PURPOSE

The purpose is to establish the policy and procedure for the Michigan Department of Health and Human Services (MDHHS) to ensure that workstations and other computer systems that may be used to send, receive, store or access Electronic Protected Health Information (ePHI) are only used in a secure, legitimate manner and the physical attributes of the surroundings are specified. Workforce members who utilize workstations and other computer systems that are used to send, receive, store and access ePHI must comply with the Department of Technology, Management and Budget (DTMB) and the MDHHS computer use policies and the functions to be performed and the manner in which those functions are to be performed are specified.

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

Workforce members are responsible for maintaining the physical security of their workstation and other computer resources under their control and for protecting the integrity and privacy of the data maintained on them by the appropriate use of physical security, lockdown devices, password controlled access, data encryption, virus protection software and routine backup procedures.

Workforce members are responsible for following the Department of Technology, Management and Budget (DTMB) 1340.00.01 Acceptable Use of Information Technology Standard and all other applicable DTMB policies and procedures.

PROCEDURE

Workforce Member

Workforce members are required to enable password protected screensavers on all Windows based workstations, except shared workstations, which PHI or sensitive information is accessed. Any exceptions must be approved in writing by the workforce member's supervisor. In cases where password protected screensavers are not available, non-password protected screensavers should be enabled.

Workforce members are authorized to disable screensaver protection in certain circumstances, for example, when computer support/repair personnel are expected. Department level procedures should define the allowable delay before automatic screensavers activate. That delay should be based on balance between operational needs and security risks, but not to exceed 15 minutes.

All systems containing PHI or sensitive information should enable auto logout capabilities, if available. This delay should be determined based upon risk criteria.

Workforce members are required to have appropriate clearance prior to accessing computer workstations.

Where possible, workstations should be segregated based on function and access privileges as it pertains to PHI or sensitive information.

Installation of personal software, purchased or downloaded, including, but not limited to, screensavers and animated GIFs is

prohibited. Software required for end user purposes must be approved and installed by Department of Technology, Management and Budget (DTMB). The workforce member must document and maintain proof of license to have such applications.

Workstations must be installed with physical safeguards to eliminate or minimize the possibility of unauthorized access to information or theft of equipment. To the extent possible, equipment should be located in areas that have some degree of physical separation from the public and, where possible, should face away from the public. Where computers cannot be protected from public view, privacy screens are mandated. When applicable, computer screens should also face away from other workforce members to ensure privacy of PHI and sensitive information.

Workstation equipment and portable computing devices will be protected from exposure to physical threats including theft, based on potential risk and available safeguards. Desktops will be physically secured to desktops, tables or walls wherever reasonable, to prevent theft. Workforce members using portable computing devices, such as notebooks and PDAs are required to follow the policies and procedures for operation as established by DTMB. The DTMB Client Service Center may be reached at 517-241-9700 or 800-968-2644.

All laptops and any other portable computer equipment must be secured (protected) when not in use. Proper security is dependent on risk factors and available resources at specific locations throughout MDHHS. Security may be provided by locking equipment in a cabinet, desk, office, etc. Where such alternatives are not feasible, keeping the device out of sight in a desk or a briefcase may be appropriate.

Keeping information stored on a portable computing device secure and current is the responsibility of the workforce member who has the device in his or her possession and control. Those in possession are responsible for breaches of security related to devices in their possession.

Computer access and password training, as provided by DTMB, should be completed if possible, before access privileges are granted to ensure adequate training has occurred.

Users are required to logout and close applications containing PHI or other sensitive business information before leaving their workstations

Users are required to save all documents containing PHI or sensitive information to the designated network drive, approval from the Security Officer is required to save PHI elsewhere

Users should not reveal passwords with anyone else. A user's password may be used to track disclosure of information to third parties and if a password has been used to disclose information to an unauthorized source, the password owner will be held responsible for the disclosure

Users, when possible, should create alphanumeric passwords containing at least one letter and one number and a symbol. Passwords should not consist of any words or numbers related to the personal information of the user, such as house address, phone number, children's name, etc.

If a workforce member's password has been compromised, or revealed to another workforce member, contact a supervisor and if possible change the password

Users must not store written passwords in or around their workstation area

Workforce members that use MDHHS information systems and workstation assets should have no expectation of privacy. To properly manage its information system assets and enforce appropriate security measures, MDHHS may log, review, or monitor any data (ePHI and non-ePHI) stored or transmitted on its information system assets.

Workforce members are responsible for following the Department of Technology, Management and Budget (DTMB) 1340.00.01 Acceptable Use of Information Technology Standard and all other applicable DTMB policies and procedures.

Division Director or Section Supervisor/Manager/DTMB

Remove or deactivate any workforce member's user privileges, including but not limited to, user access accounts and access to secured areas, when necessary to preserve the integrity, confidentiality and availability of its facilities, user services and data.

REFERENCES

MDHHS 68D-070 PHI Use and Disclosure - Minimum Necessary Policy

MDHHS 68D-072 PHI Use and Disclosure - Minimum Necessary Procedure

45 CFR 164.310(b)

DTMB 1340.00.01 Acceptable Use of Information Technology

CONTACT

DTMB Client Service Center may be contacted at 517-241-9700.

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