BACKGROUND:
Central Michigan University is a hybrid entity with health care components and a self-insured health insurance plan under the Health Insurance Portability and Accountability Act (HIPAA). According to HIPAA, CMU officers, employees, and agents must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient, client or individual covered under a CMU self-insured 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.

PURPOSE:
The purpose of this policy is to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) regarding notification in the event of Breach of Unsecured Protected Health Information, and to guide Central Michigan University’s (CMU) investigation of HIPAA incidents.

DEFINITIONS:
Breach: The acquisition, access, use or disclosure of PHI in a manner not permitted under HIPAA law and regulations, which compromises the security or privacy of the PHI. An impermissible use or disclosure is presumed to be a breach unless CMU or its Business Associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment. A breach excludes:

a. Any unintentional acquisition, access, or use of protected health information by a Workforce member or person acting under the authority of CMU or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further impermissible use or disclosure under the Privacy Rule;

b. Any inadvertent disclosure by a person who is authorized to access PHI at CMU or its business associate to another person authorized to access PHI at CMU or its business associate, or organized health care arrangement in which CMU participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule; or

c. A disclosure of PHI where CMU or its business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Except for the exceptions described above, an acquisition, access, use or disclosure of PHI not permitted under the HIPAA rules is presumed to be a Breach unless CMU or its business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

a. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of...
**HIPAA: BREACH NOTIFICATION**

re-identification;

b. The unauthorized person who used the PHI or to whom the disclosure was made;

c. Whether the PHI was actually acquired or viewed; and

d. The extent to which the risk to PHI has been mitigated.

**HHS:** Department of Health and Human Services.

**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, that 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 (2) identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

**Law Enforcement Official:** Any officer or employee of an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to investigate or conduct an official inquiry into a potential violation of law; or prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

**Protected Health Information (PHI):** Individually Identifiable Health Information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.

**Unsecured PHI:** PHI that has not been secured through the use of a technology or methodology identified by HHS as sufficient to render the information unusable, unreadable, or indecipherable to individuals. HHS guidance issued under section 13402(h)(2) of Pub. L. 111-5 identifies encryption and destruction as methods for securing PHI. To be considered secured electronic PHI must be encrypted or destroyed as specified in the HIPAA Security Rule and in accordance with the National Institute of Standards and Technology (NIST).

**Workforce:** Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for CMU, is under the direct control of CMU or a business associate of CMU, whether or not they are paid by CMU or its business associate.

**POLICY:**

1.0 CMU will provide notice to individuals, the media and HHS as required by applicable state and federal law in the event of a Breach of Unsecured PHI.

2.0 CMU as a hybrid entity with health care components and a self-insured health insurance plan has an established HIPAA Security Incident Response Team (HSIRT). The HSIRT, will consist of the HIPAA Privacy Officer and one or more of following, as applicable:
   a. HIPAA Security Officer
   b. CMU Chief Information Security Officer (CISO)
   c. HIPAA representative where the violation occurred
   d. a representative from General Counsel
   e. The HSIRT may consult with additional employees, agents, contractors, or other individuals necessary as needed.
3.0 In collaboration with the HIPAA Privacy Officer, one or more members of the HSIRT will investigate the incident according to CMU policies and procedures, determine whether a HIPAA breach has occurred, determine the probability that the PHI has been compromised, and provide appropriate breach notifications without unreasonable delay and in compliance with HIPAA regulations. CMU will demonstrate proof that all required notifications have been provided or that a use or disclosure of unsecured PHI did not constitute a breach.

4.0 If it is determined that breach notification is not required, CMU shall assure that there is documentation to demonstrate such, including its risk assessment demonstrating low probability that PHI has been compromised by the impermissible use or disclosure or by the application of any other exceptions to the definition of breach.

5.0 Detecting and Reporting a Potential Breach of Unsecured PHI: Any Workforce member who detects or has knowledge of a Breach of PHI or an incident that may potentially give rise to a Breach of PHI must immediately report the potential Breach incident to his or her supervisor, manager or director. The supervisor, manager or director and Workforce member must immediately contact the HIPAA Privacy Officer and complete an incident report form in cooperation with the Workforce member reporting the incident.

6.0 Discovery of a Breach: A Breach of PHI shall be treated as “discovered” by CMU on the first day the incident that may have resulted in a Breach is known to CMU, or by exercising reasonable diligence, would have been known to CMU. CMU shall be deemed to have knowledge of a Breach if the Breach is actually known to, or by exercising reasonable diligence would have been known, to any person, other than the person committing the Breach, who is a Workforce member or agent of CMU.

7.0 Investigation of a Potential Breach: After discovery of a potential Breach, CMU shall begin an investigation into the incident. CMU will conduct a risk assessment as part of the investigation to determine whether a reportable Breach of Unsecured PHI has occurred, and, if indicated based on the results of the risk assessment, will notify any affected individuals, HHS and the media as required by law. The HIPAA Privacy Officer shall have primary responsibility for investigating and documenting the report and investigation of the potential Breach. The HIPAA Privacy Officer shall be responsible for the management of the Breach investigation, completion of a risk assessment and coordination with HSIRT and other departments as appropriate (e.g., administration, information technology, human resources, risk management, public relations and legal counsel).

8.0 Necessity of Breach Notification: The four step process below shall be used to assist the Privacy Officer, HSIRT, and other investigators in determining whether notification is required.

   Step 1: Determine whether the use or disclosure violates the Privacy Rule. If the acquisition, access, use or disclosure of PHI is permitted by the Privacy Rule, then no notification is required. If the use or disclosure is not permitted by the Privacy rule, continue to Step 2.

   Step 2: Determine whether the PHI was Unsecured. If the PHI was secured through NIST encryption or destruction technology in accordance with HHS guidance, Breach notification is not required. If the PHI was Unsecured, then continue to Step 3.

   Step 3: Determine whether an exception to the definition of Breach applies. A disclosure is not considered a Breach, and therefore no notification is required when:

      i. A workforce member or person acting under the authority of CMU or a business associate unintentionally acquires, access, or uses PHI in good faith and within the appropriate scope of authority, and the unintentional acquisition, access or use of PHI does not result in further impermissible use or disclosure under the HIPAA Rules;

      ii. A person authorized to access the PHI at CMU or a business associate makes an inadvertent disclosure of PHI to another person similarly authorized at CMU, the same business associate, or within an organized health
care arrangement in which CMU participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Rules; or

iii. CMU or its business associate has a good faith belief that the unauthorized person to whom the PHI was disclosed would not reasonably have been able to retain the disclosed information.

If one of the above exceptions applies, then no breach notification is required. If none of these exceptions apply, continue to step 4.

Step 4: Conduct and document a risk assessment analysis. An acquisition, access, use or disclosure of PHI in a manner not permitted by the HIPAA Rules is presumed to be a reportable Breach unless CMU demonstrates that there is a low probability the PHI has been compromised, based on a risk assessment. The risk assessment will help CMU determine whether or not a reportable Breach has occurred. CMU may skip the risk assessment and make breach notifications after a potential Breach incident, but may not determine that notification is not required without a documented risk assessment supporting its determination. The risk assessment will include an examination of at least the following factors:
(See also: Risk Assessment Tool on HIPAA website at: https://www.cmich.edu/office_president/general_counsel/hipaa/Pages/Forms.aspx)

i. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

ii. The unauthorized person who used the PHI or to whom the disclosure was made;

iii. Whether the PHI was actually acquired or viewed; and

iv. The extent to which the risk to the PHI has been mitigated

CMU will sufficiently document each risk assessment to demonstrate support for its conclusion regarding whether there is a low probability the PHI has been compromised. Upon completion of the risk assessment, if CMU determines that there is a low probability that the PHI has been compromised, then Breach notification is not required. If CMU determines that there is not a low probability that the PHI has been compromised, then Breach notification is required and notification should be issued as set forth below.

9.0 Timeliness of notice: All required notifications must be made without unreasonable delay and no later than 60 calendar days after the discovery of the Breach.

10.0 Delay of notification for law enforcement purposes: CMU may delay a required notification if a Law Enforcement Official informs CMU that breach notification would impede a criminal investigation or cause damage to national security. If the Law Enforcement Official makes the statement in writing to CMU, CMU will delay the notification for the time period specified by the official. If the statement is made orally, CMU will document the statement, including the identity of the official, and delay the notification for no longer than thirty days from the date of the oral statement, unless a written statement is submitted during that time.

11.0 Content of notification: CMU will, to the extent possible, include the following information in the notice, in plain language: (i) a brief description of the incident(s); (ii) date(s) of the Breach; (iii) date the Breach was discovered (if known); (iv) description of the types of Unsecured PHI involved in the Breach (e.g., name, social security number, etc.); (v) any steps an individual should take to protect himself or herself against potential harm; (vi) a brief description of steps CMU is taking to investigate, mitigate, and prevent future Breaches; and (vii) contact procedures for individuals to obtain more information, including a toll-free telephone number, an email address, Web site or postal address.
12.0 Types of notice: CMU will provide breach notification in accordance with the following:

a. Individual notice: In all cases, written notice will be provided to each affected individual by first-class mail to the last known address of the individual or, if the individual agrees to electronic notice, by email. If CMU knows an individual is deceased, notice should be given to the individual’s next of kin or personal representative if that person’s address is known. Additional mailings may be sent as information becomes available.

b. Substitute notice. If there is insufficient or out of date contact information that precludes individual notice, CMU will provide a substitute form of notice. If there are 10 or more individuals for whom there is insufficient or out of date information, CMU will maintain for 90 days a conspicuous web posting on its home page or provide notice in a major print or broadcast media (including geographic areas where affected individuals were last known to reside.) The notice will include the toll-free number where the affected individual can obtain further information which shall remain active for 90 days. If CMU has insufficient or out of date contact information for less than 10 individuals, then substitute notice may be provided by an alternate form of written, telephone or other means.

c. Urgent notice: If CMU determines that the Breach requires urgent action due to possible imminent misuse of Unsecured PHI, CMU may, in addition to written notice, provide notice to individuals by telephone, or other means, as appropriate.

d. Media notice: If the Breach involves more than 500 individuals in a single state or jurisdiction, CMU will also provide notice through prominent media outlets serving the State or jurisdiction.

e. Notice to HHS. If the Breach involves 500 or more individuals, CMU will provide notice to HHS immediately in the manner specified on the HHS website. If the Breach involves less than 500 individuals, CMU will maintain a log of any such Breach and provide notice to HHS in the manner specified on the HHS website by March 1 following the calendar year in which the Breach occurred. Instructions for submitting notice to HHS can be found at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstructi on.html.

13.0 Breach Information Log: In addition to the reports created for each incident, CMU shall record all Breaches of Unsecured PHI regardless of the number of patients affected. The following information should be collected and recorded for each Breach: (i) a description of the incident, including the date, the date of discovery, and the number of patient affected; (ii) a description of the types of Unsecured PHI involved in the Breach; (iii) a description of the action taken to notify patients, the media and HHS of the Breach, as applicable; (iv) the results of the risk assessment; and (v) steps CMU took to mitigate the Breach and prevent future occurrences. These logs shall be provided to and maintained in a centralized location by the HIPAA Privacy Officer.

14.0 Mitigation and Protection against Future Incidents: After each investigation of a potential Breach of Unsecured PHI, CMU shall take action to contain and mitigate, to the extent practicable, any harmful effect known to result from the potential Breach of Unsecured PHI. Additionally, CMU will review each potential Breach incident to determine how a similar incident may be avoided in the future. For example, CMU may determine that further Workforce education, additional security procedures like firewalls, or an additional policy is necessary to avoid a potential breach incident in the future.

15.0 Business Associates: CMU requires all business associates to report Breaches of Unsecured PHI to CMU promptly, and in no case later than sixty (60) calendar days after the business associate discovers the Breach. CMU will document such notification. The business associate must provide CMU with all information in its possession related to the Breach of Unsecured PHI as may be reasonably requested by CMU. While CMU is ultimately responsible for ensuring individuals are notified, CMU may delegate the responsibility of providing individual notices to the business associate. CMU and the business associate will consider which entity is in the best position to provide notice to the individual, which may depend on various circumstances, such as the
functions the business associate performs on behalf of the CMU and which entity has the relationship with the individual.

16.0 Workforce Training: CMU shall train all members of its workforce on the policies and procedures with respect to PHI as necessary and appropriate for the members to carry out their job responsibilities. Workforce members shall be trained as to how to identify and promptly report potential Breaches in accordance with this policy.

17.0 Sanctions: CMU will adhere to its Sanctions Policy to assure the appropriate application of sanctions and disciplinary action to Workforce members, students, agents and others who fail to comply with privacy policies and procedures.

18.0 Complaints: Complaints regarding this policy or a failure to comply with it may be made to CMU, Attention: HIPAA Privacy Officer via email hipaa@cmich.edu.

19.0 Document Retention Requirements: CMU must retain copies of all notifications for at least six years from the date the notifications were provided, including the annual log of notifications provided to the Department of Health & Human Services. For substitute notifications, retain copies for at least six years from the date the notification was last posted on the website or the date the notification last ran in print or broadcast media. CMU must retain copies of all press releases provided to prominent media outlets for at least six years from the date the notifications were provided. The HIPAA Privacy Officer shall be the person to retain this required documentation.

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.