



**SECTION: ADMINISTRATION**

**AREA: GENERAL ADMINISTRATION**

**SUBJECT: MOBILE DEVICE SAFEGUARDS**

---

**PURPOSE**

To inform the UAMS workforce on the proper safeguards for securing mobile devices.

**SCOPE**

UAMS Workforce

**DEFINITIONS**

**Mobile Devices** are defined as Personal Digital Assistants (PDAs), tablets, cellular phones, text pagers, laptop computers, and any other types of mobile devices or media that receive, record or store information and data such as USB flash drives and memory cards, CD-Roms and DVDs.

**Confidential Information** includes information concerning UAMS research projects, confidential employee information, information concerning the UAMS research programs, proprietary information of UAMS, and sign-on and password codes for access to UAMS computer systems. Confidential information shall include Protected Health Information.

**UAMS Workforce** means for purposes of this Policy, physicians, employees, volunteers, trainees, and other persons whose conduct, in the performance of work for UAMS, is under the direct control of UAMS, whether or not they are paid by UAMS.

Click the following link to access any other terms or definitions referenced in this policy:  
<http://hipaa.uams.edu/DEFINITIONS%20-%20HIPAA.pdf>

**POLICY**

All members of the UAMS workforce who use Mobile Devices to access or record Confidential Information are responsible for the protection of the data. Confidential Information should only be stored in UAMS controlled and approved devices and users must take the necessary steps to safeguard that information from unauthorized or improper disclosure in violation of UAMS Policies and Procedures or HIPAA Regulations.

**PROCEDURE**


1. **Password Protections:** All persons who use Mobile Devices to access or store Confidential Information are required to use the device's password protection feature and the automatic time out or password protect screen saver feature if available. Confidential Information must be safeguarded in the event the

Mobile Device is lost, stolen, or otherwise accessible by someone other than the authorized user of the device.

2. Virus protection software must be installed and regularly updated on all laptop computers used for UAMS business purposes. Appropriate security updates must be maintained on all other mobile devices.
3. **Encryption:** All laptops and any other mobile device storing or manipulating data containing Confidential Information or ePHI must use encryption when technically possible. If a mobile device does not have encryption capabilities great care must be taken when accessing Confidential Information and password protections must be used. Confidential Information must never be saved to an unencrypted device.
4. **Repairs:** Before sending a Mobile Device for outside repair, the user must make certain that all Confidential Information and PHI has been deleted and erased from storage so that any Confidential Information and PHI previously stored in the device is rendered completely inaccessible to service technicians or other persons. In the event access to Confidential Information and PHI is necessary for the repairs to be made, a Business Associate Agreement must be in place with the vendor making the repairs. Please refer to: UAMS [Business Associate Policy, 3.1.33.](#)
5. **Beaming:** If Confidential Information is beamed via an infrared information stream, it is possible for another device to inadvertently pick up the transmission. Beaming is only allowed and must take place in the presence of only two (2) Mobile Devices which are held less than 4 inches apart for the duration of the transmission.
6. **Wireless Transmissions:** Security measures required by UAMS must be taken when sending Confidential Information in electronic form. Unless absolutely necessary, Confidential Information should not be stored on mobile devices. If it is necessary to store data on mobile devices, it must be encrypted. Questions regarding specific security measures required should be directed to the UAMS Technical Support Center at (501) 686-8555. Care must be taken to enter the correct pager/cellular phone number when transmitting Confidential Information in text format.
7. **Storage:** When not in use, Mobile Devices containing Confidential Information must be stored in a secure manner to prevent access by persons who are not authorized to view the Confidential Information stored in the device. Do not leave mobile devices and media in unattended vehicles or public places.
8. **Reporting:** If a Mobile Device containing Confidential Information is lost or stolen, or if you suspect someone has improperly used or accessed protected information on your Mobile Device, it must be reported immediately to the UAMS IT Security Officer by calling (501) 686-8555 and the UAMS Campus Police by calling 686-7777.
9. **Data Removal:** The Mobile Device user is responsible for deleting Confidential Information in a timely manner when storage in the device is no longer necessary. Upon termination of the user's employment or other relationship with UAMS, users must remove all Confidential Information from the Mobile Device. Questions regarding data removal should be directed to the UAMS IT Help Desk by calling (501) 686-8555.
10. **Software Installation:** Only approved software should be installed on Mobile Devices. The software should be installed by a UAMS technician.

11. **System Settings and Device Maintenance:** Changing system settings should be limited to personalization of the Mobile Device, such as voice mail and layout preferences. Other changes could compromise the overall security of the device. The Mobile Device should be reviewed by an appropriate technician every six months to ensure the integrity of the device and perform needed upgrades.
12. **Sanctions and Personal Liability:** Violation of this Policy will result in disciplinary action, in accordance with Policy 4.4.02. If it is determined that a UAMS Workforce member was in violation of a UAMS policy in relation to the loss or theft of a mobile device, that individual may be held personally liable for the costs associated with the loss. Examples of such costs include, but are not limited to, the cost of the device and the cost of notifying individuals whose Confidential Information was contained on the device.

SIGNATURE: \_\_\_\_\_

A handwritten signature in black ink, appearing to read "David J. Wilson", written over a horizontal line.

Chancellor

Date: February 27, 2009