Title/Subject: HIPAA: WORKFORCE SECURITY AND INFORMATION ACCESS MANAGEMENT

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 ensures that Workforce Members needing access to PHI and electronic protected health information (ePHI) have appropriate access and prevents anyone who does not require access from obtaining access to PHI and ePHI. For CMU, this policy applies if the IIHI is obtained by a unit that has been defined by CMU as part of the Hybrid Entity.

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 (PHI): Individually identifiable health information (IIHI) held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral unless otherwise excluded from this definition under the Privacy Rule.

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.

Authority: Neil J. MacKinnon, President
History: 03-30-2005; 10-29-2018; 06-27-2025
Last Revisited: 06-27-2025
Next Time to Review: 06-27-2026
Keywords: Access; Access Management; HIPAA

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. Workforce Clearance:
   a. Workforce clearance procedures at hire/appointment of faculty and staff include but not limited to criminal background check and review of claimed academic and professional qualifications as required by the policies and procedures of CMU's Human Resources and Faculty Personnel Services. Additionally, all required HIPAA Trainings are to be completed.
   b. Workforce clearance procedures for students include completing all required HIPAA Trainings. Background checks for students may be required depending on the requirements of the academic program in which the student is enrolled.
   c. To remain compliant with workforce clearance procedures after hire/appointment, all HIPAA Trainings that are required by the Office of HIPAA compliance must be completed throughout the Workforce Member's term. Non-compliance will result in sanctions, consistent with CMU's HIPAA Sanctions Policy.

II. Information Access Management:
   a. In collaboration with Senior Leadership, the Office of HIPAA Compliance shall approve and maintain a list of people responsible for authorizing and requesting a Workforce Member's access to PHI/ePHI within their unit. Senior Leadership must submit a request in writing to the Office of HIPAA Compliance if a change needs to be made to their unit's list.
   b. All access requests shall be appropriate for the Workforce Member's role, and as described in the Minimum Necessary requirements within CMU's HIPAA Use and Disclosure Policy. No person may authorize or request access for themselves.
   c. Technical Access Management:
      i. Healthcare Information Technology's (HCIT) established access request procedure must be followed when submitting access requests for access to systems that house ePHI.
      ii. HcIT is the only entity authorized to grant access to systems that house ePHI, and access granted must be limited to the extent authorized. HcIT may delegate granting authority to a Manager/Director of treatment or discipline-specific software.
   d. Physical Access Management:
      i. Physical access controls to areas where PHI is located, including but not limited to key fobs, keys, or combinations must be granted and monitored in accordance with the Facilities Management Building Access Controls Policy and the unit's access management procedure.
   e. Modification to Workforce Roles/Termination and Access Review:
      i. Managers/supervisors will ensure that when a Workforce Member's role is modified, that access to PHI/ePHI is reevaluated in a timely manner to assure appropriate access. HcIT shall be notified of any change in role/duty that requires change in access to ePHI.
      ii. Workforce Member's access to PHI/ePHI must be removed in a timely manner once a Workforce Member has been terminated, has left their role as a Workforce Member, or access is no longer needed.
      iii. At least once per year an access control review will occur to ensure that Workforce Members have appropriate access to PHI/ePHI and remove access from those who do not need it. The Office of HIPAA Compliance will maintain a record of such reviews.