Title/Subject: **HIPAA: Investigation of Complaints and Reports of Breach of Privacy and Security of PHI; Sanctions for Breach of Privacy and Security of PHI; Breach Notification**

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

Effective Date of This Revision: September 23, 2011

Contact for More Information:

Plan Administrator
Rowe Hall 108
989.774.3661

Health Services Director
Foust Hall 249
989.774.3944

Carls Center Director
College of Health Professions
989.774.6624

☐ Board Policy ☒ Administrative Policy ☒ Procedure ☐ Guideline

---

BACKGROUND:

Central Michigan University is a covered entity under the HIPAA law and regulations. According to this law, 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 the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

PURPOSE:

CMU has adopted this policy to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the privacy regulations, as well as to fulfill our duty to protect the confidentiality and integrity of confidential protected health information as required by law, professional ethics, and accreditation requirements.

DEFINITIONS:

The 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 CMU prohibits violations of HIPAA statutory and regulatory requirements, and CMU policies and procedures in place to uphold them. Any violation of HIPAA rules or CMU policy and procedures shall constitute grounds for disciplinary action.

Authority: G. E. Ross, President
History: 4-14-2003
Indexed as: HIPAA Breach of Privacy, HIPAA Security of PHI, HIPAA Violations, HIPAA Discipline, HIPAA Sanctions

2.0 The disciplinary process and sanctions that may be imposed for a violation of HIPAA law, regulations and/or CMU policies and procedures will vary according to the status of the person who has engaged in the violation.

2.1 Employees, including student employees, will be subject to the disciplinary processes already in place for their employee group. Disciplinary action may include termination. If the seriousness of the offense warrants such action, an employee may be terminated for the first breach of HIPAA law, regulation or CMU's HIPAA policy and procedures

2.2 Students who are engaged in clinical experiences giving them access to protected health information will be subject to discipline by the work site, up to and including termination from the clinical work. If the student is enrolled in a class, he/she will be subject to grading consequences according to the judgment of the instructor for that class. Students enrolled in clinical programs may be further subject to review for their fitness for continuation in the clinical education program according to the criteria and processes established by that clinical program.

2.3 Contractors are subject to termination of the contract.

2.4 Other workforce members will be subject to disciplinary measures deemed appropriate for the violation, up to and including termination.

3.0 Violations of HIPAA law and regulations may also subject the violator to criminal prosecution.

4.0 No CMU officer, employee or agent shall intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual who files a complaint or reports a possible breach to the integrity or confidentiality of client or other sensitive information, or who cooperates in the investigation or disciplinary procedure arising out of a complaint or report.

5.0 All officers, employees, students, contractors and agents of CMU are expected to comply and cooperate with CMU's investigation and sanctioning of violations of HIPAA law, regulations, and CMU HIPAA policy.

6.0 Any employee who knowingly falsely accuses another of a breach of HIPAA rules and policy shall be subject to disciplinary action up to and including termination.

7.0 In the event CMU discovers a potential breach of PHI, CMU will investigate and provide notice when required under HIPAA or other applicable Law.

Title/Subject: **HIPAA: Investigation of Complaints and Reports of Breach of Privacy and Security of PHI; Sanctions for Breach of Privacy and Security of PHI; Breach Notification**

PROCEDURE:

1.0 **Report of Alleged Violation of HIPAA law, regulation or CMU HIPAA policy and procedures**. Any person may report an alleged violation of HIPAA compliance by following the HIPAA Client Complaint Policy.

2.0 **Investigation of Allegations**.

2.1 If an allegation is reported to a Privacy Officer for the health care component where the violation may have occurred, the Privacy Officer may attempt to resolve the allegation. If the allegation is not resolved within one week of its filing, the Privacy Officer must report the allegation to the Complaint Officer.

2.1.1 **Conduct of Investigation**. Upon receipt of an allegation, the Complaint Officer will assure that an inquiry or investigation is conducted in coordination with the Privacy Officer of the health care component where the violation may have occurred and either Human Resources or Faculty Personnel Services. The inquiry or investigation and disciplinary process, if any, shall comply with the procedures provided in the employee's collective bargaining agreement or employee handbook. The Complaint Officer shall assure that a thorough and confidential investigation into the allegations is conducted.

2.1.2 **Notification of Complainant**. When the investigation has been completed and a decision related to the allegations has been reached and implemented, the Complaint Officer shall notify the complainant of the results of the investigation and any corrective action taken

2.1.3 **Resolutions by Privacy Officers**. If a Privacy Officer resolves an allegation, he/she shall provide a written report of the allegation and its resolution to the HIPAA Complaint Officer.

3.0 **Corrective Action.**

3.1 If the investigation of an allegation of a violation concludes that one or more employees are responsible for the violation, they may be disciplined according to the established CMU procedures for disciplining an employee in that employee group. Serious or repeated violations may lead to termination.

3.2 If the investigation of an allegation of a violation concludes that a system or procedure or policy of CMU is responsible for the violation, corrective action will be taken. The HIPAA Complaint Officer will oversee the implementation of needed changes.

4.0 **Criminal Prosecution**. Willful and grossly negligent breaches of HIPAA law or regulations may also result in criminal prosecution.

4.1 **Agency Cooperation With Criminal Prosecution**. In the event that violation of CMU's policies and standards for privacy and security of PHI constitutes a criminal offense under HIPAA or other federal or state laws, the violator should expect that CMU shall provide information concerning the violation to appropriate law enforcement personnel and will cooperate with any law enforcement investigation or prosecution.

5.0 **CMU Involvement in Professional Discipline**. In the event that violation of HIPAA law or rules or CMU's HIPAA policies and standards for privacy and security of PHI constitutes a violation of professional ethics and is grounds for professional discipline, the violator should expect that CMU may report such violations to the appropriate licensure/accreditation agencies and will cooperate with any professional investigation or disciplinary proceedings.

6.0 **Treatment of Agents and Contractors**. CMU will seek to include violations of HIPAA law or rules or CMU's HIPAA policies and procedures as grounds for termination of the contract and/or imposition of contract penalties.

7.0 **Documentation of Sanctions**. The Complaint Officer will maintain a record of allegations received and their disposition, including sanctions that are applied. This documentation will be retained for six years from the date of its creation or the date when it last was in effect.

8.0 **Breach Notification Procedures**

8.1 **Investigate Security Incidents.** In the event the Privacy Officer learns of a security violation of CMU's electronic or paper files, he or she will conduct an investigation of the security incident consistent with these Policies and Procedures.

Upon notification of a potential incident of unauthorized access to medical records, the Privacy Officer will determine whether CMU has a duty to notify individuals about a breach. In determining whether notification is required, the Privacy Officer may consult with legal counsel, employees, agents, contractors or consultants as reasonably necessary to determine CMU's notification obligations, if any.

8.2 **Determine Whether a Breach Has Occurred.** When the Privacy Officer learns of a possible breach of either electronic files or physical files, the Privacy Officer must first determine whether there has been an impermissible use or disclosure of unsecured protected health information under the Privacy Rule.

The following are examples of the types of situations that may need evaluation. These include situations in which a contractor/business associate notifies CMU that an impermissible use or disclosure has or may have occurred:

- CMU learns that an unauthorized individual has gained access to CMU's electronic information system.

- CMU learns that an authorized individual may have accessed protected health information for an improper purpose.
- CMU learns that information intended for an authorized individual was misdirected (for example, by e-mail or fax transmission).
- CMU learns that a business associate has suffered a potential data breach.
- CMU hears from individuals who are the subject of protected health information that they have been the victims of identity theft or other identity fraud crime.

If a situation requires evaluation, the Privacy Officer should gather details about the incident, including the following:

- The specific data that is involved in the incident.
- Whether the access, use or disclosure is consistent with CMU's HIPAA policies and procedures.
- The manner in which the information was accessed, used or disclosed, and the circumstances surrounding the incident.
- The date the incident was discovered.
- The date(s) the incident occurred.
- The number of individuals whose information was involved.
- The states in which the individuals reside.

8.3 Determine whether Notification is Required. If the facts indicate that the access, use, or disclosure was not permitted under HIPAA, the Privacy Officer will need to determine whether the incident falls into one of the exceptions to the HIPAA breach notification requirements. CMU may not have a duty to notify if the information is considered "secured" (see subsection 8.3.1); the incident is not considered a "breach" (see subsection 8.3.2.); or the breach does not cause a significant risk of financial, reputational, or other harm to the individuals whose information was involved (see subsection 8.3.3).

Note: while much of this policy addresses breach notification requirements under HIPAA, most states have security breach notification requirements that may also apply. Therefore, the Privacy Officer may need to consult with legal counsel to determine if CMU has any obligations under state notification laws—whether or not notification is required under HIPAA.

Note: in the event of a breach, CMU will also need to evaluate the effectiveness of its privacy and security practices and determine whether corrective action is required under Section 3.0 of these Procedures.

8.3.1 Determine whether the information is deemed "secured" under HIPAA. The first step is to determine whether the information was properly secured under HIPAA. Whether the information is properly secured will depend on the nature of the information and how well it is protected.

8.3.1.1 If the information is electronic, the data is considered secured if *both* of the following are true:

A. The data has been properly encrypted consistent with guidance issued by the Department of Health & Human Services. This guidance may change from time to time, but as of September 2009, HHS guidance called for the following:

- For data at rest (including data that resides in databases, file systems, flash drives, memory and other structured storage methods), the encryption process must be consistent with National Institute of Standards & Technology Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices.*

- For data in motion (which includes data moving through a network, including wireless transmission, whether by e-mail or structured electronic interchange), the encryption process must comply, as appropriate, with one of the following:

  - National Institute of Standards & Technology Special Publication 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*;

  - National Institute of Standards & Technology Special Publication 800-77, *Guide to IPsec VPNs;*

  - National Institute of Standards & Technology Special Publication 800-113, *Guide to SSL VPNs*; or

  - Other encryption processes that are Federal Information Processing Standards 140-2 validated.

- Data that has been destroyed may also be considered secured if one of the following is true:

  - The information was stored on paper, film or other hard copy media, and the media has been shredded or destroyed in such a way that the protected health information cannot be reconstructed. (Note that redaction is **not** an effective form of destruction.)

  - The information is in electronic form and has been cleared, purged or destroyed consistent with National Institute of Standards & Technology Special Publication 800-88, *Guidelines for Media Sanitization*, so that the protected health information cannot be retrieved.

B. The individual/entity with improper access to the information does not have access to the confidential decryption process or key.

8.3.1.2. If the information meets one of the tests above for being secured, the incident will not be considered a breach and notification will not be necessary under HIPAA. The Privacy Officer must document the analysis leading to this conclusion and retain the documentation for a period of at least six years.

8.3.2 Determine whether the incident falls within an inadvertent acquisition or disclosure exception. If the information is not considered secured, the incident may still not be considered a breach if the incident falls within one of the following exceptions:

8.3.2.1 Unintentional acquisition, access or use of protected health information. In order for this exception to apply, all of the following have to be true:

A. the unauthorized acquisition, access or use of protected health information must have been unintentional;

B. the individual who acquired, accessed or used the protected health information must be one of the following:

- a member of CMU's workforce

- A member of a business associate's workforce

- A person acting under the authority of CMU or CMU's business associate

C. The individual who acquired, accessed or used the protected health information did so in good faith.

D. The acquisition, access or use did not result in any further use or disclosure that is not permitted under the HIPAA privacy rules.

8.3.2.2 Inadvertent internal disclosure of protected health information. This exception applies if all of the following are true:

A. The disclosure is made by an individual who is authorized to access protected health information

B. The disclosure is made to an individual who is authorized to access protected health information.

C. Both individuals work for the same organization, which may be one of the following:

- CMU
- CMU's business associate
- An organized health care arrangement in which CMU participates.

D. The disclosure did not result in any further use or disclosure that is not permitted under the HIPAA privacy rules.

8.3.2.3 Where the information would not be retained. This exception applies if all of the following are true:

A. The disclosure is made to an unauthorized individual.

B. CMU or its business associate has a good-faith belief that the unauthorized individual would not reasonably have been able to retain the information.

8.3.2.4. If the Privacy Officer concludes that the incident meets one of the exception tests above, the incident will not be considered a breach and notification will not be necessary under HIPAA. The Privacy Officer must document the analysis leading to this conclusion and retain the documents for a period of at least six years.

8.3.3 Determine whether there could be a significant risk of harm. If the Privacy Officer determines that the information did not meet the requirements for being secured or did not fall within one of the exceptions noted in 8.3.1 or 8.3.2 above, the Privacy Officer must determine whether the unauthorized acquisition, access, use or disclosure of protected health information could create a significant risk of financial, reputational, or other harm to the individuals whose data was involved in the incident.

8.3.3.1 Factors to consider include:

- Who impermissibly acquired, accessed or used the information or to whom was the information impermissibly disclosed?
    - Was the recipient also a HIPAA covered entity with a legal duty not to misuse the information?
    - Does the recipient have a contractual relationship with CMU that prohibits it from misusing the information?
    - Are there other facts and circumstances that would indicate that the recipient of the information is unlikely to misuse the information?
- How much detailed information was included in the data?
    - Did it include Social Security numbers, driver's license numbers, bank account/credit card numbers, insurance numbers, or other PHI that could be used for identity theft or identity fraud crimes?
    - Did it include information about medical treatment, diagnoses, diseases, or similar details about an individual's health?
- Were immediate steps taken to mitigate an impermissible use or disclosure, such as by obtaining the recipient's satisfactory assurances that the information will not be further used or disclosed or will be destroyed?
    - Are there past dealings with the recipient or other factors that would indicate that the recipient can be trusted not to use or further disclose the information?
- Was the information returned before being accessed for an improper purpose?

8.3.3.2 The Privacy Officer should consider these and other pertinent facts to determine whether there is significant risk of harm to the individuals whose protected health information was involved. If the Privacy Officer concludes that there is not a significant risk of harm, then notification is not required under HIPAA. The Privacy Officer must document the analysis leading to this conclusion and retain this documentation for at least six years.

8.4 Special considerations for breaches involving Business Associates. Under HIPAA, a business associate who maintains protected health information on behalf of CMU has a duty to notify CMU of the breach within 60 days, but it is CMU's duty to provide notification to the individuals impacted by the breach. Moreover, in certain circumstances when the business associate is deemed to be CMU's agent, CMU may be charged with the business associate's knowledge of the breach, so that the deadline for providing notice will be based upon when the business associate knew or should have known about the breach.

In order to reduce the risk to CMU of a HIPAA violation, CMU will seek to include in its business associate agreements a provision that requires the business associate to notify CMU of a potential breach within 5 business days of discovery and to provide information about the individuals involved in the potential breach within 30 days of discovery. When appropriate, and after reaching consensus with business associate, CMU may also include a provision in the business associate agreement allocating responsibility for notification between CMU and business associate. When a business associate reports a potential breach to CMU, the Privacy Officer will work with the business associate to determine whether the incident requires notification.

8.5 Notification. If the Privacy Officer determines that CMU must provide notification of the incident, CMU will prepare appropriate notification as required below.

8.5.1 Notice to Individuals

8.5.1.1 Under HIPAA, CMU must provide notice to affected individuals without unreasonable delay, but no later than 60 days after the date CMU discovers the breach or should have discovered the breach if it had exercised appropriate diligence. In order to reduce the risk of exceeding the deadline, CMU will provide notice as soon as reasonably possible once it has discovered and determined the scope of the breach.

8.5.1.2 The HIPAA breach notification regulations require that the following information be included in the notification:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.

- A description of the types of unsecured protected health information that were involved in the breach.
- Any steps the individual should take to protect themselves from potential harm resulting from the breach.
- A brief description of what CMU is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches.
- Contact procedures for individuals to ask questions or learn additional information including a toll-free telephone number, an e-mail address, Website, or postal address.

8.5.1.3 All notifications must be written in plain language.

8.5.1.4 Notice may be provided by e-mail to individuals who have agreed in advance to receive electronic notice. Otherwise, notice must be sent via first class mail. If CMU knows that an individual is deceased and has the address of the deceased's next of kin or personal representative, CMU may send the written notification to either next of kin or the personal representative.

8.5.1.5 Under HIPAA, CMU has no more than 60 days after discovery of the disclosure to notify individuals. The date of discovery is measured as follows:

- First day the breach is known to a member of the CMU's workforce or agents;
  - workforce member includes any employee, volunteer, trainee, agent, etc.
- First day a member of the CMU workforce or its agents **would have known** of the breach by exercising reasonable diligence; or
- First day that CMU is notified of a breach by any of its independent contractors (unless the independent contractor is deemed to be an agent, in which case CMU is deemed to have notice on the date the breach is first known to the independent contractor).

Note: State security breach notification laws may also apply and may mandate a shorter time frame for notification.

8.5.2 Substitute Notice. If CMU does not have sufficient contact information for some or all of the affected individuals (or if the contact information is outdated) then CMU must provide substitute notice for such individuals in the following manner:

8.5.2.1 If fewer than 10 individuals are affected, substitute notice can be provided to these individuals via telephone or other written notice that is reasonably calculated to reach the individuals.

8.5.2.2 If more than 10 individuals are affected, HIPAA requires the following:

- a conspicuous posting for a period of 90 days on CMU's home page **or** a conspicuous notice in a major print or broadcast media in the geographic areas where the individuals affected by the breach likely reside; and

- a toll-free phone number active for 90 days where an individual can learn whether the individual's unsecured protected health information may be included in the breach.

8.5.2.3 The content of the substitute notice must include all of the elements required for the standard notice described above.

8.5.2.4 Substitute notice is not required in situations where an individual is deceased and CMU does not have sufficient contact information for the deceased individual's next of kin or personal representative.

8.5.3 Expedited Notice. If CMU believes that there is the possibility of imminent misuse of unsecured protected health information CMU may also provide expedited notice by telephone or other means. This notice is in addition to, and not in lieu of, direct written notice.

8.5.4 Notice to the Media. If the Privacy Officer determines that notification is required to more than 500 residents of a state, CMU must provide notice in the form of a press release to prominent media outlets serving the state. The press release must include the same information required in the written notice provided to individuals. The Privacy Officer may coordinate such notice with CMU's public relations department or other public relations consultants, as appropriate.

Note: State security breach notification laws should also be consulted to determine whether there are additional notification obligations to the media, state agencies, or national credit bureaus.

8.5.5 Notice to the Department of Health & Human Services

If the Privacy Officer determines that CMU or its business associate must provide notification to individuals under HIPAA, then CMU will also have to provide notification to the Department of Health & Human Services. The timing of the notification will depend on the number of individuals affected by the incident:

8.5.5.1 If the breach involves more than 500 individuals (regardless of whether they reside in the same state or in multiple states), CMU will notify the Department of Health & Human Services without unreasonable delay, but no later than 60 days after discovery. This notification is to be submitted to the Department of Health & Human Services contemporaneously with the written notifications sent to individuals and in the manner specified on the Department's Web site.

8.5.5.2 If the breach involves fewer than 500 individuals:

A. The Privacy Officer must maintain a log of notifications involving fewer than 500 individuals. The information to be recorded in the log will be set forth on the Department of Health & Human Services' Web site.

B. The Privacy Officer will submit information from the log to the Department of Health & Human Services for each calendar year by February 28 of the following year, in the manner specified on the Department's Web site.

CMU must retain copies of all notifications for at least six years from the date the notifications were provided. 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.

8.5.6 Document Retention Requirements. Notifications to the Department of Health & Human Services, including the annual log of notifications, must be maintained for at least six years from the date submitted to the Department.