Title/Subject: HIPAA: REPORTING AND INVESTIGATING INCIDENTS AND COMPLAINTS

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

Effective Date of This Revision: April 06, 2025

Policy Owner: Office of HIPAA Compliance
(989) 774-2829
HIPAA@cmich.edu

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

HIPAA and its rules direct covered entities to provide a process for individuals to lodge complaints regarding the handling of PHI and report possible Violations of HIPAA law or CMU's HIPAA policies and procedures. This policy establishes a process for individuals to register complaints, report potential Violations, and CMU's investigation of such. Finally, this policy informs individuals of their right to file complaints with the Secretary, U.S. Department of Health and Human Services (HHS).

DEFINITIONS

Breach: The acquisition, access, use, or disclosure of Protected Health Information (PHI) in a manner not permitted under HIPAA law and regulations, which compromises the security or privacy of the PHI.

I. Exceptions:
   a. A Workforce Member or person acting under the authority of CMU or a business associate unintentionally acquires, accesses, or uses PHI in good faith and within the scope of authority, and the unintentional acquisition, access, or use of PHI does not result in further impermissible use or disclosure under the HIPAA Rules;
   b. A person authorized to access the PHI at CMU or a business associate makes an inadvertent disclosure of PHI to another person similarly authorized at CMU, the same business associate, or within an organized health care arrangement in which CMU participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Rules; or
   c. CMU or its business associate has a good faith belief that the unauthorized person to whom the PHI was disclosed would not reasonably have been able to retain the disclosed information.

Incident: An event reported to the HIPAA Privacy Officer that results in an investigation to determine the possibility of an impermissible use or disclosure of PHI. Upon investigation an Incident may be determined to be a Violation or a Breach; or the investigation can determine that the Incident constitutes neither.

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.

Violation: When unsecured PHI was acquired, used, or disclosed in a manner not permitted by the HIPAA Privacy or Security Rules. A Violation is presumed to be a Breach unless it meets the definition of Breach Exception, or a completed four-factor risk assessment demonstrates low probability that the PHI has been compromised.

Workforce Member: includes employees, volunteers, students, trainees, and other persons whose conduct, in the performance of work for a unit in the CMU Hybrid Entity is under the direct control of such entity, whether or not they are paid by the entity. This includes students at a CMU work-site who have access to PHI in order to satisfy a clinical experience requirement for a program of study.

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. Individuals who believe that a CMU Workforce Member or agent of CMU may have violated the requirements of HIPAA law or rules, or CMU's HIPAA policies and procedures, or otherwise compromised the integrity or confidentiality of a patient, client or CMU self-funded health plan participant's information, should immediately report the alleged Violation to any of those listed below:
   a. Office of HIPAA Compliance; or
   b. HIPAA Security Officer; or
   c. Individual's Supervisor; or
   d. HIPAA Representative; or
   e. CMU General Counsel; or
   f. Ethics Hotline

II. Those who receive reports of actual or suspected HIPAA Violations must contact the Office of HIPAA Compliance as soon as practicable.

III. Failure to timely report an actual or suspected Violation may result in disciplinary action, consistent with CMU's HIPAA Sanctions policy.

IV. Individuals who believe that a CMU employee, HIPAA Workforce Member, or CMU agent may have violated the requirements of HIPAA rules may also file a complaint with HHS.

V. CMU's Notice of Privacy Practices ("Notice") must be accessible to clients, patients, and participants in CMU's self-funded health plans, and will include information about where a complaint may be reported. CMU's Notice shall include directives to individuals on how to submit a complaint regarding mismanagement of PHI to CMU's HIPAA Privacy Officer and/or directly to HHS.

VI. No CMU employee, Workforce Member, or agent shall intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual who files a timely complaint with CMU or with HHS.

VII. A CMU employee, Workforce Member, or agent who discriminates or retaliates against an individual who files a complaint to CMU or HHS shall be subject to disciplinary action defined within CMU's HIPAA Sanction Policy.

VIII. In the event the Office of Information Technology (OIT) detects or learns of a security Incident, OIT will conduct an investigation of the security Incident consistent with OIT Security Incident Policies and

Procedures. If it is determined that the Incident may involve unauthorized access, use, disclosure, or acquisition of PHI, OIT will immediately notify the Office of HIPAA Compliance.

IX. The Office of HIPAA Compliance, under the management of the HIPAA Privacy Officer, shall be responsible to lead the investigation, assuring that all investigation activities are thoroughly documented using the HIPAA investigation tools/templates. The investigation shall be completed and documented within thirty (30) days, unless extenuating circumstances occur.

X. The HIPAA Privacy Officer or his/her delegate has the authority to engage others within CMU as needed, to conduct a thorough and timely investigation. The HIPAA Privacy Officer/delegate shall engage members of its HIPAA Security Incident Response Team (HSIRT) and other Workforce Members or other CMU employees who may have information pertinent to the Incident, and in accordance with defined HSIRT procedures. The HSIRT will consist of the following, as determined by the HIPAA Privacy Officer, and as necessary to respond to each Incident:

a. HIPAA Security Officer: for Incidents requiring an electronic medical record audit trail or analysis, and other security Incidents requiring a transition and collaboration between OIT and the Office of HIPAA Compliance in accordance with Security Incident Response Team (SIRT) and HSIRT policies and procedures.
b. Chief Information Security Officer (CISO): for Incidents requiring an electronic audit trail or IT analysis of more than an electronic medical record access report.
c. HIPAA Hybrid Unit Representative: from the Hybrid Entity unit where the Incident occurred.
d. General Counsel Representative: for legal advice and/or Incidents involving potential criminal activity.
e. Risk Management: if the Incident requires the engagement of CMU's liability carrier.
f. Human Resources/Employee Relations or Faculty Personnel Services: if union representation is required or if the Incident investigation may lead to discipline for the Workforce Member involved in the Incident.
g. Business Owner/delegate: if a Business Associate is involved.
h. Other: additional Workforce Members, employees, agents, contractors, or other individuals necessary as determined by the HSIRT or HIPAA Privacy Officer.

XI. Upon investigation completion, if an Incident is determined to constitute a Violation or a Breach, then necessary action will be taken in accordance with CMU's HIPAA Breach Notification Policy. If it is determined that there is no Violation or Breach, then no further action is required.

XII. CMU shall take action to contain and mitigate, to the extent practicable, any harmful effect known to result from the Incident. Additionally, the Office of HIPAA Compliance will record a Violation or Breach onto the HIPAA Incident Log for monitoring patterns and trends to help identify workforce training needs.

XIII. HSIRT members shall participate in post-mortem lessons learned activities for reportable Breaches, and for other Incidents as deemed necessary by the HIPAA Privacy Officer, in consultation with the HSIRT.

XIV. Accounting of Disclosure Logs: Whether or not a Breach is reportable to the individual or HHS, CMU shall record impermissible disclosures in its HIPAA Accounting of Disclosure log.

XV. Workforce Training: CMU shall train all Workforce Members on the policies and procedures with respect to PHI as necessary and appropriate for the members to carry out their job responsibilities. Workforce Members shall be trained on what constitutes a Breach, and on the policies and procedures for reporting a HIPAA Incident.

XVI. CMU will adhere to its HIPAA Sanctions Policy, to assure the appropriate application of sanctions and disciplinary action to employees, Workforce Members, agents and others who fail to comply with HIPAA policies and procedures.

XVII. In accordance with CMU's HIPAA Organization for Compliance Policy, the HIPAA Privacy Officer will, at a minimum, as part of the annual review process, provide the HIPAA Council and HIPAA Executive Steering Committee with a summary of Violations and/or Breaches, including any appropriate resolutions and corrective actions taken. Incident reporting shall be used as an ongoing review process to determine if the HIPAA policies and procedures are effective and relevant to the privacy and security of PHI, including electronic PHI.

XVIII. All documentation of the investigation and retention of all information to CMU regarding its management of PHI, the disposition of complaints, including applied sanctions when applicable, and the details of investigations will be filed in the Office of HIPAA Compliance in a manner that all documentation can be easily retrieved for review and/or audit. The documentation shall be retained for a period of six years from the date the complaint investigation was completed.

RELATED POLICIES AND OTHER RESOURCES

I. Information Security Policy 3-42
II. Information Security Incident Response Policy 3-53

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.

Related Policies and Laws (Add Number & Name of Significantly Related Policy(ies))	3-42 Information Security Policy 3-53 Information Security Incident Response Policy
Appendices (Optional)	
Approval Authority	Neil J. MacKinnon, President
History of Review	04/14/2003; 09/23/2011; 10/29/2018; 06/27/2025
Last Reviewed Date	04/06/2026
Anticipated Review Date	04/01/2027
Change/No Change	Change - Name
Keywords	HIPAA; Reporting; Investigation; Privacy; Security; Incident; Complaint