
PURPOSE

The purpose is to establish the policy and procedure for the Michigan Department of Health and Human Services (MDHHS) to implement procedures that will appropriately guard against the unauthorized modification of Electronic Protected Health Information (ePHI) that is being transmitted over an electronic communications network or via any form of removable media.

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.

Encryption means the manipulation of data to prevent accurate interpretation by all but those for whom the data is intended.

POLICY

It is the policy of MDHHS to implement procedures to encrypt ePHI whenever ePHI is transmitted. These procedures may vary depending on the type of transmission.

PROCEDURE

Workforce Members

The possibility of access to ePHI and secure data by individuals who are not the intended recipients of this data will be prevented by

encrypting the data, where applicable, by workforce members that are transmitting any ePHI or otherwise secure data.

The encryption method must be Advanced Encryption Standard (AES) compliant, which specifies the Federal Information Processing Standards.

REFERENCES

45 CFR 164.308(a)(1)

FIPS Publication 197 Advanced Encryption Standard (AES)

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

CONTACT

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