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

Applies to:  ☒ faculty  ☒ staff  ☒ students  ☒ student employees  ☐ visitors  ☒ contractors  ☒ student clinicians

Effective Date of This Revision:  October 29, 2018

Contact for More Information:  **HIPAA Privacy Officer**
255 Foust
989-774-2829
hipaa@cmich.edu

☐ Board Policy  ☒ Administrative Policy  ☒ Procedure  ☐ Guideline

**BACKGROUND:**

Central Michigan University is a covered entity under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and regulations. Its business activities include both covered and non-covered functions. It has decided to designate itself as a Hybrid Entity.

HIPAA requires that all CMU officers, employees and agents of units within the Hybrid Entity must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient, client, or participant in the CMU self-funded health plan. This IIHI is protected health information (PHI) and shall be safeguarded in compliance with the requirements of the security and privacy rules and standards established under HIPAA.

For additional information on the measures Central Michigan University is implementing in order to comply with this legislation, visit the official HIPAA web site, [https://www.cmich.edu/office_president/general_counsel/hipaa/Pages/default.aspx](https://www.cmich.edu/office_president/general_counsel/hipaa/Pages/default.aspx).

**PURPOSE:**

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

**DEFINITIONS:**

Individually Identifiable Health Information (IIHI). A subset of health information, including demographic information collected from a patient/client/employee, that is created or received by a health care provider, health plan or employer and relates to the past, present, or future physical or mental health or condition of a patient/client/employee, the provision of health care to a patient/client/employee, or the

Authority:  M. Rao, President; Robert O. Davies, President
History:  2005-03-30
Indexed as:  Access; HIPAA Access Management
past, present or future payment for the provision of health care to a patient/client/employee, and which identifies the patient/client/employee, or with respect to which there is a reasonable basis to believe that the information can be used to identify the patient/client/employee.

Protected Health Information (PHI). Individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.

Electronic Protected Health Information (EPHI). Individually identifiable health information (IIHI) that is transmitted by electronic media; maintained in electronic media, such as magnetic tape, disc, optical file; or transmitted or maintained in any other form or medium, except that it does not include IIHI in education records covered by the Family Educational Rights and Privacy Act, certain treatment records of CMU students as described at 20 USC 1232g(a)(4)(B)(iv), and employment records held by a covered entity in its role as employer.

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 the access appropriate to their job.

Workforce Member. A “Workforce Member” includes employees (and student employees), volunteers, 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:

1.0 A unit that grants access to EPHI is required to document all access authorization and any changes in authorization for each workforce member to whom access is granted.

2.0 Units are required to grant only the access that is appropriate for the job and as described in the Minimum Necessary requirements within the Use and Disclosure Policy #12-6.

3.0 Units are required to assure that workforce clearance has been established, including background check, completion of HIPAA training, understanding of appropriate information usage, and is aware of the CMU HIPAA policies available on the website.

4.0 The clinical program director, or the faculty member who supervises students within the units of the Hybrid entity, must assure that the students receive the CMU HIPAA training before they are allowed access to PHI.

5.0 The Privacy Officer will designate in writing those managers/supervisors within the Hybrid entity, who may authorize individual Workforce Members to have access to EPHI and at what levels appropriate for their roles. No manager/supervisor (except the Privacy Officer) may authorize access for her/himself. The manager/supervisor must approve access levels for individuals in writing.

6.0 The Manager/supervisor within the unit will provide in writing to the HIPAA Privacy Officer and Office of Information Technology, one or more designated Access Coordinator(s) who will be
responsible for controlling access for each system with EPHI.

7.0 Managers/supervisors will assure that when a workforce member has terminated, the workforce member’s access is terminated immediately. For alterations in access for workforce members, managers/supervisors shall assure that access is changed in a manner that assures appropriate and timely access.

8.0 At least once per year, managers/supervisors and clinical program directors shall assure that the unit or clinical program reviews the types and levels of access being granted to within each system to workforce members as well as students in the clinical programs. This will include a review to assure the appropriate person has the appropriate access. Records of these access control reviews shall be maintained by HIPAA Privacy Officer for 6 years from the date of review.

Further detailed procedures may be found on the CMU HIPAA website: https://www.cmich.edu/office_president/general_counsel/hipaa/Pages/Policies_and_Procedures.aspx

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 relative to this subject.