- Personally owned devices that access MCW's electronic network or information through another means.

- 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

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.

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.

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.

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.