PURPOSE

To provide the requirements, procedures and protocols for managing a Mobile Device for accessing any Confidential Information that resides on UAMS systems or networks.

SCOPE

UAMS Workforce members to whom UAMS grants permission to access or connect to UAMS networks and systems from a Mobile Device for appropriate and authorized UAMS business purposes. Such UAMS Workforce members include those who use a Mobile Device that is 1) owned by UAMS or 2) owned by the individual who utilizes the Mobile Device to conduct business on behalf of UAMS. This policy applies to such UAMS Workforce members whether they are using a Mobile Device within or outside of their standard working hours.

DEFINITIONS

A **Mobile Device for purposes of UAMS Policy** is defined as any portable electronic device that runs an operating system that allows for network connectivity (wireless or wired) to UAMS systems and networks. Such devices include, but are not limited to, laptop computers, tablets, smart phones, wearable devices, text pagers, Personal Digital Assistants (PDAs), and any other types of mobile device or media that receive, record or store information and data such as USB flash drives and memory cards, CD-ROMS and DVDs, digital cameras and portable hard drives. Mobile Devices include those that are 1) personally owned by members of the UAMS Workforce who utilize the Mobile Device to conduct business on behalf of UAMS and 2) owned by UAMS.

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 for purposes of this Policy refers to, 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 to whom this policy applies who use Mobile Devices, as such term is defined in this policy, to access, record or store Confidential Information are responsible for complying with requirements, procedures and protocols to safeguard and protect the Mobile Devices. Only those Mobile Devices managed and approved by UAMS may be used to connect to UAMS networks and systems. UAMS Workforce members must comply with the terms of this policy and other UAMS policies and procedures related to using Mobile Devices and accessing, recording and storing Confidential Information on such Mobile Devices. This policy applies to UAMS Workforce members whether they are using a Mobile Device within or outside of their standard working hours. Failure to adhere to UAMS policies and procedures for a Mobile Device will result in immediate suspension of the UAMS Workforce member's access to UAMS systems and networks using that Mobile Device. Corrective action up to and including termination of employment, dismissal or termination of other association with UAMS may occur.

PROCEDURE

UAMS IT shall have the responsibility and authority to configure appropriate settings and options for Mobile Devices in a manner that ensures access to UAMS systems, networks and Confidential Information is protected and secured.

ACCESS CONTROL

1. UAMS Workforce members accept the terms and conditions of this policy before using a Mobile Device to connect to UAMS networks and systems. Users' agreement to the terms and conditions of this policy is indicated by registering their Mobile Device with UAMS IT. UAMS Workforce members will not be granted access to UAMS networks or systems using their Mobile Device until their Mobile Device is registered.

2. Any Mobile Device not in compliance with UAMS security policies, procedures or protocols or any Mobile Device that represents a threat to UAMS systems or networks or Confidential Information will not be allowed to connect to the UAMS network. Laptop computers or personal computers may only access UAMS Network and Data using managed and approved secure connections. These connections may include, but are not limited to, Firewalls, Secure Socket Layer (SSL) through VMWare or Citrix Sessions, an HTTPS connection or a Virtual Private Network (VPN) connection. Devices will have access to the Network and Data using Device Management enabled through software installed by IT on the Mobile Device. UAMS Workforce members may determine it is necessary to deregister a Mobile Device, and in doing so, the Mobile Device will no longer have the ability to access the UAMS Network and Data.

3. A Mobile Device will not be registered or may be deregistered without advance warning if a device is suspected of being used in a manner that puts UAMS networks, systems or confidential information at risk, a device is reported missing, or a UAMS Workforce member fails to adhere to this policy.

SECURITY

To ensure security measures and controls are in place on Mobile Devices and in accordance with UAMS Policies (referenced on the last page of this policy) the minimum requirements may include, but are not limited to, those security measures and controls listed below.

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 Mobile Devices used for UAMS business purposes, including laptop computers personally owned by members of the UAMS Workforce and laptop computers owned by UAMS. Appropriate security updates must be maintained on all other mobile devices.

3. **Encryption**: All Mobile Devices storing or manipulating data containing Confidential Information or ePHI must use encryption. If a Mobile Device does not have encryption capabilities, Confidential Information must never be saved to the Mobile Device and great care must be taken when accessing Confidential Information. Password protections must be used.

4. **Repairs:** Before sending a Mobile Device for outside repair, the user must make certain that all Confidential Information and PHI have 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: *Administrative Guide Policy 2.1.18, Business Associate Policy.*

5. **Beaming/Bluetooth:** 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. Verbal communications via Bluetooth are allowed. Please refer to: *Administrative Guide Policy 2.1.23, Safeguarding Protected Health Information.*

6. **Wireless Transmissions and Texting:** 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 Confidential Information 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 number when transmitting Confidential Information in text format. Texting Confidential

Information via Mobile Devices is not allowed, unless a UAMS authorized secure texting application is utilized.

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. **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. As may be necessary to ensure the security, confidentiality and protection of Confidential Information, UAMS IT may, at its discretion, delete and remove Confidential Information from a Mobile Device. Questions regarding data removal should be directed to the UAMS Technical Support Center by calling (501) 686-8555.

9. **Software Installation:** Great care must be taken when installing software or applications on Mobile Devices to ensure they do not compromise the overall security of the device. The Device Management system will install in a secure container UAMS business related software and applications, excluding Microsoft ActiveSync applications, used to access UAMS systems or networks or Confidential Information. Updates to such UAMS business related software and applications will be provided through the Device Management system. UAMS Workforce members may install software or applications of their choice on their personally owned or UAMS owned Mobile Device outside the Device Management software secure container. UAMS may block users' access to UAMS systems or networks if any software or application or data presents a threat to UAMS Confidential Information, UAMS Workforce, patients or visitors.

10. **System Settings:** For all UAMS owned Mobile Devices, system setting changes should be limited to personalization, such as voice mail and layout preferences. Other changes could compromise the overall security of the device.

11. **Users** must check with UAMS IT for compatibility and security before inserting any removable media, compact flash, memory cards, or other storage media into a UAMS owned Mobile Device.

REPORTING

1. 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 (24/7) to the UAMS IT Security Officer by calling (501) 686-8555 and the UAMS Campus Police by calling (501) 686-7777. Immediate reporting may allow for mitigation of a potential breach. If the Mobile Device is managed utilizing the approved Device Management system or Microsoft ActiveSync it

will be remotely wiped of all Confidential Information and locked to prevent unauthorized access. If the Mobile Device is recovered, a request can be submitted to IT for re-provisioning.

2. The **user agrees to immediately report** to his/her manager and to notify UAMS IT by calling (501) 686-8555 **any incident or suspected incidents of unauthorized access to Confidential Information**, loss of Confidential Information, and/or unauthorized disclosure of Confidential Information.

CONFIGURATION OF MOBILE DEVICE

Mobile Devices connecting to UAMS business resources will be configured utilizing a UAMS approved device management system. These management systems will configure the Mobile Devices for personal use with minimal security controls and a secure container for the UAMS business related applications that requires stronger security controls. Such configurations of settings and options include, but are not limited to, the following:

Mobile Device Controls:

1. Mobile Device Password / PIN - a password or PIN that must be entered before access to the Mobile Device is granted or available;

2. Mobile Device Screen Timeout - a password or PIN that must be entered after a period of inactivity before access to the device is granted or available;

Secure Container Controls:

The following basic phone services **must never** be used to conduct UAMS business outside of the secure container. UAMS users must use services that are compliant with HIPAA security controls. However, for applications located in the secure container, such as UAMS email, the following will be disabled and unavailable.

1. Photo Streaming – this service is disabled within the secure container; photos within the secure container cannot automatically be shared to other devices or users; if the camera on the mobile device is used to take a picture related to UAMS business purposes, the picture cannot automatically be transmitted to other devices or users;

2. iCloud – Data and Documents – this service is disabled within the secure container; downloaded attachments, files, and other data files are not stored, maintained or backed as part of the iCloud Device Backup. Confidential Information contained in attachments or files cannot be saved to 3rd party backup or storage services that are not approved HIPAA Business Associates (i.e. Dropbox and Siri);

3. Backup Services – this service is disabled within the secure container; when an email attachment or other document is opened and then saved to the device, the associated file is not included in the automatic backup feature (such as iCloud or Google). Confidential Information contained in email attachments or files shall not be saved to an outside

vendor or company that provides backup or storage services unless such vendor or company has been approved and authorized by UAMS.

ACCESS BY UAMS IT TO INFORMATION ON MOBILE DEVICES

When a Mobile Device is registered with IT, authorized members of the UAMS IT department are provided certain basic information about the Mobile Device. Access to this basic information is needed to manage the Mobile Device and access to UAMS networks and systems using the Mobile Device. Other information is not available to or accessible by UAMS IT.

1. Information about the Mobile Device that is available to and accessible by authorized members of the UAMS IT department may include the following:
    A. Mobile Device GPS location only if enabled and only on certain devices,
    B. Applications installed in the event a malicious application or an application has been identified as a privacy or security risk, UAMS IT staff needs the ability to perform a risk assessment based on applications installed on managed devices;
    C. Device Name, OS version, Battery level, Serial Number, UDID, Model in the event a known security or privacy event arises and a risk assessment needs performed;
    D. Email configuration settings in order to allow the synchronization of email, calendar and contacts from the UAMS email system.

2. Information about the Mobile Device that is not available to or accessible by any UAMS IT department staff include the following:
    A. SMS (text messages), MMS (picture messages), iChat, iMessage or other non-UAMS communication / messaging applications – IT does not have the ability to view, edit, or delete non-UAMS communication or messaging applications
    B. Phone call Logs (missed calls, placed calls, etc.) - IT does not have the ability to view, edit, or delete Phone call logs
    C. Phone Address Book entries or contacts - IT does not have the ability to view, edit, or delete Address book entries or Contacts
    D. Email Messages and Calendar (UAMS or non-UAMS) - IT does not have the ability to view, edit, or delete directly on the device. IT can view Email messages and Calendar Entries from the UAMS Email Server. IT cannot view non-UAMS Email or Calendar entries in any way.
    E. Pictures or videos taken with device camera or received via text message, email, or other methods - IT does not have the ability to view, edit or delete pictures taken with the device camera. IT does not have the ability to view, edit or delete photo albums, camera rolls, or video taken with a device
    F. Application usage such as content posted or viewed on social media applications, stored passwords for secure access to banking or other financial based applications, or any other information other than application version installed on the device - IT does not have the ability to access usage logs or other data associated with applications installed on a device. IT cannot view usernames and / or passwords associated to installed applications.

HELP & SUPPORT

1. Users will make no modifications of any kind to UAMS-owned and installed hardware or software without the express approval of the IT department. This includes, but is not limited to, any reconfiguration of the Mobile Device.

2. Where personal Mobile Devices are used, IT will manage sanctioned hardware and software, but will not manage or support unsanctioned media, hardware, or software. This includes Device Operating Systems that may be "jail-broken" or "rooted." This applies even to Mobile Devices already known to the IT department.

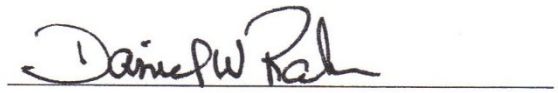
3. IT reserves the right, through policy enforcement and any other reasonable means it deems necessary, to limit the ability of Users to transfer Confidential Information to and from specific devices or data repositories on UAMS networks or systems.

MONITORING AND AUDITING

IT will establish audit trails which will be accessed, published and used by UAMS without notice to users. Such trails will track the attachment of an external device to a PC, and the resulting reports may be used by UAMS for business reasons such as for investigation of possible breaches and/or misuse. The user agrees to and accepts that his or her access and/or connection to UAMS systems and networks may be monitored to record dates, times, duration of access, etc., in order to ensure security and software configurations are maintained on the Mobile Device and to identify unusual usage patterns, abuse or other suspicious activity. This is done in order to identify accounts/computers that may have been compromised by external parties. In all cases, the protection and integrity of Confidential Information remains UAMS's highest priority.

SANCTIONS AND PERSONAL LIABILITY

Violation of this Policy will result in disciplinary action, in accordance with *Administrative Guide Policy 4.4.02 Employee Discipline* and *Administrative Guide Policy 2.1.42, HIPAA Sanctions Policy*. If it is determined that a UAMS Workforce member was grossly negligent 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: 

Date: August 3, 2016