I. PURPOSE

The purpose of this policy is to define a process for purchasing, securing, and supporting mobile devices that connect to UW Health business systems (e.g., email, calendar, and Health Link). Security controls are required to protect sensitive corporate data such as protected health information (PHI), per regulatory requirements for privacy and the Payment Card Industry Data Security Standard (PCI DSS).

This policy does not address devices that run a desktop/server operating system.

II. SCOPE

This policy applies to all users of mobile devices used to access UW Health business systems and the UW Health Information Services (IS) staff who support these devices. This policy does not address devices that run a desktop/server operating system.

III. DEFINITIONS

Mobile device: Any device running a mobile device operating system (OS), including, but not limited to, mobile phones, music players, and tablets. Common mobile device operating systems include Apple Computer iOS, Google Android, Microsoft Windows Mobile, and Research In Motion Blackberry OS.

MDM: Mobile Device Management system, a software and hardware platform for managing the configuration and security of mobile devices.

Jailbreak/root: Modifying a mobile device's OS to remove limitations imposed by the OS developer.

IV. POLICY

A large variety of mobile devices are available today, many of which are capable of synchronizing with corporate messaging services. The degree of compatibility varies greatly by device and operating system. It is not practical for UW Health Information Services to acquire and test all available devices. Synchronizing personal devices with UW Health business systems is supported at a best effort level. Employees are limited to two devices configured on the MDM platform.

A. Acceptable Use

1. Both personal and corporate owned mobile devices that synchronize with UW Health business systems must not be shared with co-workers, family members, or anyone else. Most mobile device operating systems are configured for only one person to use the device. Additional control systems are required to allow secure use of a device by more than one person. Anyone that wishes to use a corporate mobile device in a shared capacity should consult with the UW Health IS department before purchase to determine if the proposed use is possible.

2. UW Health IS uses appropriate measures to secure mobile devices accessing corporate data. This responsibility includes informing users of expected standards of conduct and the disciplinary measures for not adhering to them.

3. Anyone using a mobile device to access UW Health business systems who attempts to circumvent security mechanisms on the device will have their privileges revoked and may face disciplinary action.

4. If necessary for security reasons, UW Health IS may erase any and all data from the mobile device, including personal data. The user is responsible for backing up their personal data to prevent loss.

B. Eligibility Requirements

1. To protect patient and business data, access to corporate resources via mobile devices is limited to staff who need access to enhance patient care or conduct UW Health business.

2. Because the security risks associated with mobile devices are largely the same as the risks associated with remote access, users must obtain authorization for remote access as a prerequisite, except where an employee is issued a corporate mobile device. Refer to Hospital Administrative Policy 1.01-Remote Access to Electronic Information Systems for more
information. Note: Users must have a legitimate business need to work remotely to be eligible for this access. It is not appropriate to request remote access solely for personal convenience.

3. Personal or corporate mobile devices assigned to a single user require completion of the Mobile Device Consent and Device Data Form by the user, acknowledging the device owner’s responsibilities to protect sensitive patient and business data.

C. Personally Owned Devices
1. UWHC employees with authorized remote access may use personal mobile devices for business purposes, under the requirements of this policy.
2. UWMF employees eligible to use personal mobile devices are the following:
   a. Doctors and Mid-level providers
   b. Managers and above
3. Exceptions require approval at the director level or above.
4. Personally owned devices that are jail broken or rooted may not be used to access corporate business systems. This represents a security risk and may result in corporate data being erased from the device without warning.

D. Corporate Supplied Devices
1. Corporate supplied device platforms for mobile phones and tablets are determined by UW Health IS, based on negotiated contracts that afford good value in corporate pricing and functionality. Please contact the Help Desk for current supported models and pricing.
2. Director approval is required for all corporate supplied devices issued to individual users (UWHC only).
3. For UWHC:
   a. Data plan costs are assumed by the UW Health IS budget.
   b. Handset and related equipment costs are charged back to departments.

E. Security
1. To protect PHI and other sensitive business data, UW Health IS enforces security controls on all devices that are authorized to connect to corporate resources. Security controls may change over time to account for changing security threats.
2. Any lost or stolen mobile device must be reported to the Help Desk immediately.

F. Support
1. For corporate owned devices, UW Health IS supports device hardware and operating system troubleshooting, corporate applications, and synchronization with corporate messaging services (email and calendar), through standard Help Desk procedures. Where readily available alternatives for access exist (e.g., using a computer instead of a mobile device), support is limited to business hours.
2. Support of personal devices is limited to those hardware and software combinations that have been tested and confirmed compatible with corporate data systems, and the MDM platform’s capabilities to secure the mobile device. Support is limited to providing instructions to establish access to corporate applications and best effort troubleshooting related to accessing these applications with mobile devices. No other application or device support is provided.

G. Fees
1. UW Health IS covers all licensing and maintenance fees for a single mobile device connecting to the MDM platform.
2. Users who would like to use a second personal device must pay the initial licensing fees for MDM and any associated software. This one-time fee depends on the device being used.

H. Mobile Device Repair and Replacement
1. At retail service centers, mobile devices are often replaced, not repaired and returned. Any data on the mobile device may be accessible to buyers of surplus equipment, so corporate data on the mobile device must be erased by UW Health IS before it is sent to an authorized repair center. In addition, any mobile devices to be discarded or returned to manufacturers must have their data erased before leaving UW Health IS control.
   a. Corporate owned mobile devices that are damaged or broken and need to be replaced must be returned to UW Health IS.
   b. Users must contact UW Health IS before replacing a personally owned device or sending it in for service, so that someone may assist them.

V. PROCEDURE

A. Acquisition
1. When a user requests mobile device access to UW Health business systems:
   a. IS verifies the user is eligible to receive mobile device access to UW Health business systems (email, calendar, and/or Health Link) as described in the Mobile Device Policy.
   b. Note: All devices connecting to the MDM system for the first time will have a minimum OS requirement of Android 4.0 or iOS 4.2.
2. The user reviews, completes, and signs the UW Health Mobile Device Consent and Device Data Form on U-Connect. All requests are handled as low priority. Exceptions may be made on a case by case basis.

3. The request is routed to the appropriate IS staff to complete setup of the mobile device on the MDM system.

4. Software is installed on the mobile device to provide access to UW Health business systems and apply the required security.

B. Security

1. To protect corporate data stored on and accessed via mobile devices, the following security measures are applied to mobile devices connecting to corporate resources.
   a. A code (PIN), phrase, or similar user entered authentication mechanism is set up on the device before it can access applications or data. The mobile device owner is solely responsible for establishing and remembering this access code.
   b. After a period of inactivity, the user is required to re-enter the access code to access the device.
   c. If an incorrect access code is entered repeatedly, the device is remotely erased.
   d. Data stored on the device is encrypted.
   e. The mobile device owner is responsible for backing up all personal data (photos, music, documents, etc.) to a location off of the device. If the mobile device must be remotely erased, personal data on the device may be destroyed.
   f. The user is expected to immediately contact the Help Desk if the device is lost or stolen. If reported lost or stolen, the device is remotely erased the next time it connects to any UW Health data network to ensure patient and sensitive business data are not accessible to unauthorized persons. Refer to the Lost or Stolen Mobile Device Procedure for more information.
   g. Upon termination of employment, all corporate data and software are remotely deleted from the device. Every effort will be made to preserve personal data.
   h. UW Health IS monitors connections from mobile devices to the MDM system. Users with registered mobile devices that have not connected to the MDM system in more than 14 days may be disconnected from the MDM system, and all corporate data and software on the device will be remotely deleted.
   i. Corporate applications installed on the mobile device must be authorized and applied through methods established by UW Health IS. Users must not install alternate versions of corporate software from publicly available sources (i.e., app stores like iTunes or Google Play/Android Market).
   j. Additional security mechanisms may be activated on the device to address potential vulnerabilities as they become known.
   k. If a device is lost, stolen, or found, report it to UW Health Information Services immediately.

VI. FORMS

UW Health Mobile Device Consent and Device Data Form

VII. OTHER

UW Health is not a legal entity. UW Health comprises three separate entities. This policy applies to facilities and programs operated by the University of Wisconsin Hospitals and Clinics Authority and the University of Wisconsin Medical Foundation, Inc. and to clinical facilities and programs administered by the University of Wisconsin School of Medicine and Public Health.

Each entity is responsible for enforcement of this policy in relation to the facilities and programs that it operates.

VIII. COORDINATION (the details of Coordination of UWHC, UWMF, and UWSMPH are shown below. Approval and coordination of this policy by those entities occurs per their individual processes).

UWHC Sr. Management Sponsor: UW Health Chief Information Officer
UWHC Author: UW Health IS Director – Systems Security
UWHC Reviewer(s): UW Health IS Directors; UWHC Internal Auditor
UWHC Approval committee: Administrative Policy & Procedure Committee

UWMF Sr. Management Sponsor: UW Health Chief Information Officer
UWMF Author: UW Health IS Director – Systems Security
UWMF Approval: UW Health IS Directors

UWSMPH Approval: UW Office of Legal Affairs
SIGNED BY

Ronald Sliwinski
President & CEO