

PURPOSE

The purpose is to establish the policy and procedure for the Michigan Department of Health and Human Services (MDHHS) to establish the requirement for MDHHS to have a documented security plan to safeguard its facilities from unauthorized physical access and to safeguard the equipment therein from unauthorized physical access, tampering, and theft.

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.

Physical Access Control Mechanism is any mechanism that limits access to any physical location. Code locks, badge readers and key locks are examples of physical access control mechanisms.

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.

FTI is the acronym for Federal Tax Information. It is information received from the Internal Revenue Service (IRS) pertaining to tax return information.

POLICY

It is the policy of the MDHHS in accordance with Department of Technology Management and Budget (DTMB) Procedure 0250.01: Security and Safety Measures that DTMB will ensure that steps are taken that provide for the security of property as well as for the safety of workforce members, tenants and visitors in DTMB managed facilities. DTMB services will include but are not limited to: locking and unlocking of doors to the buildings, providing

periodic security checks, and keeping logs and records of access outside of regular business hours.

MDHHS will direct questions and concerns regarding matters of physical security to the applicable facility manager.

MDHHS shall comply with the Department of Technology Management and Budget policies and procedures.

National Institute of Standards and Technology (NIST)
Recommendations for Minimum Security Controls for Information Systems:

- NIST has released a Special Publication, 800-53, which recommends minimum security controls for federal systems that NIST has categorized as having low or moderate protection needs.
- The following are examples of physical security measures used to prevent unauthorized physical access:
 - Prominently marking restricted areas and separating them from non-restricted areas by physical barriers.
 - Controlling/manning main entrances to restricted areas.
 - Using cameras or electronic detection devices, such as card keys, to control access to secondary entrances.
 - Investigating apparent security violations and resolving them, if necessary.
 - Requiring staff and visitors to wear identification badges.
 - Ensuring that emergency exits and reentry procedures allow only authorized personnel to reenter restricted areas after emergency or drill.

PROCEDURE

Workforce Member

All workforce members must abide by the Department of Technology Management and Budget (DTMB) Procedure 0210.06 regarding appropriate conduct on State property.

Wear and display their MDHHS badge at all times when at their workplace.

Present a current identification card to security personnel when entering any building outside of regular business hours.

Return issued keys and identification cards to their respective personnel offices upon their termination of employment or when required by the Tenant Services Division (TSD). No workforce member shall duplicate any key issued.

Report a lost key immediately in writing to the facility manager. This report must include the circumstances of the loss.

Workforce Member/Vendor

All workforce members or vendors must sign the register maintained at the lobby desk or designated security entrance in each building when entering a building outside of regular business hours. Workforce members unsure of the proper entrance to the facility outside of regular business hours should contact the appropriate facility manager.

Do not remove office equipment from the buildings without approval from an authorized official of the department involved. If permission is given to remove equipment, the security officer will record the name of the workforce member or vendor and the type of equipment removed.

Visitors

Visitor access will be monitored in accordance with Department of Technology Management and Budget (DTMB) Procedures 0250.01.

All visitors requiring access to facilities containing ePHI-based systems must sign in providing information regarding their identity and the purpose of their visit.

Provide a temporary identification badge or be escorted to and from their destination.

Division Director or Section Supervisor/Manager

A physical access control mechanism must be utilized to control physical access to all facilities containing ePHI-based systems.

REFERENCES

45 CFR 164.310(a)(1)
DTMB 0250.01 Security Measures at State Facilities

CONTACT

DTMB 0210.06 Conduct on State Property

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