PURPOSE

To identify and respond to suspected or known security incidents, mitigate (to the extent practicable) harmful effects of security incidents that are known to Michigan Department of Health and Human Services (MDHHS); and document security incidents and their outcomes.

REVISION HISTORY

Reviewed: 01/01/2024.
Next Review: 01/01/2025.

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.

Security Incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

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.

PROCEDURE

A common HIPAA Incident Response and Reporting System must be created and implemented to support the reporting, mitigation and documentation of HIPAA security incidents and violations.

All workforce members must complete a security incident report for each known or suspected security incident and forward the completed form to the MDHHS security officer. All incidents, threats or violations that affect or may affect the confidentiality, integrity or availability of ePHI must be reported using the following procedures:

- Users must notify Department of Technology, Management and Budget (DTMB) Client Service Center in a timely manner

for issues involving viruses, local attacks, denial of service (DOS) attacks, etc.

- Incidents directly affecting ePHI must be immediately reported to both (1) the immediate supervisor or manager of the workforce member's department, and (2) the MDHHS security officer. If the immediate supervisor or manager is unavailable, reporting processes should include the following steps:
    - Notify local DTMB Client Service Center. The local helpdesk must notify DTMB if the incident effects or may affect other systems and networks.
    - DTMB investigates and propagates recommended updates or fixes.
    - DTMB notifies the MDHHS security officer if there is a viable threat to ePHI.
    - It is the responsibility of each department, division, bureau, area or section, whichever appropriate, to aggregate and assess the severity of incidents within their departments, sections, areas or bureaus involving ePHI and report those incidents, when appropriate, to the MDHHS security officer. Incidents that should be reported include, but are not limited to:
        - Virus, worm or other malicious code attacks.
        - Network or system intrusions.
        - Persistent intrusion attempts from a particular entity.
        - Unauthorized access to ePHI, ePHI based system or ePHI based network.
        - ePHI data loss due to disaster, failure or error.

The MDHHS security officer and the MDHHS privacy officer shall notify each other of security or privacy issues if they determine that an incident or issue could affect the other office (privacy or security).

The MDHHS security officer shall notify DTMB if a security incident involves an outside entity.

Communications between DTMB and the MDHHS security officer shall be open so that DTMB has a pathway to directly notify the MDHHS security officer of incidents that may impact ePHI in MDHHS systems.

All HIPAA related incidents, security and privacy, must be logged and documented by each department, division, bureau, area or section, whichever is appropriate. The MDHHS security officer will be responsible for documenting and logging all incidents related to HIPAA security.

The MDHHS security officer shall notify the MDHHS supervisors and managers of policy updates and changes. The MDHHS security officer shall also make the department aware of any virus or other malicious software updates, state-wide threats to ePHI and all other appropriate security threats that it becomes aware of through DTMB.

MDHHS supervisors and managers must propagate recommendations, policy and procedure changes and security reminders to their departments. MDHHS managers and supervisors may receive updates by way of:

- MDHHS security officer policy updates.
- MDHHS security officer incident or threat updates.

All instances of failures, outages or data loss that involve critical ePHI must be reported to the MDHHS security officer.

All correspondence with outside authorities such as local police, FBI, media, etc. must go through the State Attorney General's Office (AGO).

REFERENCES

45 CFR 164.308(a)(6)

DTMB 1340.00.01, Acceptable Use of Information Technology.

DTMB 1340.00.110.01.01, Lost or Stolen State-Owned or Managed IT Equipment.

DTMB-0052, Lost or Stolen Equipment Report Form.

CONTACT

DTMB Client Service Center may be contacted at 1-9700 or 1-800-968-2644 or by emailing DTMBservice@michigan.gov.

For more information regarding this procedure, contact the MDHHS Compliance and Data Governance Bureau at MDHHSPrivacySecurity@michigan.gov.