PURPOSE

The State of Michigan and the Michigan Department of Health and Human Services (MDHHS) apply appropriate sanctions against workforce members who fail to comply with data privacy and security policies and procedures controlling the appropriate access, use, or disclosure of Protected Health Information (PHI) in accordance with applicable laws and regulations.

REVISION HISTORY

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

DEFINITIONS

Covered Entity

Health care organizations and other types of organizations/entities to which the HIPAA Regulations apply.

Electronic Protected Health Information (ePHI)

Protected Health Information transmitted or maintained in electronic form.

Federal Information Database (FID)

A database of information maintained by the federal government that contains confidential or personal information, including, but not limited to, federal tax information.

Federal Tax Information (FTI)

Consists of tax returns and tax return information. FTI can be either or both. FTI is any return or return information received from the IRS or an IRS secondary source, such as the Social Security Administration, Federal Office of Child Support Enforcement, Bureau of Fiscal Services, or the Center of Medicare and Medicaid Services (CMS). Statute or regulations may also allow FTI sharing.

HIPAA

The Health Insurance Portability and Accountability Act of 1996, as amended.

Protected Health Information (PHI)

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

Sanction

An official course of action taken or imposed in response to a noted violation or instance of non-compliance with applicable regulations, policies and procedures.

Violation

Any action that is not in accordance with applicable regulations, policies and procedures.

Workforce Member

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 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

Protected health information (PHI) is confidential and protected from access, use, or disclosure except to authorized individuals requiring access to such information. Attempting to obtain or use, actually obtaining or using, or assisting others to obtain or use PHI, when unauthorized or improper, in violation of MDHHS data privacy and security policies, may be grounds for disciplinary action up to and including termination of employment or contractual agreement and loss of professional privileges.

MDHHS will appropriately apply sanctions to workforce members for any violations of privacy and security policies and procedures and will investigate and reasonably mitigate privacy and security violations and incidents in a timely manner. Privacy and security sanctions commensurate with the gravity of the implications will be enforced by human resources in conjunction with union contracts and current civil service policies and procedures.

SANCTIONS

Workforce members found to have violated this policy will be sanctioned, up to and including termination. Sanctions may include, but are not limited to, training, written counseling, written reprimand, unpaid suspension, interim service rating, demotion or termination.

A person who knowingly obtains or discloses individually identifiable health information may face criminal and civil penalties under federal and state law.

Except where otherwise required by law, the type of sanction administered by MDHHS will depend on the facts and circumstances of each case. Human resources determine the appropriate sanction and will work with the impacted departments, Compliance and Data Governance, and MDHHS Legal Affairs where necessary.

PENALTIES

Offenses in violation of HIPAA are subject to civil and criminal prosecution.

Civil Penalties

Individual who Unknowingly Violate HIPAA

$100 fine per violation with annual maximum of $25,000 for repeated violations. There is also $50,000 for repeat violations, and an annual maximum of $1.5 million.

Violation Due to Reasonable Cause and not Willful Neglect

There is $1000 charge per violation, an annual maximum of $100,000 for repeat violations. There is also $50,000 penalty per violation and an annual maximum of $1.5 million.

HIPAA Violation due to Willful Neglect, Violation Corrected Within the Required Period

There is $10,000 penalty per violation, an annual maximum of $250,000 for repeat violations. There is $50,000 penalty per violation with an annual maximum of $1.5 million.

HIPAA Violation due to Willful Neglect and Not Corrected

There is a penalty of $50,000 per violation, and an annual maximum of $1.5 million.

Note: For unauthorized inspection or disclosure, the penalty is $1,000 for each unauthorized access or disclosure, or actual damages, whichever is greater, plus punitive damages in the case of willful or gross negligence.

Criminal Penalties

- For covered entities and specified individuals who obtain or disclose individually identifiable health information willfully and knowingly: The penalty is up to $50,000 and imprisonment up to 1 year.
- For offenses committed under false pretenses, the penalty is up to $100,000 with imprisonment up to 5 years.
- For offenses committed with the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain or malicious harm, the penalty is up to $250,000 with imprisonment up to 10 years.

Offenses in violation of FTI are subject to civil and criminal prosecution.

- Willful unauthorized disclosure of returns or return information by an employee or former employee is a felony.
- The penalty can be a fine of up to $5,000 or up to five years in prison, or both, plus costs of prosecution.
- Willful unauthorized access or inspection of taxpayer records by an employee or former employee is a misdemeanor.
- Violators can be subject to a fine of up to $1,000 and/or sentenced to up to one year in prison.

  Note: MDHHS reserves the right to refer matters for civil or criminal prosecution which may include notifying law enforcement officials and regulatory accreditation and licensure organizations.

REFERENCES

45 CFR 164.308(a)(1)

Michigan Department of Health and Human Services Work Rules

Mental Health Code: Record Confidentiality 330.1748 Confidentiality Sec. 748

Public Health Code 368

HIV/AIDS Confidentiality MCL 333.5131; Public Act 488 of 1988, as amended

Michigan Civil Service Commission Rules, Chapter 2: Employment Provisions, 2-6 Discipline

CONTACT

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