Title/Subject: HIPAA: BREACH NOTIFICATION

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

Effective Date of This Revision: April 06, 2026

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

The purpose of this policy is to comply with HIPAA rules regarding notification in the event of Breach of Unsecured Protected Health Information.

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.

Law Enforcement Official: Any officer or employee of an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to investigate or conduct an official inquiry into a potential violation of law; or prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

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.

Unsecured PHI: Protected Health Information (PHI) that has not been secured through the use of a technology or methodology identified by the Department of Health and Human Services (HHS) as sufficient to render the information unusable, unreadable, or indecipherable to individuals. HHS guidance issued under section 13402(h)(2) of Pub. L. 111-5 identifies encryption and destruction as methods for securing PHI. To be considered secured, electronic PHI must be encrypted or destroyed as specified in the HIPAA Security Rule and in accordance with the National Institute of Standards and Technology (NIST).

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. Upon completion of investigating a HIPAA complaint/Incident in accordance with CMU's HIPAA Reporting and Investigating Incidents and Complaints Policy, CMU will provide notice to individuals, the media, and HHS as required by applicable state and federal law.

II. Necessity of Breach Notification: The four-step process below shall be used to assist the HIPAA Privacy Officer in determining whether notification is required:

   a. Step 1: Determine whether the use or disclosure violates the HIPAA Privacy Rule. If the acquisition, access, use or disclosure of PHI is permitted by the Privacy Rule, then no notification is required. If the use or disclosure is not permitted by the Privacy rule, continue to Step 2.

   b. Step 2: Determine whether the PHI was Unsecured. If the PHI was secured through NIST encryption or destruction technology in accordance with HHS guidance, Breach Notification is not required. If the PHI was Unsecured, then continue to Step 3.

   c. Step 3: Determine whether an exception to the definition of Breach applies. A disclosure is not considered a Breach if it meets the definition of a Breach Exception, therefore no notification is required. If an exception does not apply, continue to Step 4.

   d. Step 4: Conduct and document a risk assessment, using the Office of HIPAA Compliance Risk Assessment form. An acquisition, access, use or disclosure of PHI in a manner not permitted by the HIPAA Rules is presumed to be a Breach unless CMU demonstrates that there is a low probability the PHI has been compromised, based on a risk assessment. The HIPAA Privacy Officer may choose to skip the risk assessment and make Breach notifications after a Violation, but may not determine that

notification is not required without a documented risk assessment supporting its determination. The risk assessment will include an examination of at least the following four factors:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the PHI or to whom the disclosure was made;
3. Whether the PHI was actually acquired or viewed; and
4. The extent to which the risk to the PHI has been mitigated

e. Upon completion of the risk assessment, if CMU determines that there is a low probability that the PHI has been compromised, then Breach notification is not required. If CMU determines that there is not a low probability that the PHI has been compromised, then Breach notification is required, and notification should be issued as set forth below.

III. Timeliness of Notice: All required notifications must be made without unreasonable delay and no later than 60 calendar days after the discovery of the Breach.

IV. Delay of Notification for Law Enforcement Purposes: CMU may delay a required notification if a Law Enforcement Official informs CMU that Breach notification would impede a criminal investigation or cause damage to national security. If the Law Enforcement Official makes a statement in writing to CMU, CMU will delay the notification for the time period specified by the official. If the statement is made orally, CMU will document the statement, including the identity of the official, and delay the notification for no longer than 30 days from the date of the oral statement, unless a written statement is submitted during that time.

V. Content of Notification: CMU will, to the extent possible, include the following information in the notice, in plain language:

a. A brief description of the Incident(s);
b. Date(s) of the Breach;
c. Date the Breach was discovered (if known);
d. Description of the types of Unsecured PHI involved in the Breach (e.g., name, social security number, diagnosis, etc.);
e. Any steps an individual should take to protect himself or herself against potential harm;
f. A brief description of steps CMU is taking to investigate, mitigate, and prevent future Breaches; and
g. Contact procedures for individuals to obtain more information, including a toll-free telephone number, an email address, website, or postal address.

VI. Types of Notice: CMU will provide Breach notification in accordance with the following:

a. Individual Notice: Written notice will be provided to each affected individual by first-class mail to the last known address of the individual or, if the individual agrees to electronic notice, by email. If CMU knows an individual is deceased, notice shall be given to the individual's next of kin or personal representative if that person's address is known. Additional mailings may be sent as information becomes available.
b. Substitute Notice: If there is insufficient or out of date contact information that precludes individual notice, CMU will provide a substitute form of notice. If there are 10 or more individuals for whom there is insufficient or out-of-date information, CMU will maintain for 90 days a conspicuous web posting on its home page or provide notice in a major print or broadcast media (including geographic areas where affected individuals were last known to reside.) The notice will include the toll-free number where the affected individual can obtain further information which shall remain active for 90 days. If CMU has insufficient or out of date contact information for less than 10 individuals, then substitute notice may be provided by an alternate form of written, telephone, or other means.
c. Urgent Notice: If CMU determines that the Breach requires urgent action due to possible imminent misuse of Unsecured PHI, CMU may, in addition to written notice, provide notice to individuals by telephone, or other means, as appropriate.
d. Media Notice: If the Breach involves more than 500 individuals in a single state or jurisdiction, CMU will also provide notice through prominent media outlets serving the State or jurisdiction.

e. Notice to HHS: If the Breach involves 500 or more individuals, CMU will provide immediate notice to HHS in the manner specified on the HHS website. If the Breach involves less than 500 individuals, CMU will maintain a log of any such Breach and provide notice to HHS in the manner specified on the HHS website within 30 calendar days following the calendar year in which the Breach occurred. Instructions for submitting notice to HHS can be found on the hhs.gov website.

VII. Discovery of a Breach: A Breach shall be treated as "discovered" by CMU as of the first day on which such Breach is known, or by exercising reasonable diligence, would have been known to CMU. CMU shall be deemed to have knowledge of a Breach if such Breach is known to, or by exercising reasonable diligence would have been known, to any person, other than the person committing the Breach, who is a Workforce Member or agent of CMU.

VIII. Burden of Proof Requirements: CMU shall demonstrate that all required notifications have been provided or that, based on the risk assessment, the use or disclosure of Unsecured PHI did not constitute a Breach. Use of the HIPAA Incident report, HIPAA Investigation Tool, HIPAA Risk Assessment tool, and other forms are required in order to assure the completion and retention of documentation that all required notifications were made, or, alternatively, documentation to demonstrate that notification was not required: (1) its risk assessment demonstrating a low probability that the PHI has been compromised by the impermissible use or disclosure; or (2) the application of any other exceptions to the definition of Breach.

IX. 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.

X. Mitigation and Protection against Future Incidents: After each investigation of an Incident of Unsecured PHI, CMU shall take action to contain and mitigate, to the extent practicable, any harmful effect known to result from the Incident of Unsecured PHI. Additionally, CMU will review each HIPAA Incident to determine how a similar Incident may be avoided in the future. For example, CMU may determine that further workforce education, additional security procedures like firewalls, or an additional policy is necessary to avoid a potential Breach in the future.

XI. Business Associates: BA's shall, following the discovery of a Breach of Unsecured PHI, notify CMU of such Breach without unreasonable delay and in no case later than 60 calendar days after the BA discovers the Breach. However, in order to provide CMU with enough time to be compliant with its 60-day notification obligation, CMU will seek to include in its Business Associate Agreements (BAA) a provision that the BA shall notify CMU within 10 days of discovery and to provide CMU with information about the individuals involved in the potential Breach within 30 days of discovery. The BA must provide CMU will all information in its possession related to the Breach of Unsecured PHI as may be reasonably requested by CMU.

a. When appropriate and after reaching consensus with BA, CMU may also include a provision in the BAA, allocating the BA with the responsibility for notifications. CMU and the BA will consider which entity is in the best position to provide notice to the individual, dependent on various circumstances, such as the functions the BA performs on behalf of CMU, and which entity has the relationship with the individual.

XII. Workforce Training: CMU shall train all members of its workforce 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 and documenting a possible Breach of Unsecured Protected Health Information.

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

XIV. Document Retention Requirements: CMU must retain copies of all risk assessments and Breach notifications for at least six years from the date the notifications were provided, including the annual log of notifications provided to HHS. For substitute notifications, retain copies for at least six years from the date the notification was last posted on the website or the date the notification last ran in print or broadcast media. CMU must retain copies of all press releases provided to prominent media outlets for at least six years from the date the

notifications were provided. The HIPAA Privacy Officer shall be the person to retain this required documentation.

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))	
Appendices (Optional)	
Approval Authority	Neil J. MacKinnon, President
History of Review	04/14/2003; 09/23/2011; 11/16/2018; 06/27/2025
Last Reviewed Date	04/06/2026
Anticipated Review Date	04/01/2027
Change/No Change	Minor changes
Keywords	HIPAA; Breach; Breach Notification