PURPOSE

To establish policy that must be implemented by the Michigan Department of Health and Human Services (MDHHS) workforce members regarding cloud-based storage and computing solutions to ensure the confidentiality, integrity, and availability of information created and maintained by MDHHS.

REVISION HISTORY

Reviewed:01/01/2026.
Next Review: 01/01/2027.

DEFINITIONS

CSP is the acronym for Cloud Service Provider.

Cloud-based Email is storing and accessing email over the Internet (ex. Gmail, Yahoo and Hotmail).

Cloud-based Storage is storing, sharing, or accessing data over the Internet instead of your computer's hard drive (ex. GoogleDrive, DropBox, SharePoint, and OneDrive).

SaaS is the acronym for Software-as-a-Service, a software licensing and delivery model in which software is licensed on a subscription basis and accessed over the Internet (ex. Office 365 and GoogleDocs).

IaaS is the acronym for Infrastructure-as-a-Service, a cloud computing form that provides computing resources over the internet. Cloud IaaS providers host infrastructure components for users (ex. Amazon, Microsoft, Google, and Rackspace).

PaaS is the acronym for Platform-as-a-Service, a category of cloud computing services that provides a platform allowing customers to develop, run, and manage web applications without building and maintaining the infrastructure associated with developing and launching an app (ex. SalesForce and Amazon).

PII is the acronym for Personally Identifiable Information. It is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

PHI is the acronym for Protected Health Information. It is 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.

It excludes individually identifiable health information in: (a) education records covered by the Family Educational Rights and Privacy Act (FERPA); and (b) employment records held by the MDHHS in its role as employer.

ePHI is the acronym for Electronic Protected Health Information. It is health related data pertaining to an individual who can be identified and is in electronic format.

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

SSPI is the acronym for Social Security-Provided Information. It is data received or accessed from the Social Security Administration (SSA) as defined by MDHHS' Information Exchange Agreement (IEA) with SSA for the purpose of administrating federally funded and/or state-administered programs.

POLICY

Use of cloud computing services for work purposes must be formally authorized by the MDHHS chief Compliance and Data Governance Bureau officer who will evaluate risk and certify that security, privacy and all other applicable state and federal requirements will be adequately addressed by the CSP. The use of such services must comply with all laws and regulations governing the handling of PII, PHI, ePHI, FTI, SSPI, and other sensitive data created or maintained by MDHHS. The MDHHS Compliance and Data Governance Bureau determines what data may or may not be stored and/or processed in the cloud.

The use of a storage or computing solution in which the CSP stores MDHHS data on servers outside of the United States is not permitted.

Personal cloud storage and computing accounts may not be used for the storage, manipulation or exchange of MDHHS data (such as DropBox, GoogleDrive, OneDrive). Conversely, any MDHHS approved cloud-based storage or computing service may not be used for personal use.

For cloud services that require users to agree to terms of service, such agreements must be reviewed and approved by the Department of Technology, Management and Budget (DTMB).

The use of cloud services must comply with DTMB 1340.00.130.02, Acceptable Use of Information Technology Standard.

For HIPAA covered components of MDHHS, a CSP is a business associate when the covered component engages the services of the CSP to create, receive, maintain, or transmit ePHI (such as to process and/or store ePHI) on its behalf. A HIPAA-compliant Business Associate Agreement (BAA) is required between MDHHS and the CSP.

Violations of any MDHHS privacy and security policy may be grounds for disciplinary action up to and including termination of employment or contractual agreement and loss of professional privileges. Sanctions for privacy and security violations will comply with other applicable MDHHS policies and procedures, regulations, and state and federal laws. MDHHS reserves the right to pursue civil or criminal penalties which may include notifying law enforcement officials and regulatory accreditation and licensure organizations.

A process (ongoing or one-time) that deviates from this policy and procedure must be documented by the business area and approved by the MDHHS chief Compliance and Data Governance Bureau officer prior to implementation.

If there is uncertainty as to whether a service is cloud-based or not, please contact the MDHHS Compliance and Data Governance Bureau.

REFERENCES

MDHHS APL 68E-340 Time Limit, Availability and Updates Policy

MDHHS APL 68A-60 Sanctions

MDHHS APL 68E-020 Data Privacy and Security Sanctions Policy

Michigan Civil Service Commission Rules, 2.6 Discipline

DTMB 1340.00.130.02 Acceptable Use of Information Technology Standard

DTMB 1340.00.020.01 Access Control Standard

Office for Civil Rights Guidance on HIPAA and Cloud Computing

CONTACT

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