PURPOSE

To ensure that only authorized users (or processes, devices or other information systems functioning on behalf of authorized users) are provided access to a Michigan Department of Health and Human Services (MDHHS) information system under specified conditions.

REVISION HISTORY

Issued: 10/01/2020.
Next Review: 10/01/2021.

DEFINITIONS

Confidential Information

Sensitive information wherein unauthorized disclosure could cause serious financial, legal or reputational damage to an Agency or the SOM. Confidential data may include personally identifiable information (PII) or confidential non-public information that relates to an Agency's business.

Electronic Protected Health Information (ePHI)

Protected Health Information that is transmitted or maintained in electronic form.

Federal Tax Information (FTI)

Information that consists of federal tax returns and return information (and information derived from it) covered by the confidentiality protections of the Internal Revenue Code (IRC). FTI includes return or return information received directly from the IRS or obtained through an authorized secondary source, such as Social Security Administration (SSA), Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS),Centers for Medicare and Medicaid Services (CMS), or another entity acting on behalf of the IRS.

Personally Identifiable Information (PII)

Any information about an individual maintained by an agency with respect to, but not limited to, education, financial transactions, medical history, and criminal or employment history, and information that can be used to distinguish or trace an individual's identity (e.g., name, Social Security Number, date and place of birth, mother's maiden name, biometric records) including any other personal information linked or linkable to an individual..

Protected Health Information (PHI)

Individually identifiable health related information that is collected by a HIPAA covered entity or component and is transmitted by, or maintained in, electronic or any other form or medium.

Workforce Member

Includes full and part-time employees, affiliates, associates, students, volunteers, contractors, and staff from third party entities.

POLICY

MDHHS must protect the confidentiality and integrity of information by implementing safeguards to manage and enforce authorizations for access to information and system resources.

In compliance with Department of Technology, Management and Budget (DTMB) 1340.00, Information Technology Information Security Policy, MDHHS must ensure implementation of all moderate baseline security controls catalogued in the National Institute of Standards and Technology (NIST) Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations (Revision 4) from the NIST Computer Security Resource Center. This policy sets forth requirements from the access control [AC] family of NIST controls managed by MDHHS in accordance with DTMB 1340.00.020.01, Access Control Standard. MDHHS must review this policy annually.

Where applicable, this policy requires compliance with other federal and state laws, rules and regulations, policies, standards or other guidelines, including but not limited to the following:

- Centers for Medicare and Medicaid Services (CMS) Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges (MARS-E)
- Federal Bureau of Investigation Criminal Justice Information Services (CJIS) Security Policy.
- Internal Revenue Service (IRS) Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies and Entities
- Social Security Administration (SSA) Technical System Security Requirements (TSSR)

- U.S. Department of Health and Human Services Health Insurance Portability and Accountability Act (HIPAA), 45 CFR Part 160 and Part 164, Subparts A and C

Account Management [AC-2]

MDHHS must:

- Identify and select the following types of information system accounts to support department mission/business functions: individual, group, system, application, guest/anonymous, emergency, and temporary.
- Assign account managers for information system accounts.
- Establish conditions for group and role membership.
- Specify authorized users of the information system, group and role membership, and access authorizations (for example, privileges) for each account.
- Require approvals by an authorized requestor for requests to create information system accounts.
- Establish standards and procedures for creating, enabling, modifying, disabling, and removing accounts for each account type. These procedures include the following activities:
    - Authorizing information system access based on:
        - A valid access authorization.
        - Intended system usage.
        - With information systems that receive, process, store, or transmit FTI, a valid access authorization, need-to-know permission, and under the authority to disclose FTI under the provisions of IRC §6103.
        - Account, type of account, or a combination of both.
        - System-related requirements such as scheduled maintenance and system upgrades.
        - Mission/business requirements such as time zone differences, customer requirements, and remote access to support travel requirements.

- Other attributes required for authorizing access, such as restrictions on time-of-day, day-of-week, and point-of-origin.

- Monitoring the use of information system accounts.
- Notifying account managers:
  - To close unneeded accounts when accounts are no longer required.
  - When users are terminated or transferred.
  - When individual information system usage or need-to-know changes.
- Establishing a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.
- Reviewing accounts for compliance with account management requirements at a minimum of annually for user accounts and semi-annually for privileged accounts.

Account Information System Account Management [AC-2(1)]

MDHHS must employ automated mechanisms to support the management of information system accounts. This can include using the information system, email, text messaging, or telephonic communication to automatically monitor account usage, including termination or transfer of user accounts and atypical system account usage.

Removal of Temporary/Emergency Accounts [AC-2(2)]

MDHHS must employ automatic mechanisms to disable temporary accounts automatically after thirty days and within twenty-four hours for emergency accounts.

Disable Inactive Accounts [AC-2(3)]

MDHHS must employ automatic mechanisms to disable inactive user accounts after sixty days and system accounts after one-hundred-twenty days of inactivity.

Automated Audit Actions [AC-2(4)]

MDHHS must employ automatic mechanisms to audit account creation, modification, disabling, and removal actions and notifies,

as required, appropriate individuals such as account managers, system owners, as defined in the system security plan.

Role-Based Schemes [MARS-E AC-2(7)]

MDHHS must:

- Establish and administer privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles.
- Establish and administer application-specific privileged user accounts in accordance with a role-based access scheme that allows access based on user responsibilities associated with application use.
- Monitor privileged role assignments as well as application-specific privileged role assignments.
- Inspect administrator groups, root accounts, and other system-related accounts on demand, and at least one every fourteen days to ensure that unauthorized accounts have not been created. Privileged user roles associated with applications should be inspected every thirty days.

Access Enforcement [AC-3]

MDHHS must ensure that the information system enforces:

- Authorizations approved by Michigan Cyber Security (MCS) for logical access to the system resources in accordance with applicable access control policies.
- With information systems that receive, process, store, or transmit FTI, a role-based access control policy over defined subjects and objects and control access based upon a valid access authorization, intended system usage, and the authority to disclose FTI under the provisions of IRC §6103.

Access Enforcement - Controlled Release [MARS-E AC-3(9)]

MDHHS must ensure that the information system does not release information outside of the established system boundary unless:

- The receiving department information system or system component provides comparable security safeguards.

- Safeguards consistent with 45 CFR §155.260, paragraph (b)(2) are used to validate the appropriateness of the information designated for release.

Separation of Duties [AC-5]

MDHHS must:

- Separate duties of workforce members as necessary to prevent harmful activity without collusion.
- Document separation of duties.
- Define information system access authorizations to support separation of duties.

Least Privilege [AC-6]

MDHHS must employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with department missions and business functions.

Authorize Access to Security Functions [AC-6(1)]

MDHHS must, at a minimum, explicitly authorize access to the following list of security functions (deployed in hardware, software, and firmware) and security-relevant information for all system components:

- Setting/modifying audit logs and auditing behavior.
- Setting/modifying boundary protection system rules.
- Configuring/modifying access authorizations (such as permissions, privileges).
- Setting/modifying authentication parameters.
- Setting/modifying system configurations and parameters.

Non-Privileged Access for Non-Security Functions [AC-6(2)]

MDHHS must, at a minimum, require that users of information system accounts, or roles, with access to the following list of security functions or security-relevant information, use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audit any use of privileged accounts, or roles, for such functions:

- Setting/modifying audit logs and auditing behavior.
- Setting/modifying boundary protection system rules.
- Configuring/modifying access authorizations (such as permissions, privileges).
- Setting/modifying authentication parameters.
- Setting/modifying system configurations and parameters.

Privileged Accounts [AC-6(5)]

MDHHS must limit authorization to privileged accounts on the information system to roles designated by the system owner and/or data custodian.

Auditing Use of Privileged Functions [AC-6(9)]

MDHHS must ensure that the information system audits the execution of privileged functions to detect misuse.

Prohibit Non-Privileged Users from Executing Privileged Functions [AC-6(10)]

MDHHS must ensure that the information system prevents non-privileged users from executing privileged functions. This includes disabling, circumventing, or altering implemented security safeguards/countermeasures.

Unsuccessful Logon Attempts [AC-7]

MDHHS must ensure that the information system enforces a DTMB-specified limit of consecutive invalid logon attempts by a user; and automatically locks the account/node for a DTMB-specified time period or locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded, consistent with DTMB 1340.00.020.01, Access Control Standard.

System Use Notification [AC-8]

MDHHS must ensure that the information system:

- Displays an approved system use notification message or warning banner before granting access to the system that provides privacy and security notices consistent with applicable state and/or federal laws, executive orders, directives, policies,

regulations, standards, and guidance. The approved message states that:

- Users are accessing a State of Michigan information system.
- Usage may be monitored, recorded and subject to audit.
- Unauthorized use of the system is prohibited and subject to criminal and civil penalties.
- Use of the system indicates consent to monitoring and recording.

- Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system.
- For publicly accessible systems:
  - Displays system use information before granting further access.
  - Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities.
  - Includes a description of the authorized uses of the system.

Session Lock [AC-11]

MDHHS must ensure that the information system:

- Prevents further access to the system by initiating a session lock after ten minutes of inactivity of an operating system, after fifteen minutes of inactivity for applications, or upon receiving a request from a user.
- Retains the session lock until the user reestablishes access using established identification and authentication procedures.

Pattern-Hiding Displays [AC-11(1)]

MDHHS must ensure that the information system employs a session lock mechanism, when activated on a device with a display screen, places a publicly viewable pattern (an image that does not

convey sensitive information) onto the associated display, concealing what was previously visible on the screen.

Session Termination [AC-12]

MDHHS must define conditions and trigger events requiring automatic session termination of user applications (i.e. user-initiated logical sessions) and ensure that the information system enforces these parameters.

Permitted Actions without Identification or Authentication [AC-14]

MDHHS must:

- Identify, document, and provide supporting rationale in the system security plan for user actions not requiring identification or authentication.
- Configure the information system to permit public access without first requiring individual identification and authentication only to the extent necessary to accomplish mission objectives.

Information Sharing [AC-21]

MDHHS must facilitate information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for department-defined circumstances; and must employ mechanisms or processes to assist users in making information sharing/collaboration decisions.

Publicly Accessible Content [AC-22]

MDHHS must:

- Designate individuals authorized to post information onto a publicly accessible information system.
- Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information.
- Review the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included.

- Review the content on the publicly accessible information system for nonpublic information bi-weekly and removes such information, if discovered.

ROLES AND RESPONSIBILITIES:

The MDHHS security officer and privacy officer must determine roles and responsibilities for Compliance and Data Governance Bureau personnel to support implementation of this policy.

MDHHS workforce members are responsible for reading, understanding, and complying with policies, standards, and procedures based on access controls.

ENFORCEMENT

Violations of this policy or failure to implement provisions of this policy may result in disciplinary action up to and including termination, civil litigation, and/or criminal prosecution.

REFERENCES

Federal Standards/Regulations:

NIST 800-53 rev.4:

AC-1 Access Control Policy and Procedures
AC-2 Account Management
AC-2(1) Account Information System Account Management
AC-2(2) Removal of Temporary/Emergency Accounts
AC-2(3) Disable Inactive Accounts
AC-2(4) Automated Audit Actions
AC-3 Access Enforcement
AC-5 Separation of Duties
AC-6 Least Privilege
AC-6(1) Authorize Access to Security Functions
AC-6(2) Non-Privileged Access for Non-Security Functions
AC-6(5) Privileged Accounts
AC-6(9) Auditing Use of Privileged Functions
AC-6(10) Prohibit Non-Privileged Users from Executing Privileged Functions
AC-7 Unsuccessful Logon Attempts
AC-8 System Use Notification
AC-11 Session Lock
AC-11(1) Pattern-Hiding Displays

AC-12 Session Termination
AC-14 Permitted Actions Without Identification or Authentication
AC-21 Information Sharing
AC-22 Publicly Accessible Content

MARS-E 2.0

AC-2(7) Role-Based Schemes
AC-3(9) Access Enforcement – Controlled Release

IRS Publication 1075

9.3.1.2 Account Management
9.3.1.3 Access Enforcement

45 CFR §164.308(a)(3)

164.308(a)(3)(i) Workforce Security (R)
164.308(a)(3)(ii)(A) Authorization and/or Supervision (A)
164.308(a)(3)(ii)(B) Workforce Clearance Procedure (A)
164.308(a)(3)(ii)(C) Termination Procedure (A)

45 CFR §164.308(a)(4)

164.308(a)(4)(i) Information Access Management
164.308(a)(4)(ii)(B) Access Authorization (A)
164.308(a)(4)(ii)(C) Access Establishment and Modification (A)

45 CFR §164.308(a)(5)

164.308(a)(5)(ii)(C) Log-in Monitoring (A)

45 CFR §164.310

164.310(a)(2)(iii) Access Control and Validation Procedures (A)
164.310(b) Workstation Use (R)

45 CFR §164.312(a)

164.312(a)(1) Access Control (R)
164.312(a)(2)(ii) Emergency Access Procedure (R)
164.312(a)(2)(iii) Automatic Logoff (A)

State Standards/Regulations:

MDHHS Policy Manuals

- 68E-040 Authorization and or Supervision Policy and Procedure
- 68E-050 Termination Policy and Procedure
- 68E-060 Workforce Clearance Policy and Procedure
- 68E-070 Access Authorization Policy and Procedure
- 68E-080 Access Establishment and Modification
- 68E-090 Login Monitoring
- 68E-200 Access Control and Validation Policy and Procedure
- 68E-240 Workstation Use Policy and Procedure
- 68E-300 Automatic Log Out Policy and Procedure

DMB Administrative Guide

DTMB IT Technical Policies, Standards and Procedures

- 1340.00.020.01 Access Control Standard

CONTACT

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