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: January 13, 2020

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) has designated itself a Hybrid Entity under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) law and regulations, as CMU's business activities include both covered and non-covered functions.

HIPAA requires that all CMU Workforce Members preserve the integrity and the confidentiality of all individually identifiable health information (IIHI) pertaining to each patient, client, or participant in any healthcare activity or CMU funded health plan. CMU's Workforce includes but is not limited to CMU officers, employees, students, and agents of units within the Hybrid Entity. CMU's 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.

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:

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 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, 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:

Workforce Clearance:

1.0 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.

2.0 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.

3.0 To remain compliant with workforce clearance procedures after hire/appointment, all HIPAA Trainings that are required by the HIPAA Privacy Office must be completed throughout the Workforce Member's term. Non-compliance will result in sanctions, including but not limited to loss of access to PHI/ePHI and if applicable, and may include the initiation of additional sanctions according to HIPAA Sanctions policy #12-10.

Information Access Management:

4.0 In collaboration with Senior Leadership, the HIPAA Privacy Office 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 HIPAA Privacy Office if a change needs to be made to their unit's list.

5.0 All access requests shall be appropriate for the Workforce Member's role, and as described in the Minimum Necessary requirements within CMU's Use and Disclosure Policy #12-6. No person may authorize or request access for themselves.

Technical Access Management:

6.0 Healthcare Information Technology's (HCIT) established access request procedure must be followed when submitting access requests for access to systems that house ePHI.

7.0 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 a treatment or discipline-specific software.

Physical Access Management:

8.0 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 to the Facilities Management Policy #3-21 Lock & Key Policy and the unit's access management procedure.

Modification to Workforce Roles/Termination and Access Review:

9.0 Managers/supervisors will assure that when a Workforce Member's role is modified, that the 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.

10.0 Workforce Member's access to PHI/ePHI must be removed in a timely manner once a Workforce Member has been terminated, left their role as a Workforce Member, or access is no longer needed.

11.0 At least once per year a unit shall conduct an access control review to ensure that Workforce Members have appropriate access to PHI/ePHI and remove access from those who do not need it.

Further detailed procedures may be found on the CMU HIPAA website: HIPAA.cmich.edu

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.