PURPOSE

The purpose is to establish the policy and procedure for the Michigan Department of Health and Human Services (MDHHS) to commit to compliance with all applicable laws, regulations and State of Michigan policies. MDHHS has adopted this policy and procedure to set forth its compliance with those standards established under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) regarding the security of Electronic Protected Health Information (ePHI).

The scope of this policy covers MDHHS' general approach to compliance with the security regulations. As a covered entity under the security regulations, MDHHS must:

1. Ensure the confidentiality, integrity and availability of all ePHI MDHHS creates, receives, maintains or transmits.

2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required.

4. Ensure compliance with the security regulations by its workforce. Compliance with the security regulations will require MDHHS to implement:

    - Administrative Safeguards--administrative actions, policies and procedures to manage the selection, development, implementation and maintenance of security measures to protect ePHI and to manage the conduct of MDHHS' workforce in relation to the protection of that information.

    - Physical Safeguards--physical measures, policies and procedures to protect MDHHS' electronic information systems and related buildings and equipment, from natural and environmental hazards and unauthorized intrusion.

    - Technical Safeguards--the technologies and the policy and procedures for its use that protect ePHI and control access to it.

REVISION HISTORY

Issued: 09/20/2006
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.

POLICY

It is the policy of MDHHS to abide by the following:

A Hybrid Entity

MDHHS is a hybrid entity under the security regulations with both covered and non-covered components. MDHHS covered components are set forth in the MDHHS organizational chart, as shown in the Appendix of the MDHHS Security Binder, which may be revised from time to time. In addition, when using or disclosing PHI, HIPAA covered components shall treat the non-covered components as if they were legally separate entities. References within the MDHHS HIPAA security policies to MDHHS mean the HIPAA covered entity components of MDHHS.

Security Personnel and Implementation

On behalf of its covered entity component parts the director of MDHHS shall appoint a Security Officer with overall responsibility for the development, implementation and maintenance of policies that conform to the security regulations (security policies). The Security Officer is responsible for ensuring that MDHHS complies with the HIPAA security policies.

The security regulations permit MDHHS to implement any security measure that allows it to reasonably and appropriately comply with a specific security standard in the security regulations. In determining which security measures to implement MDHHS must

take into account its size, complexity, capabilities, technical infrastructure, hardware and software security capabilities, the costs of the security measures and the probability and criticality of potential risks to ePHI.

Security Complaints

The Security Officer shall be responsible for facilitating a process for workforce members to file a complaint regarding MDHHS' security policies or the handling of ePHI by a MDHHS HIPAA covered component. The Security Officer shall be responsible for ensuring that the complaint and its disposition are appropriately documented and addressed.

Mitigation, Sanctions and Non-Retaliation

MDHHS shall ensure that its covered components mitigate damages for any violation of HIPAA security regulations. The MDHHS will use security policies and security procedures, appropriate discipline and sanction employees and other workforce members for any violation. MDHHS will refrain from intimidating or retaliating against any person for exercising his or her rights under the security regulations or for reporting any concern, issue or practice that such person believes in good faith to be in violation of the security regulations or the MDHHS security policies and procedures.

MDHHS shall not require any persons to inappropriately waive any rights of such person to file a complaint with the MDHHS.

Security Policies and Procedures

The MDHHS security policies and procedures are designed to ensure compliance with security regulations. Such security policies and procedures shall be kept current and in compliance with any changes in the law, regulations or practices of MDHHS' covered components.

PROCEDURE

The director of MDHHS must appoint a Security Officer.

The Security Officer must:

- Develop, implement and maintain policies and procedures that conform to the security regulations and is responsible for

ensuring that MDHHS complies with the HIPAA security policies.

- Facilitate a process for workforce members to file a complaint regarding MDHHS security policies or the handling of ePHI by a MDHHS HIPAA covered component. Ensure that the complaint and its disposition are appropriately documented and addressed.

Every member of the MDHHS workforce within a HIPAA covered component of MDHHS is responsible for being aware of and complying with the security regulations policies and procedures.

REFERENCES

45 CFR 164.306, 45 CFR 164.308

CONTACT

For more information regarding this policy, contact the MDHHS Compliance Office at MDHHSPrivacySecurity@michigan.gov.