

PURPOSE

The purpose is to establish the policy and procedure for the Michigan Department of Health and Human Services (MDHHS) to ensure and implement physical safeguards for all MDHHS workstations that access sensitive Electronic Protected Health Information (ePHI) and other sensitive information by implementing guidelines to restrict access to authorized users.

REVISION HISTORY

Issued: 11/02/2006
Revised: 01/01/2016
Reviewed: 01/01/2017
Next Review: 01/01/2018

DEFINITIONS

ePHI is the acronym for Electronic Protected Health Information. It is Protected Health Information that is transmitted or maintained in electronic form.

PHI is the acronym for Protected Health Information. It is information that can identify a person and contains health related data pertaining to that person.

Workforce Member means employees, volunteers 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. This includes full and part time employees, affiliates, associates, students, volunteers and staff from third party entities who provide service to the covered entity.

Workstation means an "electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions and electronic media stored in its immediate environment." (164.304) Thus PDAs, tablet computers and other portable/wireless devices are included (Department of Health and Human Services noted specifically in its Final Rule commentary that the standards are not to be interpreted as limited to "fixed location devices" Final Rule, p.22).

POLICY

It is the policy of the MDHHS to be committed and required to provide security to protect sensitive information and ePHI in its systems. MDHHS computer system hardware and software as well as the information and data carried by the system are the sole

property of MDHHS. Any misuse of MDHHS workstations may result in withdrawal of access to the system or MDHHS information or data.

MDHHS shall ensure, whenever possible, that each workstation has the necessary access controls to restrict unauthorized users and programs from accessing sensitive information or electronic protected health information. MDHHS shall ensure, whenever possible, that software on each workstation on the system (network) is internally compatible and will not lead to degradation of the system. MDHHS shall ensure that workforce member users are oriented and trained on workstation use.

PROCEDURE

Workforce Members

Any ePHI or other confidential information that resides on a mobile computing device that is State-owned or privately-owned (laptops, tablet PCs, Blackberries, PDAs, etc.) must be encrypted according to DTMB's encryption standards.

All computing devices must have current versions of anti-virus software enabled. Operating systems must have all critical updates installed.

All MDHHS workstations must be positioned or located in a manner that will minimize the exposure of any displayed patient or sensitive business information. When necessary, privacy screens should be used.

Workforce members accessing the MDHHS network or information from remote locations, such as connections from home, should employ appropriate security safeguards.

MDHHS workforce members may not independently install connectivity hardware or software to the computing resources of MDHHS.

All workforce members must comply with MDHHS and Department of Technology, Management and Budget (DTMB) policies, state and federal laws and regulations regarding the proper acquisition, use and copying of copyrighted software and commercial software licenses.

Department of Technology, Management and Budget

All MDHHS workstations with fixed storage that support more than one user, process sensitive information or electronic protected health information, including modems, shall be equipped, whenever reasonable, with security that secures hardware and restricts access to software.

All MDHHS workstations shall be equipped, whenever reasonable with updated software for detecting the presence of malicious software (for example computer viruses).

REFERENCES

45 CFR 164.310(c)

DTMB 1340.00.01 Acceptable Use of Information Technology

DTMB 1340.00.170.03 Electronic Data Encryption Standard

DTMB 1340.00.110.03 Storage of Sensitive Information on Mobile Devices and Portable Media Standard

APL 68D-070 PHI Use and Disclosure – Minimum Necessary Policy

APL 68D-072 PHI Use and Disclosure – Minimum Necessary Procedure

CONTACT

DTMB Client Service Center may be contacted at 517-241-9700 or 800-968-2644.

For additional information concerning this policy and procedure, contact the MDHHS Compliance Office at MDHHSPrivacySecurity@michigan.gov.