Title/Subject: HIPAA: CONTINGENCY PLANS FOR ELECTRONIC PROTECTED HEALTH INFORMATION

Applies to: ☒Faculty ☒Staff ☒Students ☒Student Employees ☐Visitors ☒Contractors

Effective Date of This Revision: June 27, 2025

Contact for More Information: Office of HIPAA Compliance
989-774-2829
HIPAA@cmich.edu

☐Board Policy ☒Administrative Policy ☒Procedure ☒Guideline

BACKGROUND:

Central Michigan University (CMU) is a covered entity under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) law and regulations. CMU has designated itself as a hybrid entity as its business activities include both covered and non-covered functions. HIPAA requires that all CMU officers, employees and agents of units within the hybrid entity must preserve the confidentiality and integrity of Individually Identifiable Health Information (IIHI) pertaining to each patient, client, or participant in CMU's self-funded health plan. This IIHI is considered Protected Health Information (PHI) and shall be safeguarded in compliance with the rules and standards established under HIPAA.

For additional information on the measures Central Michigan University has implemented to comply with this legislation, visit CMU's official HIPAA website at HIPAA.cmich.edu.

PURPOSE:

This policy assures compliance with the HIPAA regulations requiring covered entities to establish a contingency plan which consists of policies and procedures for responding to an emergency or other occurrence that damages systems that contain electronic protected health information. For CMU, this policy applies if the IIHI is obtained by a unit that has been defined by CMU as a part of the Hybrid entity. In addition, some units may elect to protect personally identifiable health information within the secured network, even if they are not within the hybrid entity. In those cases, these policies will also apply.

DEFINITIONS:

The terms used in this policy have the same meaning as those terms in the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 and the regulations at 45 CFR Parts 160, 162, and 164.

POLICY:

I. Healthcare Information Technology (HcIT) will maintain a list of systems containing ePHI and work with the Office of Information Technology (OIT) (or the appropriate external Covered Entity or Business Associate) to ensure that they are appropriately maintained and classified relative to items II-X below.

II. Data backup
   a. All systems that contain ePHI must be backed up periodically based on how frequently the data on the system is updated, in most cases not less than once a day.
   b. When appropriate, backups will be encrypted and/or copied to a secondary location.

III. Disaster recovery plan
   a. All systems containing ePHI will be included in the appropriate tier level for systems and data restoration.

IV. Emergency mode operation plan

Authority: Neil J. MacKinnon, President
History: 03-30-2005; 11-16-2018; 06-27-2025
Last Revisited: 06-27-2025
Next Time to Review: 06-27-2026
Keywords: HIPAA; Health Information; Protected Health Information; Contingency Plans; Electronic Health Information

a. Each department is responsible for determining critical functions and related data that will allow those operations to continue until normal business can resume.
b. Each department is responsible for developing written manual procedures that will enable the continuation of critical business processes until their system has been restored.
c. These procedures must ensure the security of PHI until such time as the system has been restored and the data has been entered into the system. At that time, paper documentation will be shredded or stored in a manner that limits access as appropriate.
d. The emergency mode operation plans must include alternate workstations and workspaces in the event the department location is destroyed.

V. Testing and revision procedures
a. Departments shall annually test their emergency mode operation plans and document revisions of those plans based on the outcome of that testing. Documentation of testing, outcome, and revisions shall be provided to the HIPAA Privacy Officer each year.
b. The HIPAA Privacy Officer will maintain a record of each Department's annual testing and revisions. This documentation will be retained for six years from the date of its creation.
c. OIT is responsible for annual testing of its backup and disaster recovery plans and revisions of those plans based on the outcomes of that testing.
d. The HIPAA Security Officer will maintain a record of the OIT annual testing of its backup and disaster recovery plans and revisions. This documentation will be retained for six years from the date of its creation.

PROCEDURE:

I. Departments requiring assistance creating and testing their emergency mode operation plans may contact the HIPAA Privacy Officer for assistance.

GUIDELINES:

I. The above policies and procedures apply to the loss and recovery of ePHI. It is recommended that contingency plans also consider damage to or complete destruction of physical facilities by wind, fire, explosion, earthquake, flooding or other means. Develop plans and procedures for creating a physical work environment in which the department can continue its business processes in emergency mode. Consider proactive steps to backup and/or acquire essential resources other than ePHI that the department will need to conduct business during an emergency situation.