Title/Subject: HIPAA: RISK MANAGEMENT AND SECURITY STANDARDS

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

Effective Date of This Revision: July 30, 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, integrity, and availability 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:

In accordance with HIPAA Privacy and Security Rules, CMU has adopted this policy to fulfill its duty to protect the confidentiality, integrity, and availability of PHI and electronic PHI (ePHI). CMU is committed to safeguarding the information sharing and transmission of health information required to provide and promote high quality health care, protecting the public's health and well-being, fostering an innovative educational environment, and carrying out the necessary functions of the self-funded health plan, as required by law. This policy identifies how CMU will implement, assess, and monitor the physical, technical, and administrative safeguards in place to ensure PHI is safeguarded appropriately and to detect and prevent potential security risks.

DEFINITIONS:

Confidentiality: PHI/ePHI is not available or disclosed to unauthorized persons.

Integrity: PHI/ePHI is not altered or destroyed in an unauthorized manner.

Availability: PHI/ePHI is accessible and usable on demand by an authorized person.

All other 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. CMU will take reasonable precautions to prevent, detect, contain, and correct security violations. All workforce members and agents of CMU's Hybrid Entity shall adhere to CMU policies and HIPAA rules to maintain reasonable and appropriate physical, technical, and administrative safeguards for protecting PHI and ePHI.

Authority: President; Neil J. MacKinnon, President
History: 09-23-2011; 11-21-2018; 07-30-2025
Last Revisited: 07-30-2025
Next Time to Review: 07-30-2026
Keywords: HIPAA Safeguards; HIPAA Protected Health Information

II. The HIPAA risk management program shall include a collaboration between the HIPAA Privacy Officer, HIPAA Security Officer, and Chief Information Security Officer to recommend and monitor the effectiveness of safeguards intended to reduce risks and vulnerability to a reasonable and appropriate level to:
   a. Ensure the confidentiality, integrity, and availability of all PHI/ePHI that is created, received, maintained, or transmitted.
   b. Identify and protect against reasonably anticipated threats to the security or integrity of the information.
   c. Protect against reasonably anticipated, impermissible uses or disclosures.
   d. Ensure compliance with HIPAA Rules and the CMU HIPAA policies.

III. The HIPAA Security Officer will identify and maintain an inventory of the information systems that house ePHI. When a new system is implemented a security and privacy review will be conducted.

IV. CMU will regularly perform review of information system activity (e.g., audit logs and trails, information system activity records, facility access records) for the purpose of detecting:
   a. Unauthorized access to PHI/ePHI.
   b. Unusual patterns of use or activity.
   c. Other potential security violations.

V. The HIPAA Privacy Officer and HIPAA Security Officer will collaborate with other HIPAA Security Incident Response Team (HSIRT) members to assure procedures are developed, implemented, and documented to:
   a. Identify possible security incidents.
   b. Respond to suspected or known security incidents.
   c. Mitigate, to the extent practical, harmful effects of known security incidents.
   d. Document and report security incidents and their outcomes.

VI. Individuals who are allowed access to ePHI assume personal responsibility to maintain the integrity and security of the system and the network they use, by following established guidelines for personal login, password, and workstation controls.

VII. Documentation of risk assessment and system activity reviews shall be retained for at least six years, in accordance with HIPAA documentation requirements.

VIII. All workforce members and agents of CMU's Hybrid Entity are required to adhere to all CMU Policies, including HIPAA, OIT, and record retention policies which establish CMU's physical, technical, and administrative safeguards.
   a. For certain safeguards to be effective, workforce members must do their part in ensuring appropriate use and application of available controls. Expectations of a workforce member's duties, while not all encompassing, are outlined in Exhibit A. Additional expectations can be found in other CMU policies and the HIPAA Training Program.

Safeguard Standards
Examples and Guidance for HIPAA Workforce and Agents

I. Appropriate application of available controls includes, but is not limited to:
   a. Locking rooms and cabinets containing PHI and media used to access PHI when not in use.
   b. Secure keys, fobs, codes, and combinations in a manner that limits access to only those who need it.
   c. Ensuring paper records are stored in a manner where they are protected against environmental threats, such as floods or fires. Storing records in fireproof cabinets and off the floor is recommended.
   d. Situating monitors in a manner where they are not viewable by others, be cautious of public spaces and windows.
   e. When it is permissible to move records outside of a clinical space, do so in a way where records are concealed and not vulnerable to theft.
   f. Only use the CMU approved vendor shred bins or crosscut shredders to dispose of paper PHI.
   g. Reasonable precautions are taken to ensure that records containing PHI are not left out in the open or unattended. Following the clean desk principle is the best practice.
   h. Reasonable precautions are taken to ensure that conversations containing PHI are not overheard by others.
   i. Logoff or lock the system when leaving a workstation unattended so that it prompts for a password upon return to the workstation.