PURPOSE

Michigan Department of Health and Human Services (MDHHS) employees must ensure that all suspected or actual privacy and security breaches, incidents and violations, including unauthorized or impermissible uses or disclosures, are appropriately identified, reported, documented, responded to, mitigated to the extent practicable, and evaluated for the implementation of breach notification procedures when required by law.

REVISION HISTORY

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

DEFINITIONS

Breach

The unauthorized acquisition, access, use, or disclosure of confidential information, Federal Tax Information (FTI), Personally Identifiable Information (PII), or Protected Health Information (PHI) that compromises its security or privacy.

Confidential Information

Sensitive information wherein unauthorized disclosure could cause serious financial, legal or reputational damage to an agency or the State of Michigan (SOM). Confidential information may include personal identifying information (PII) or confidential non-public information that relates to an Agency's business.

Electronic Protected Health Information (EPHI)

Protected Health Information 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 Internal Revenue Service (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),or Centers for Medicare and Medicaid Services (CMS), or another entity acting on behalf of the IRS.

Impermissible Use or Disclosure

The acquisition, access, use, or disclosure of confidential information, FTI, PII, or PHI in a manner not permitted under HIPAA or other applicable confidentiality laws that may or may not compromise the security or privacy of the confidential information, FTI, PII, or PHI.

Incident

An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. Includes privacy incidents involving the actual or potential unauthorized disclosure of personally identifiable information.

IRS Office of Safeguards

The office within the Internal Revenue Service responsible for ensuring federal, state, and local agencies receiving federal tax information protect it as if the information remained in IRS's hands.

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 (such as 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 collected by a HIPAA covered entity or component transmitted by, or maintained in, electronic or any other form or medium.

SSA-Provided Information

Confidential information provided by the Social Security Administration (SSA).

Treasury Inspector General for Tax Administration (TIGTA)

TIGTA provides independent oversight of IRS activities to prevent and detect fraud, waste, and abuse.

Workforce Member

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

POLICY

MDHHS must implement procedures to address suspected or actual privacy or security breaches, security incidents and violations, including unauthorized or impermissible uses or disclosures of confidential information, FTI, PII, or PHI and create documented procedures defining the process for reporting such occurrences.

A reasonable security incident reporting mechanism for electronic confidential information, FTI, PII, or PHI tested by MDHHS on a regular basis.

MDHHS must have a documented process that alerts appropriate authorities in the event of an information security threat, incident or other lapse in information security.

MDHHS must put in place procedures and processes to report, document and track breaches, security incidents, and unauthorized or impermissible uses or disclosures of confidential information, FTI, PII, or PHI including but not limited to, recording incidents and how they were handled (for example what happened, when, cause, mitigation, prevention, who performed and when).

Incident Investigation and Risk Assessment

Following receipt of a report of unauthorized use or disclosure of PHI, PII and/or other confidential information, the MDHHS Compliance and Data Governance Bureau must conduct and document the results of an incident investigation, including a risk assessment by completing a Data Risk Assessment Form.

Include all the following factors in the incident investigation and risk assessment:

- The nature and extent of the PHI, PII and/or other confidential information involved, including the types of identifiers and the likelihood of re-identification.
- The unauthorized person or entity who used the information or made the disclosure.
- Whether the information was acquired or viewed.
- The extent to which the risk to affected individuals has been mitigated.
- Whether the information was secured (encrypted and rendered unusable, unreadable, or indecipherable to unauthorized persons.)

Presume a breach has occurred unless bureau personnel conducting the investigation and risk assessment find a low probability that PHI, PII and/or other confidential information has been compromised.

The following conditions constitute exceptions to a reportable breach and must be accounted for in the risk assessment:

- Any unintentional acquisition, access, or use of such information by a workforce member, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure not permitted by the privacy rule.
- Any inadvertent disclosure by one person who is authorized to access such information to another person likewise authorized, provided the information received is not further used or disclosed in a manner not permitted by the privacy rule.
- A disclosure of information where a workforce member has a good faith belief the unauthorized recipient would not reasonably be able to retain the information.

Required Notifications following a Breach

If bureau personnel determine through a risk assessment that a breach of unsecured PHI, PII and/or other confidential information had taken place, timely notification of the breach to affected individuals, entitles, and, in certain circumstances, to the media, is required.

- Bureau personnel must use a notice letter which includes the following:
    - A brief description of the breach
    - A description of the types of information that were involved in the breach.
    - The steps affected individuals should take to protect themselves from potential harm.
    - A brief description of what MDHHS is doing to investigate the breach, mitigate the harm, and prevent further breaches.
    - Contact information for the covered entity (or business associate, as applicable).

Provide breach notification to the affected individual(s) as required under the Michigan Identity Theft Protection Act.

Breach of SSA-Provided Information - Notice to SSA

If MDHHS experiences or suspects a breach or loss of PII or a security incident, which includes SSA-provided information, the MDHHS security officer or privacy officer must notify the state official responsible for systems security designated in the agreement. That state official or delegate must then notify the SSA regional office contact or the SSA systems security contact identified in the agreement. If, for any reason, the responsible state official or delegate is unable to notify the SSA regional office or the SSA systems security contact within one hour, the responsible state agency official or delegate must report the incident by contacting SSA's National Network Service Center (NNSC) toll free at 877-697-4889; select *security and PII reporting* from the options list). MDHHS will provide updates as they become available to the SSA contact, as appropriate.

Breach of FTI - Notice to Internal Revenue Service

If MDHHS experiences or suspects a breach or loss of PII or a security incident, which includes FTI, the MDHHS security officer or privacy officer must notify TIGTA and the IRS Office of Safeguards immediately, but no later than 24 hours after discovery of the suspected or known improper inspection or disclosure. Notification must not wait until an internal investigation is conducted. Contact information can be found in the IRS Publication 1075

Breach of PHI - Individual Notice

Bureau personnel will provide individual notice without unreasonable delay, and in no case later than 60 days following the discovery of a breach, in written form by first-class mail, or alternatively, by email if the affected individual has agreed to receive such notices electronically.

- If MDHHS has insufficient or out-of-date contact information for 10 or more individuals, Bureau personnel must provide substitute individual notice by either posting the notice on the home page of its web site for at least 90 days or by providing the notice in major print or broadcast media where the affected individuals likely reside. The notice must include a toll-free phone number that remains active for at least 90 days where individuals can learn if their information was involved in the breach. If MDHHS has insufficient or out-of-date contact information for fewer than 10 individuals, Bureau personnel may provide substitute notice by an alternative form of written notice, by telephone, or other means.

- Delegation to of Individual Notice to Business Associate: MDHHS as the covered entity may delegate the responsibility of providing individual notices to the business associate, depending on various circumstances, such as the functions the business associate performs on behalf of the covered entity and which entity has the relationship with the individual.

Breach of PHI - Notice to Secretary of the U.S. Department of Health and Human Services (HHS)

In the event a breach affects 500 or more individuals, bureau personnel will notify HHS at the same time notice is made to the affected individuals, by visiting the HHS web site and filling out and electronically submitting a breach report form. If fewer than 500 individuals are affected, bureau personnel will maintain a log of the breaches to be submitted annually to HHS no later than 60 days after the end of each calendar year, in the manner specified on the HHS website, along with all other breaches discovered during the preceding calendar year.

Breach of PHI - Notice to Media

In the event of a breach affecting more than 500 individuals, bureau personnel must provide notice to prominent media outlets serving the state or jurisdiction, without unreasonable delay and in no case

later than 60 days following the discovery of a breach. Notice may take the form of a press release but must include the same information required for the individual notice.

Breach of PHI - Notification to MDHHS by Business Associate

If a breach of unsecured protected health information occurs at or by a business associate, the business associate must notify bureau personnel without unreasonable delay and no later than 60 days from the discovery of the breach. To the extent possible, the business associate should provide bureau personnel with the identification of everyone affected by the breach as well as any other available information required to be provided in its notification to affected individuals.

PROCEDURE

MDHHS Security Officer

The MDHHS security officer is responsible for:

- General oversight of procedures and processes involving reporting, investigation, mitigation, notification and documentation of breaches, security incidents, and unauthorized or impermissible uses or disclosures of confidential information, FTI, PII, or PHI.
- Notifying the Department of Technology, Management and Budget (DTMB) if a security incident involves an outside entity.
- Through collaboration with DTMB, maintaining department awareness of:
    - Viruses or other malicious software.
    - State-wide threats to electronic confidential information, FTI, PII, or PHI.
- All other security threats. Notifying MDHHS supervisors and managers of policy updates and changes.
- Conducting a post-incident review to ensure this incident response policy and procedure provides adequate guidance.
- Ensuring workforce members with access to confidential information, FTI PII or PHI receive training on this incident response policy and procedure.

Department of Technology, Management and Budget/MDHHS Security Officer

DTMB and the MDHHS security officer must maintain open communication so that DTMB has a pathway to directly notify the MDHHS security officer of incidents that may impact electronic confidential information, FTI, PII, or PHI in MDHHS systems.

Division Director or Section Supervisor/Manager

The division director or section supervisor/manager must document and report all breaches, security incidences, and unauthorized or impermissible uses or disclosures of confidential information, FTI, PII, or PHI.

The division director or section supervisor/manager must propagate recommendations, policy and procedure changes and security reminders to their areas. MDHHS managers and supervisors may receive updates by way of:

- MDHHS privacy and security officer policy updates.
- MDHHS security officer Incident or threat updates.

MDHHS Compliance and Data Governance Bureau Personnel

Bureau personnel are responsible for the following:

- Receipt of completed DCH-1422, HIPAA/Data Incident Report, form and related documentation.
- Investigating reported incidents and performing risk assessments to determine if a breach has taken place and the risk of harm.
- In the event of a breach, notifies affected individuals, federal agencies, and media as required according to the type of information involved, as required by law.
- Tracking and documenting actions taken to investigate, assess, mitigate, and communicate as required by law.

Workforce Member

All workforce members must complete an incident report for each known or suspected incident and forward the completed form to the privacy and security officers at MDHHSPrivacySecurity@michigan.gov. All breaches, security

incidents, and unauthorized or impermissible uses or disclosures of confidential information, FTI, PII, or PHI, threats or violations that affect or may affect the confidentiality, integrity or availability of FTI, PII, or PHI must be reported using the following procedures:

Users must notify DTMB Client Service Center in a timely manner for issues involving viruses, local attacks, Denial of Service (DOS) attacks, etc.

Incidents that involve confidential information, FTI, PII, or PHI must be immediately reported to:

1. The immediate supervisor or manager of the workforce member's department.

2. The MDHHS privacy and security officers.

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 FTI, PII, or PHI.
- Incidents that must 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 or disclosure of: FTI, PII or PHI; FTI, PII or PHI-based system; or FTI, PII, or PHI-based networks.
    - FTI, PII, or PHI data loss due to disaster, failure or error.
    - Unauthorized or impermissible uses or disclosures of confidential information, FTI, PII, or PHI in any format.

Report all instances of failures, outages or data loss that involve FTI or PHI to the MDHHS security officer.

All correspondence with outside authorities such as local police, FBI, IRS, SSA, media, etc. must go through the MDHHS privacy and security officers.

REFERENCES

Public Act 452 of 2004

45 CFR 164.402

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 IT or Managed Equipment.

DTMB-0052, Lost or Stolen Equipment Report Form.

MCL 445.61 et seq.

CONTACT

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