Title/Subject: HIPAA: PROTECTING 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 establishes how CMU has and will comply with the HIPAA Security regulations and includes what measures have been or will be implemented to remain compliant. Compliance by all units within CMU's Hybrid Entity is required. For CMU, this policy applies if IIHI is obtained by a unit within CMU's Hybrid Entity. In addition, some units may elect to protect PHI within the secured network, even if they are not a part of the Hybrid Entity. In those cases, these policies will also apply.

**DEFINITIONS:**

Electronic Protected Health Information (ePHI): Protected Health Information (PHI) that is transmitted or maintained in electronic media unless otherwise excluded from the definition of PHI under the Privacy Rule.

Individually Identifiable Health Information (IIHI): Information that is a subset of health information, including demographic information collected from an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Protected Health Information Network (PHIN): The secured network established by CMU for HIPAA protected health information. This network consists of appropriately protected segments of the broader CMU network and appropriately protected extensions established as a result of contractual relationships with third-party providers. Access to this network is only available from HIPAA workstations by authorized personnel who have been properly trained and granted access appropriate to their job.

*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.*

Authority: Neil J. MacKinnon, President
History: 03-30-2005; 11-16-2018; 11-21-2019; 06-27-2025
Last Revisited: 06-27-2025
Next Time to Review: 06-27-2026
Keywords: Workstation, Personal Security, Security, HIPAA

**POLICY:**

I. All Workforce Members within CMU's HIPAA Hybrid Entity are responsible for maintaining the privacy and security of all Electronic Protected Health Information (ePHI). To help maintain a high level of security for protecting ePHI, HIPAA Workforce Members shall adhere to established policies, procedures, and guidelines of the Office of Information Technology (OIT) and Healthcare Information Technology (HcIT).

II. CMU has adopted the following general strategy as a mechanism for protecting ePHI:
   a. OIT maintains a Protected Health Information Network (PHIN) as an added layer of defense to protect CMU's ePHI.
   b. ePHI should only be stored on systems hosted on the PHIN or covered by a Business Associate Agreement.
   c. Whenever possible, ePHI shall remain in its primary host system. (Refer to the HIPAA unit's training protocol and procedures for maintaining communication within the Electronic Medical Record (EMR) systems.
   d. ePHI removed from its host system, for any reason, must be encrypted both at rest and in transit.
   e. ePHI should only be accessed from approved devices/systems that have appropriate security controls in place.
   f. The HIPAA Privacy Officer and the HIPAA Security Officer will jointly maintain procedures and guidelines for the protection of ePHI.
      i. The procedures and guidelines noted above will inherit or strengthen the requirements found in existing CMU policies set forth to protect CMU's systems and devices, notably:
         1. CMU Policy 3-49: Secure Configurations Policy – Workstations
         2. CMU Policy 3-48: Password Policy

***Central Michigan University reserves the right to make exceptions to modify or eliminate this policy and or its content. This document supersedes all previous policies, procedures or guidelines related to this subject.***