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: March 30, 2005

Contact for More Information:

HIPAA Chief Privacy Officer
Associate Dean/Administration & Finance
College of Medicine
989-774-7547

HIPAA Security Officer
Foust Hall 019
989.774.6633

☐ 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.

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.

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:

1.1 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

---

Authority: M. Rao, President
History: No Prior History
Indexed as: HIPAA Health Information; HIPAA Protected Health Information; HIPAA Contingency Plans; HIPAA Electronic Health Information

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.

1.2 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

1.3 Protected Health Information Network (PHIN). The secured network established by CMU for HIPAA protected health information. 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.

1.4 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. Data backup
   1.1 All systems that contain EPHI must be backed up periodically based on how frequently the data on the system is updated, in most cases not less than once a day.
   1.2 If the system is not within PHIN or co-located in Foust, department personnel are responsible for data backup and media security.
   1.3 When possible, backups must be encrypted and the media stored off site in a secure location or placed in a fireproof safe.
   1.4 All data within the Protected Health Information Network (PHIN) will have encrypted backup tapes made daily and will be included in the daily tape rotation for secure off site storage.
2. Disaster recovery plan
   2.1 Each department that stores data within the PHIN is responsible for providing adequate disaster recovery systems and application software.
   2.2 Information Technology will include all systems within PHIN in the appropriate tier level for systems and data restoration.
   2.3 If a Disaster Recovery system has not been provided, the department will work with its vendor for alternate systems and when a system is available, Information Technology will restore the data.
   2.4 Any department that stores EPHI on servers not within PHIN and not physically located in Foust is responsible for developing, following and providing written data backup procedures and a description of the steps it would follow to recover from a system failure or a disaster that affects its systems.
   2.5 These plans and procedures will be centrally stored in a share provided by Information Technology. Once they are placed in this share, an existing process will include these procedures in daily backup and rotation to an off site location.
3. Emergency mode operation plan
   3.1 Each department is responsible for developing manual procedures that will enable continuation of critical business processes until their system has been restored.
   3.2 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.

3.3 The emergency mode operation plans must include alternate workstations and work space in the event the department location is destroyed.

4. Testing and revision procedures
   - 4.1 Departments are responsible for periodic testing of their emergency mode operation plans.
   - 4.2 The results of these tests will be logged in the centralized storage folders provided by Information Technology and will include documentation on revisions made to the data backup and/or disaster recovery plans.
   - 4.3 Information Technology will include departmental backup and restore of data with their periodic disaster recovery testing.
   - 4.4 Information Technology will document disaster recovery test results for HIPAA systems and any plan revisions that result in the documentation share.
5. Applications and data criticality analysis
   - 5.1 Information Technology will assign a tier level for each system and establish a restore schedule that estimates the period of down time by system.
   - 5.2 Each department is responsible for determining critical functions and related data that will allow those operations to continue until normal business can resume.
6. The HIPAA Compliance Council is the enforcement entity for these policies and the Internal Audit department is a member of this council. The compliance council may ask for periodic audits for HIPAA compliance and to make appropriate recommendations for improvement as needed.

PROCEDURE:

Procedures for developing department contingency plans can be found on the secured document link from https://www.cmich.edu/office_president/general_counsel/hipaa/Pages/default.aspx

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.