

## PURPOSE

The purpose is to establish the policy and procedure for the Michigan Department of Health and Human Service (MDHHS) to ensure that MDHHS servers and workstations that access, transmit, receive or store Electronic Protected Health Information (ePHI) are appropriately controlled.

## 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.

## POLICY

It is the policy of the MDHHS to employ inactivity timers or automatic log out mechanisms on servers, workstations, or other computer systems containing ePHI repositories that that have been classified as high risk, under the HIPAA Security Risk Analysis.

## PROCEDURE

### **Workforce Member**

High risk systems as classified under the HIPAA Security Risk Analysis must terminate a user session after a maximum of, but not limited to, 15 minutes of inactivity.

Servers, workstations or other computer systems located in open, common or otherwise insecure environments, that access, transmit, receive or store ePHI must employ inactivity timers or automatic log out mechanisms.

Servers, workstations, or other computer systems that have access to, transmit, receive or store ePHI and are located in locked, secure

environments need not implement inactivity timers or automatic log out mechanisms.

If a system requires the use of an inactivity timer or automatic log out mechanism, but does not support an inactivity timer or automatic log out mechanism, one of the following procedures shall be implemented:

The system must be upgraded or moved to support the minimum HIPAA security automatic log out procedures

The system must be moved into a secure environment

All ePHI must be removed and relocated to a system that supports the minimum HIPAA security automatic log out procedures.

## REFERENCES

[45 CFR 164.308\(a\)\(1\)](#)

## CONTACT

For additional information concerning this policy and procedure, contact the MDHHS Security Officer at [MDHHSPrivacySecurity@michigan.gov](mailto:MDHHSPrivacySecurity@michigan.gov).