Regions Hospital®

Subject **Employee Mobile Device or Remote Access**	**Attachments** ☐ Yes ☒ No
Key words mobile devices, laptop, cameras, smartphones, tablets, user responsibilities, mobile computing devices, patient photos, patient images, remote access, data storage	**Number** REG-SEC-100-6
Category Management of Information (MI)	**Effective Date** October 1, 2009
Manual Information Security	**Last Review Date** March 9, 2014
Issued By IS&T Security Management	**Next Review Date** March 9, 2017
Applicable Everyone Must Follow	**Implementation Date** October 1, 2009
	Retired Date
Review Responsibilities IS&T Risk and Compliance, IS&T Disaster Recovery/Security Committee, IS&T Sr. Director Services Delivery, IS&T Sr. Vice President and CIO	

I. PURPOSE

The purpose of this Policy is to establish controls for mobile device security, device utilization, data storage (USBs, CDs, etc) and employee remote access.

II. POLICY

HealthPartners/REG Responsibilities

IS&T Security Management is responsible for the Employee Mobile Device and Remote Access Policy at HealthPartners/REG and shall conduct a risk analysis to document safeguards for each device to be used on the network or on equipment owned by HealthPartners/REG. IS&T Security Management is responsible for developing any related Standards and Procedures for implementing this Policy.

User Responsibilities

Users of mobile computing and storage devices must protect such devices from loss of equipment and disclosure of HealthPartners/REG Data belonging to or maintained by HealthPartners/REG.

- Mobile devices and data storage devices must be kept on the authorized employee's person, stored in a locked drawer, or otherwise secured from others.

- Data stored on mobile devices owned by HealthPartners/REG or managed by

HealthPartners/REG' security, must not be moved or copied to non-HealthPartners/REG devices.

- The IS&T Support Center must be notified immediately when a mobile computing or storage device **may** have been lost or stolen.

- Patient images must only be taken with approved HealthPartners/REG cameras. Patient photos should not be taken with personal smartphones, personal cameras or any other personal device. Patient images on cameras must be immediately downloaded and saved to the patient's record, then immediately deleted from the camera's memory and/or the memory stick/card.

- While incidental personal use is allowed; HealthPartners/REG-owned mobile computing and storage devices should be used only for HealthPartners/REG business.

The Desktop Standards Group will maintain a list of approved mobile computing and storage devices. The list is available on the myPartner website.

Mobile Computing Devices
Mobile computing and storage devices containing or accessing HealthPartners/REG information may be personally owned or HealthPartners/REG-owned. Mobile devices include but are not exclusive to: smartphones, tablet computers, laptop computers, handheld wireless devices and cameras.

The following requirements apply to the security of mobile devices and network connections:

- IS&T will maintain mobile device Standards for connectivity to HealthPartners/REG' networks.

- IS&T will maintain wireless e-mail access software to ensure secure access to HealthPartners/REG' networks.

- All mobile device types/brands will be assessed for risk prior to being added to the Mobile Device Standard and permitted network access.

- Mobile devices that are allowed to direct connect to HealthPartners/REG' network or contain HealthPartners/REG' Data must have:

  - ✓ Encryption capabilities
  - ✓ Defined owner to ensure physical security and restrict access to the device
  - ✓ Up-to-date virus protection
  - ✓ Approved wireless e-mail software

  Note: Citrix or other portal type software is not included in these requirements as they meet compliance in a different type of control.

- Connectivity to HealthPartners/REG' network or storage of HealthPartners/REG' data with a mobile computing or storage device must be approved by an Authorized Approver.

- Patient images must only be taken with approved HealthPartners/REG cameras.

- Patient photos should not be taken with personal smartphones, personal cameras or any other personal device.

- Patient and member data must never be stored on non-HealthPartners/REG owned or managed devices.

- It is acceptable to view your personal e-mail from your mobile device, but prohibited to synchronize your HealthPartners/REG e-mail (Microsoft Outlook) to your personal e-mail account via your mobile device.

- Personal Wi-Fi or hotspot capability is not allowed on or at any HealthPartners/REG facilities and must be disabled. These radio frequencies can interfere with other equipment in use at HealthPartners/REG facilities.

Remote Access
HealthPartners/REG employees must ensure the appropriate physical and logical security controls are implemented at any remote location that is used to access HealthPartners/REG systems, applications and data beyond the functionality of Microsoft Outlook (e-mail and calendar).

The following security requirements apply to logical and physical requirements for employee remote access privileges to HealthPartners/REG' network:

- Non-HealthPartners/REG workstations used for accessing HealthPartners/REG' network must maintain protections when connecting to the organizations' network: physically secured, up-to-date anti-virus software, firewall protection, operating system patches and remote access only by authorized personnel.

- Protected Information must not be copied to non-HealthPartners/REG devices or to personally-owned devices not managed by HealthPartners/REG' security including workstations, laptops, tablets, smartphones or removable media devices.

- Workstations accessing HealthPartners/REG network remotely must not be connected to any other network concurrently.

- Reconfiguration of any personal equipment used for HealthPartners/REG' network access for the purpose of split-tunneling or dual homing is not permitted.

- Remote access must utilize two-factor authentication.

Data Storage
Portable storage devices that contain any HealthPartners/REG' Protected Information are only allowed if approved by an Authorized Approver. The ability to use the device is controlled at the workstation. The following requirements apply to all data storage devices:

- Data storage devices must be encrypted using HealthPartners/REG' approved encryption software. Individuals (e.g. patients or members) or their legal representative can consent

to receiving their own information in an unencrypted format (i.e. unencrypted CD).

- Data on a USB, flash drive, CD/DVD or other data storage device must be encrypted per HealthPartners/REG' Encryption Policy REG-SEC-100-7.

- Protected Information must not be copied to non-HealthPartners/REG devices or to personally-owned devices not managed by HealthPartners/REG' security including workstations, laptops, tablets, smartphones or other portable media devices.

III. RISK

Adherence to Policies, Standards and Procedures reduces the risk of exposure of organizational information assets.

IV. DEFINITIONS

CD a compact disc (disk) is a small, portable, round medium made of molded polymer for electronically recording, storing, and playing back audio, video, text, and other information in digital form.

DVD the digital versatile disc stores much more information than a CD and is used for playing back or recording movies. The audio quality of a DVD is comparable to that of current audio compact discs. A DVD can also be used as a backup media because of its large storage capacity.

Email the electronic transmission of information through a electronic mail protocol such as SMTP or IMAP. HealthPartners/REG / REG has standardized on Microsoft Outlook email client.

Flash Drive a plug-in-play portable storage device that uses flash memory and is lightweight enough to attach to a key chain. The computer automatically recognizes the removable drive when the device is plugged into its USB port. A flash drive is also known as thumb or USB drive. A flash drive can be used in place of a, CD, or DVD.

Handheld Wireless Device a communication device small enough to be carried in the hand or pocket. Various brands are available, and each performs some similar or some distinct functions. It can provide access to other internet services, can be centrally managed by a server, and can be configured for use as a phone or pager. In addition, it can include software for transferring files and maintaining a built-in or synchronized address book and personal schedule.

HealthPartners/REG Data is defined as the data HealthPartners/REG stores, manages and processes on behalf of our patients and members, as well as other financial, marketing and other data that is generated in the process of conducting HealthPartners/REG operations.

Media Type for the purposes of this Policy, the term "media type" is interchangeable with "mobile device." Not to be confused with media makes, models, or brands.

Media Type Model refers to the brand of media device such as Apple iPad, iPhone, Android.

Mobile Devices include, but are not limited to: smartphones, tablets, cameras, PDAs, USB port devices, CDs, DVDs, flash drives, handheld wireless devices, and any other existing or future media device.

V. COMPLIANCE

Failure to comply with this Policy, Standards or the Procedures may result in disciplinary action, up to and including termination.

VI. MONITORING AND MEASUREMENT

This Policy will be reviewed every three years to determine its timeliness and relevance.

VII. OTHER RESOURCES

ISO 27002:2005 Section 11.7.1, Mobile Computing and Communications
Mobile Devices Standard REG-SEC-200-6-1
Encryption Policy REG-SEC-100-7
Encryption Standard REG-SEC-200-7-1
Data Classification Standard REG-SEC-200-10-1
Data Storage Standard REG-SEC-200-10-3