned restricted and/or regulated data must be owned by the institution and encrypted using an approved method of encryption to protect data at rest.

4. **Lost, Missing or Stolen Mobile Device** must be reported immediately to Public Safety and the Information Security Office. Information regarding loss or theft will be shared between entities as required. The workforce member with custodial responsibility for the mobile device preceding the incident must complete a *Lost/Stolen Equipment Report* form describing the data contents of the device and to assist with recovery, device wipe, and breach investigation as applicable. The Information Security Office will report all incidents of compromised regulated information to the Enterprise Privacy Officer for analysis and possible action.

5. **End of Life / Surplus:** All mobile devices, regardless of ownership, authorized for connection to enterprise information resources must be properly cleansed / wiped as specified by NIST standards of all institutional owned regulated data prior to donation, surplus, trade-in, redistribution or disposal. Contact the Information Security Office for device specific information for cleansing and disposal.

6. **Technical Specifications and Standards:** Questions regarding specific technical specifications associated with securing a mobile or remote device can be found by contacting the Information Security Office.

7. **Enforcement / Sanctions.** Any workforce member found to have violated this policy will be subject to disciplinary action, up to and including termination of employment.

REFERENCES, SUPPORTING DOCUMENTS, AND TOOLS

Lost/Stolen Equipment Form

RELATED POLICIES

Breach Notification - Protected Health Information Policy

APPROVED BY

Chief Executive Officer, Georgia Regents Medical Center **Date:** 06/13/2017