Medical College of Wisconsin Affiliated Hospitals, Inc.

Institutional Policy

ENCRYPTION FOR ELECTRONIC PROTECTED HEALTH INFORMATION – MOBILE DEVICES

Category: Electronic Protected Information (PI)

Policy #: IT.PI.200

Applies to: All MCW Faculty, Staff, Students, and Business Associates

PURPOSE

The purpose of this policy is to address the appropriate protection and encryption of all MCW Electronic Protected Information (EPI) when it is stored, transferred or accessed on any mobile device. Full mobile device encryption and related controls are required to access MCW's electronic network or information through another means.

DEFINITIONS

Mobile Device - For the purposes of this policy a Mobile Device is defined as any portable computing device including but not limited to: laptops, tablets, smartphones, portable computers, flash drives or external hard drives.

Mobile Device Management (MDM) - Software that secures, monitors, manages, encrypts and supports mobile devices used within an institution's computing environment.

Access - The ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

Authentication - The corroboration that a person attempting to access the device or its information is the one authorized to do so. This can be accomplished in one of three ways.

1. Something the user knows such as a user name/password pair
2. Something the user possesses such as a smart card swiped through a reader or a card that dynamically generates a unique PIN at an approved interval, or
3. Physical identification biometrics such as a fingerprint scan.

Backup - Creating a retrievable, exact copy of data at a given point in time.

Business Associate - A person or vendor, who on behalf of The Medical College of Wisconsin (MCW) performs or assists in the performance of:

1. A function or activity involving the use or disclosure of PHI; or
2. Providing legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for MCW, other than a member of MCW's workforce, where the provision of the service involves the disclosure of individually identifiable health information to MCW or from another business associate, to the person or vendor.

All Business Associates must have a signed Business Associate Agreement with MCW. In addition the Business Associate may be required to complete MCW security education.

BYOD (Bring Your Own Device) - Personally owned devices that access MCW's electronic network or information through another means.

Electronic Protected Information (EPI) - Includes all classes of sensitive and/or confidential electronic data and information of the College and its employees, students and contractors. EPI includes Protected Health Information (PHI) as defined in the Health Insurance Portability and Accountability Act (HIPAA), and other information considered confidential by the MCW and/or Regulatory agencies including but not limited to the Health Information Technology for Economic and Clinical Health Act (HiTech), Federal Information Security Management Act (FISMA), Payment Card Industry Data Security Standard (PCI-DSS), Family Educational Rights and Privacy Act (FERPA) and MCW Institutional Review Boards (IRBs). EPI does not include information or data that is available or was obtained legitimately through publicly accessible sources, or information or data that is intended to be made available to the public. Examples of EPI include, but are not limited to, MCW's enterprise email system, the learning management system for MCW's Medical and Graduate schools, any clinical system that contains identified information or research repositories.

Encryption - The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

Password - Confidential authentication information composed of a string of characters, numbers or symbols.

PIN - Personal Identification Number, similar to a password.

Workforce - Employees, MCW volunteers, trainees, adjunct faculty, collaborators, emeritus faculty, contractors and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

POLICY

All Workforce members must protect MCW EPI. Workforce members using a Mobile Device owned by a workforce member, an external entity or one provided by MCW, to access or store EPI must have encryption using an institution-approved tool. The list of approved tools is available at:

http://infoscope.mcw.edu/is/support/Guidelines/EncryptionSecurity.htm

In addition, MCW students are also responsible for adhering to any mobile device policies and procedures detailed in the Student Handbook and/or within course syllabi.

Compliance with MCW's MDM and mobile device security standards is required on all MCW provided devices.

On personally owned devices (i.e. BYOD), should a workforce member choose not to permit MCW's MDM tools and supporting processes on their personal device, access to MCW's secured resources will be limited as outlined in procedure below.

Each workforce member is both responsible and accountable for securing EPI on all mobile devices, regardless of the owner of the device.

PROCEDURE

1. In the event of a lost or stolen Mobile Device, the affected workforce member shall immediately contact the MCW-IS Service Desk to report the incident. A member of the MCW Information Security Office, and other departments as necessary, will coordinate with the workforce member to:

a. confirm the Mobile Device was enrolled in MCW's MDM software

b. take the appropriate actions to safeguard all information stored on the Mobile Device

c. locate the device (if the workforce member has individually enabled the GPS service on their device)

d. coordinate communications required in event of a lost or stolen mobile device

e. document all known facts and actions taken as a result of the incident, including those related to a personally owned device that was lost or stolen and was not enrolled in MCW's MDM software

2. When a workforce member chooses not to permit MCW's MDM tools and supporting processes on their personal device, MCW reserves the right to deny access to MCW secured resources.

3. MCW-IS reserves the right to suspend the ability of a Mobile Device to connect to the MCW network infrastructure. MCW-IS will remove, disable or otherwise deny access to Mobile Devices considered a threat to MCW's systems, data, users, and/or patients. Devices without the approved Encryption solution installed will only be permitted access to the general Internet after authentication using MCW credentials has been established. Examples of the suspension from MCW's computer network could include:

    a. A virus or other malicious threat is identified and originates from the Mobile Device

    b. Any attempt to bypass security is identified such as rooting or "jail breaking" a device.

4. MCW reserves the right to log and audit access of EPI systems and data sets by its workforce as required, to meet regulatory, administrative, and security requirements. Examples include audit trail requirements stated within current HIPAA, FERPA and FISMA regulations.

    a. Specific to HIPAA, a Covered entity must, in accordance with HIPAA Security Rule §164.306...Implement a mechanism to encrypt and decrypt electronic protected health information." (45 CFR § 164.312(a)(2)(iv))

5. A backup or archive copy of the Mobile Device's content to another Mobile, or non-mobile device must also be encrypted. Encryption of the mobile device back-up file is the responsibility of the individual who uses and/or owns that device.

6. All mobile devices are required to have at minimum a four (4) digit PIN or password, or in the case of domain connected devices must follow MCW approved domain password policy. Additional complexity may be required depending on the level of security required by applicable regulatory controls.

7. MCW reserves the right to manage all Mobile Devices accessing the MCW wireless network using mobile device management software, domain software or other software tools.

8. All workforce members in possession of one or more mobile devices must protect the devices using MCW-IS and Public Safety approved physical security measures. Workforce members are expected to physically secure all mobile devices

whether or not they are actually in use and/or being carried.

9. Significant changes to this policy will require a formal review process including the Faculty Information Technology Advisory Committee, Office of Compliance, etc. An example of such change would be a request (internal or external to MCW-IS) to activate call, text or data utilization within the MDM software.

10. MCW-IS can be audited as necessary by the MCW Office of Corporate Compliance to ensure it has not operated beyond the permitted administration and management tasks referenced within this policy. Internal compliance audits will also be performed by the MCW Information Security Office. See Infoscope for details regarding MDM's permissible interaction with MCW workforce mobile devices.

11. Access to centralized information for registered mobile devices is as follows:

Tablet & Smartphone Administration Console (MDM)
Authorized Access
MCW-IS Server & Storage Division

Manager, Server/Systems Engineering & Enterprise Storage
Sr. Systems Engineer
Systems Engineer

Capabilities: System configuration, profile development, MCW applications. Full access to AirWatch console.

Tablet & Smartphone Administration Console (MDM)
Authorized Access
MCW-IS Service Desk

Manager, Server Desk
Technical Support Representative

Capabilities: Check for enrollment, wipe profiles, wipe devices, MCW application, and limited access. First call for timely resolution.

Tablet & Smartphone Summary Report Only (MDM)
MCW-IS Leadership

VP, Chief Information Officer
Information Security Officer
Information Security Analyst

Capabilities: Summary of system change log data only. No individual level data.

Laptop Administration Console
Authorized Access

MCW-IS Systems Administration & Support Staff
Decentralized Departmental IS Administrators

Note: Access to the Laptop Administration Console will be granted through a standard request process with proper role based access.

12. When a workforce member leaves the organization, MCW will remove the device encryption, MDM software and the MCW Exchange account(s). It is the sole responsibility of the workforce member to delete all other MCW content in their possession. MCW also reserves the right to require formal signoff acknowledging the destruction, deletion, and removal of MCW data stored somewhere other than Exchange on their mobile device has been completed.

13. MCW reserves the right to temporarily or permanently block applications on Mobile Devices registered with the MDM software. Reasons for blocking include malware, viruses, and any application that could copy EPI data without the user's consent. An application will not be removed through the MDM software without the written approval of the workforce member associated with the device.

REFERENCES

Electronic Protected Information (EPI) Security Definitions IT.PI.010
Health Insurance Portability and Accountability Act (HIPAA)
Health Information Technology for Economic and Clinical Health Act (HiTech)
Federal Information Security Managment Act (FISMA)
Payment Card Industry Data Security Standard (PCI-DSS)
Family Educational Rights and Privacy Act (FERPA)
MCW Institutional Review Boards (IRBs)

ATTACHMENTS

Not Applicable

Effective Date:	09/16/2013
Revision History:	01/19/2015
Supersedes Policy:	N/A
Review Date:	N/A
Approved By:	Kenneth B. Simons, MD Executive Director & DIO MCWAH

MCW policy #IT.PI.200 "Encryption For Electronic Protected Information – Mobile Devices" including revisions, has been adopted and incorporated in its entirety by MCWAH.