PURPOSE

This policy establishes guidelines for WellSpan Health (WSH) Employees and Medical Staff configuring personally owned mobile devices for work-related purposes.

DEFINITIONS

I. *Eligible Staff:* Any WSH Employee or Medical Staff member who has purchased their own mobile device and has a business need to have access to WSH systems on their device(s).

A. All exempt employees are eligible.

B. Non-exempt employees are eligible upon management approval due to work hour implications.

C. Medical Staff: A member of the Medical Staff of any WSH-affiliated entity.

II. *Mobile Device Management (MDM):* An industry term for the administration of mobile devices such as smartphones, tablets, and laptops, to ensure protection and security of data on these devices. MDM is usually implemented with the use of a third party application that has management features such as passcode protection, encryption, wiping, and disabling mobile devices (because security risks are similar, this also applies to personally owned non-mobile desktops).

III. *Encryption:* The process of rendering information unreadable by cryptography so that only authorized parties with a key or password can read it.

IV. *Data Container:* A secure area within an MDM application that adds another level of encryption, while still permitting access to the secured data.

V. *Personal Mobile Devices:* Personally owned cellphones, smartphones, tablets, laptop computers, or similar devices. Personal desktop computers are also treated in compliance with this policy.

VI. *Biometric:* Authentication technique that relies on measurable physical characteristics (i.e., finger or thumbprint).

VII. *Jailbreaking (Apple) / Rooting (Android):* The disabling of the standard, factory installed operating system. Usually done to allow reprograming of the device.

VIII. *Protected Health Information (PHI):* Any information that can be used to identify a patient – whether living or deceased – that relates to the patient's past, present, or future physical or mental health or condition, including healthcare services provided, and payment for those services.

POLICY

I. All personally owned devices that an eligible staff member wishes to use to access and download WSH email or business content must be managed in a secure encrypted container managed via current IS standard procedures.

II. Upon separation from WSH, loss of the device by theft or accident, transfer of the device to another owner/user, replacement of the device, or discarding the device, the eligible user MUST

contact WSH Information Services via the Service Desk within 24 hours of the event.

III. The protection of WSH owned PHI and business content is a primary responsibility of WSH. As such, WSH reserves the right to use the full capacity of its MDM technology to verifiably remove or destroy any WSH owned container and data (including, but not limited to, email and documents) that might be on the device.

IV. WSH will make every attempt to only remove information contained in the MDM container, but the eligible user acknowledges that preservation of non-WSH data on the device could be put at risk.

V. Back-up of WSH PHI data from an MDM device to a personal back-up site (i.e., iCloud, Google Drive, Drop Box, Evernote, etc.) is not permitted and may be considered a breach.

VI. While users may access WSH mail and other content from within their web browser on a non-WSH owned desktop computer, users SHOULD NOT download PHI or other confidential information to their device, due to the likelihood of breach.

PROCEDURE

I. WSH will deploy and manage a third party application for MDM. Using the application's technical and administration functions, WSH will:

A. Require the use of a passcode to access the device.

B. Force encryption.

C. Provide a secure data container that will allow:

1. Access to WSH e-mail, calendar, and contacts.

2. Access to WSH documents.

3. Access to approved applications.

4. Access to WSH INET.

D. Allow remote wiping of the WSH Container and/or disabling the mobile device.

E. Provide verification that Personal Mobile Device meets standard minimum requirements.

F. Oversee and analyze device deployment, and ensure and maintain compliance.

II. Eligible staff will be permitted to connect up to two (2) personal mobile devices to access the WSH data. Approval of 3 or more devices for any individual requires recommendation of a SVP and approval of the CIO or CTO.

III. Eligible Staff will be required to acknowledge the following upon downloading and connecting to WSH systems on their personal mobile device:

A. WSH assumes no responsibility for the eligible staff member's mobile device or agreement with a cellular carrier. WSH will not act as an agent to a cellular carrier for the mediation of equipment or billing disputes.

B. WSH data (i.e., e-mail, documents, and approved applications) remain the property of WSH.

C. WSH maintains the right to disconnect personal mobile devices to the WSH data upon termination of employment.

D. A passcode will be forced and required to gain access to the personal mobile device. Personal mobile devices with biometric capability will be able to access the device after the passcode is established and biometric access is configured.

E. Incorrect entry of a passcode 10 times will result in the device being locked. A call to the WSH Service Desk will be required for the device to be re-enabled.

F. Use of personal mobile devices by anyone other than eligible staff should be monitored. Access of WSH data by anyone other than eligible staff is considered a violation of this policy.

G. The loss, theft, damage, or security breach of a connected personal mobile device is to be reported immediately to the WSH Service Desk. Access to the device will be disabled and the WSH data container removed to assure that no unintended transmission of protected information occurs.

H. Upon upgrading/trading in a personal mobile device, a call to WSH Service Desk must be made to disconnect the old device and allow for the new device to be connected.

I. Intentional attempts to compromise a personal mobile device (i.e., jailbreaking or rooting) in order to gain access to WSH data via bypass of the WSH MDM product is a violation of this policy.

IV. With limited exception, the use of Mobile Devices that can take photographs and/or video is strictly prohibited to be used as an imaging device to take photos of PHI. Exceptions will be considered on an individual basis by the HIPAA Security Officer and CMIO or CTO.

V. Upon termination of employment the container will be removed and access to WSH data will be disabled.

VI. All Employees and Medical Staff shall adhere to and abide by all governmental rules, statutes, and regulations pertaining to the use of mobile devices while operating a motor vehicle.

VII. All Employees and Medical Staff will practice appropriate meeting etiquette when carrying mobile devices, such as not disrupting a meeting by ringing phones or distracting other attendees by texting or answering e-mails during meetings.

VIII. Any violation of this policy could result in a breach of WSH patient data, as well as sanctions to the employee up to and including termination.

IX. Non-exempt employees will be required to submit an Access Request through the Access Request Management (ARM) system from the WSH INET. The employee's immediate supervisor will be

required to approve/deny the request.

X. Eligible employees will need to contact the WSH Service Desk to obtain instructions on how to configure their devices.

SCOPE

This policy applies to all WSH Employees and Medical Staff.

REFERENCES:

MAP 304 – Information Systems Electronic Communication
MAP 312 - Password Policy
HR Policy ER-50 – Corrective Action

APPROVED BY: HIPAA Privacy and Security Steering Committee

CREATED DATE: 03/01/2010

REVIEW/REVISE DATES: 03/08/10, 03/11/15

SEARCH KEYWORDS: MAP, cell, cellular, phone, mobile device