Title/Subject: **HIPAA: CONTINGENCY PLANS FOR ELECTRONIC PROTECTED HEALTH INFORMATION**

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

Effective Date of This Revision: November 16, 2018

Contact for More Information: **Office of HIPAA Compliance**
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.

According to the law, 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 or client, 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.

**PURPOSE:**

This policy assures compliance with the HIPAA regulations requiring covered entities to establish a contingency plan which consists of policies and procedures for responding to an emergency or other occurrence that damages systems that contain electronic protected health information. 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. In addition, some units may elect to protect personally identifiable health information within the secured network, even if they are not within the hybrid entity. In those cases, these policies will also apply.

**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.

---

Authority: M. Rao, President; Robert O. Davies, President
History: 2005-03-30
Indexed as: HIPAA Health Information; HIPAA Protected Health Information; HIPAA Contingency Plans; HIPAA Electronic Health Information

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 data is only available from certified workstations by authorized personnel who have been properly trained and granted the access appropriate to their job.

Department. A unit that has been previously defined as part of the hybrid entity as defined on https://www.cmich.edu/office_president/general_counsel/hipaa/Pages/default.aspx. In addition, any entity that has elected to secure EPHI within the PHIN is considered a department as used in this policy.

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 Healthcare IT will maintain a list of systems containing ePHI and work with OIT (or the appropriate external Covered Entity of Business Associate) to ensure that they are appropriately maintained and classified relative to items 2-5 below.

2.0 Data backup
- 2.1 All systems that contain EPHI must be backed up periodically based on how frequently the data on the system are updated, in most cases not less than once a day.
- 2.2 When appropriate, backups will be encrypted and/or copied to a secondary location.

3.0 Disaster recovery plan
- 3.1 All systems containing ePHI will be included in the appropriate tier level for systems and data restoration.

4.0 Emergency mode operation plan
- 4.1 Each department is responsible for determining critical functions and related data that will allow those operations to continue until normal business can resume.
- 4.2 Each department is responsible for developing written manual procedures that will enable continuation of critical business processes until their system has been restored.
- 4.3 These procedures must assure the security of PHI until such time as the system has been restored and the data has been entered into the system. At that time, the manual documentation will be shredded or stored in a manner that limits access as appropriate.
- 4.4 The emergency mode operation plans must include alternate workstations and work space in the event the department location is destroyed.

5.0 Testing and revision procedures
- 5.1 Departments shall annually test their emergency mode operation plans and document revisions of those plans based on the outcome of that testing. Documentation of testing, outcome, and revisions shall be provided to the HIPAA Privacy Officer each year.
- 5.2 The HIPAA Privacy Officer will maintain a record of each Department's annual testing and

revisions. This documentation will be retained for six years from the date of its creation.

5.3 OIT is responsible for annual testing of its backup and disaster recovery plans and revisions of those plans based on the outcomes of that testing.

5.4 The HIPAA Security Officer will maintain a record of the OIT annual testing of its backup and disaster recovery plans and revisions. This documentation will be retained for six years from the date of its creation.

**PROCEDURE:**

Departments requiring assistance creating and testing their emergency mode operation plans may contact the HIPAA Privacy Officer for assistance.

**GUIDELINES:**

The above policies and procedures apply to the loss and recovery of EPHI. It is recommended that contingency plans also consider damage to or complete destruction of physical facilities by wind, fire, explosion, earthquake, flooding or other means. Develop plans and procedures for creating a physical work environment in which the department can continue its business processes in emergency mode. Consider proactive steps to backup and/or acquire essential resources other than EPHI that the department will need to conduct business during an emergency situation.