

PURPOSE

The purpose is to establish the policy and procedure for the Michigan Department of Health and Human Services (MDHHS) to establish guidelines that require a record of the actions of a workforce member relative to the receipt and removal of hardware and/or software that contain Electronic Protected Health Information (ePHI) and sensitive information into and out of MDHHS facilities that are traceable to that workforce member.

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.

Trojan Horse means a program which appears to be benign, but has the potential to be malicious since it can capture sensitive information and compromise information by clandestinely sending it to an outside entity.

Virus means a man-made program or piece of code, often disguised, that replicates itself and causes unexpected and typically negative effects upon computers, applications and networks.

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.

POLICY

It is the policy of the MDHHS to document when necessary hardware or electronic media containing sensitive information or ePHI coming into the facility, as "clean" to assure that there is no type of virus or Trojan horse present that might allow an entity other than MDHHS to access the hardware. This may include testing of portable hardware brought back to MDHHS after being removed. Maintenance of hardware containing sensitive information or ePHI should be completed within the secured facility where the hardware resides. Removal of hardware from the secured areas for

maintenance purposes should be considered only if absolutely necessary.

PROCEDURE

Division Director or Section

Maintenance Logs

Supervisor/Manager

MDHHS shall keep a log of any hardware checked out for maintenance. The log shall contain:

- Name of the workforce member who is removing the item
- Date and time of checkout
- Description of the hardware including serial number
- Description of any PHI previously contained in the hardware
- Anticipated duration of checkout
- Maintenance problem being addressed

Incident Logs

MDHHS shall keep a log of media containing sensitive information or ePHI. The log shall contain:

- Name of the workforce member who checked out the media
- Date and time on which it was taken
- Date and time on which it was returned

Data Warehouse

For those MDHHS workforce members who have unrestricted access to the data in the data warehouse, a log shall be kept containing information related to what type of data they have access to and when they accessed that data.

REFERENCES

[45 CFR 164.302\(d\)\(1\)](#)

[Department of Management and Budget Procedure 1270.13: Internal Audit Plans](#)

[DTMB 1270.06: Annual Internal Audit Activities Reporting](#)

[DTMB 1270.12: Monitoring of Internal Controls Related to Information Technology](#)

CONTACT

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