Title/Subject: HIPAA: MAINTENANCE OF PHI

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:

To ensure there is a standard approach to the maintenance of PHI across CMU's Hybrid Entity and preserve the confidentiality, integrity, and availability of PHI. Maintenance of PHI may include the transmission, transfer, duplication, or conversion of the medical record in paper or digital format. For example, maintenance may include scanning, faxing, sweeping, and storing information. In the event of errant maintenance of information, response and mitigation steps must be followed in accordance with this policy as well as any other applicable CMU Policy.

DEFINITIONS:

Individually Identifiable Health Information: 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.

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.

Authority: Neil J. MacKinnon, President
History: 03-14-2024; 07-30-2025
Last Revisited: 07-30-2025
Next Time to Review: 07-30-2026
Keywords: Maintenance of PHI, Maintenance of medical record

POLICY:

I. All workforce members involved in the process of maintaining documents containing PHI must be fully trained on procedures specific to the systems and software they are using to complete the job function.

II. A quality assurance process must be used when converting digital and paper documents containing PHI. Refer to Attachment A for Quality Assurance Standards.
   a. Standard Operating Procedures must be maintained by CMU's Hybrid Entity units, with language specific to the unit, and retained within in the HIPAA Council.

III. Workforce members must apply reasonable safeguards when working with any form of PHI, in accordance with CMU policies and procedures.

IV. Failure to comply with this policy may result in sanctions up to and including termination pursuant to HIPAA Policy 12- 10: Sanctions for Breach of Privacy and Security of PHI.

PROCEDURE:

I. If transferring a document into an Electronic Medical Record System, trained workforce members will identify and select the correct patient chart by using a minimum of two (2) unique Protected Health Information identifiers that appear both in the patient chart and on the document to be transferred. Examples of acceptable identifiers include date of birth, full legal name, social security number, medical record number, or maiden name. If document identifiers cannot be matched between the patient's chart and the document to be transferred, the workforce member may not transfer the document until the proper identifiers can be verified.

II. If transferring a document to be stored in a system approved by Healthcare Information Technology to retain electronic PHI, trained workforce members will identify and select the correct destination to file the record and will ensure the document is titled and filed appropriately.

III. In the event of a minor transfer error (document filed under the wrong heading, document labeled incorrectly) the workforce member will notify their direct supervisor or Healthcare Information Technology so that a correction can be made.

IV. In the event of a serious transfer error (e.g. document transferred under the wrong patient chart) the workforce member will notify their direct supervisor immediately. The supervisor will immediately contact Healthcare Information Technology who will initiate the investigation/corrective action process and will contact the Office of HIPAA Compliance and Business Associates as applicable.

V. In the event that a patient identifies an error in their medical record's content and alerts a workforce member, the workforce member will notify the HIPAA Privacy Officer who will provide direction to the staff on the necessary corrective action steps and complete an investigation pursuant to CMU HIPAA policies.

---Remainder of this page left blank intentionally, however, additional pages follow---

ATTATCHMENT A

Quality Assurance Standards

I. Documentation verifying the integrity of maintenance processes.
II. Periodic testing and cleaning of equipment.
III. When digitizing or digitally transferring paper records, prepare paper records with care by removing staples and unfolding corners to ensure information is not obscured.
IV. Validate the number of pages on original records compared to the number on duplicated, transferred, or transmitted records to ensure record loss did not occur. In this process one should:
    a. Check for two sided pages.
    b. Note blank pages as “Intentionally left blank”.
V. Conduct a random quality review check after paper records are digitized. Check the digital record to examine:
    a. Smallest detail legibility captured (e.g. smallest type size for text; clarity of punctuation marks, including decimal points),
    b. Completeness of detail (e.g. acceptability of broken characters, missing segments of lines),
    c. Dimensional accuracy compared with the original (i.e. can you still read the document),
    d. Scanner-generated speckle (i.e. speckle not present on the original),
    e. Completeness of overall image area (i.e. missing information at the edges of the image area),
    f. Density of solid black areas, and
    g. Color fidelity.
VI. Always check for critical errors such as:
    a. Documents transferred to the wrong chart,
    b. Documents that are not complete/clear/readable,
    c. Documents missing patient identifiers,
    d. Documents missing pages with no explanation or identification of what was excluded.
VII. If a digitized document is to replace the original paper record these common problems must be corrected:
    a. Skewed images,
    b. Poor quality/illegible.
        i. Please note, diagnostic imaging is exempt from this standard as scans are not intended to replace the quality of the original.
VIII. Poor quality original:
    a. Sometimes the condition of the original paper record precludes quality digitization. In these instances, document the poor quality of the original record to avoid future confusion over the poor quality of the digitized image. This documentation can be accomplished by:
        i. Tagging the image as "best transfer possible"; or
        ii. When indexing/naming the document include, "bestTransferPossible".
    b. You may also need to keep the paper copy of the records that did not digitize well.