Title/Subject: **HIPAA: Using or Accessing Protected Health Information Outside the Office**

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

Effective Date of This Revision: September 23, 2011

Contact for More Information:

**HIPAA Privacy Officer
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 information that is subject to protection under HIPAA.

PURPOSE:

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) mandates that Protected Health Information be kept confidential. CMU has adopted this policy to set uniform guidelines as to how the integrity and security of Protected Health Information (PHI) must be protected when used or accessed from outside of the office. A Workforce member who uses or accesses PHI when working from outside the office is expected to follow the practices and procedures outlined below.

This policy applies to CMU workforce members who are using PHI to perform their job duties. It does not apply to CMU employees or students who access their own personal information through an online access portal that CMU has established. For example, a CMU employee accessing his or her health plan enrollment information or a University student accessing personal account information online is not subject to this policy.

PROCEDURE:

1.0 Protected Health Information is not to be removed from CMU or accessed offsite by members of the Workforce without prior approval and a signed confidentiality agreement on file.

1.1 The Workforce member is responsible for maintaining the privacy and security of all Protected Health Information that he or she may be transporting, storing or accessing offsite. This includes, but is not limited to the following:

Authority: G.E. Ross, President
History: No Prior History
Indexed as: Using Protected Health Information; Accessing Protected Health Information; Offsite Use of Protected Health Information

- Protected Health Information and Electronic Protected Health Information (ePHI) relating to the Carls Center, University Health Services, or the self-funded health plans offered through the Central Michigan University Flexible Benefits Plan
- Computers, smart phones, USB memory devices or other electronic devices that contain or access ePHI
- Paper documents, including confidential working papers that contain PHI.

2.0 CMU HIPAA Policies are in effect whether the Workforce member is working off-site or in a CMU facility. A Workforce member is expected to apply the same confidentiality principles in remote locations as apply in the office.

3.0 Each unit of the CMU Hybrid Entity will determine the extent to which PHI may be taken to or accessed from a remote location.

4.0 PHI that is physically transported between CMU offices or from CMU offices to an off-site location must be kept secured in transit or in public areas – whether in paper or electronic form. Workforce members must safeguard the PHI in the same way that they protect their own valuables. Examples of ways to secure information include:

4.1 not leaving PHI unattended in a vehicle or in public areas where the information is vulnerable to theft.

4.2 when transporting paper documents containing PHI, securing the documents in a briefcase, backpack, box, or other transportation container that conceals the documents and prevents others from seeing the content of the documents.

4.3 when transporting electronic media that contain or that can be used to access PHI, such as computers, smart phones, and USB memory devices, securing the media in a briefcase, backpack, purse, or pocket in a manner that conceals the device and prevents it from being mislaid.

5.0 PHI my be used or accessed in off-site locations only in accordance with the following restrictions:

5.1 Paper documents should only be accessed in a location where information cannot be viewed by others. When the information is not being used, it must be securely stored where others cannot easily access it. Paper documents containing PHI must not be reviewed in places where others may see the content of the documents.

5.2 Telephone calls relating to PHI must be made in a private location where others cannot overhear the conversation. Wireless, cellular and cordless telephones shall be used for communicating PHI only if no other means of communicating is available and the communication is necessary at the time to complete a work-related function.

5.3 Workforce members may not access PHI over unsecured public networks, such as at a coffee shop. Home networks must be secured according to CMU requirements.

5.4 If a Workforce member uses his or her own personal computer or device (rather than a CMU computer or device) to access the information, and other household members share that computer or device, the computer or device must be configured so that other users of the device may not access PHI through the device.

5.5 Password protected automatic screensavers must be set to appear on computers after a few minutes of non-use. Devices that may display information must be physically situated in a work area where others are unable to easily view PHI while the device is in use.

5.6 If possible, any PHI transmitted between CMU and laptops, smartphones and other mobile electronic devices should be encrypted.

5.7 All equipment, briefcases, etc., used off-site shall be labeled with updated contact information so that they can be returned to the proper location if lost or misplaced.

6.0 CMU security policies that apply to access to PHI at work shall also apply to the Workforce member's personal computer or other electronic device used to access and/or store PHI.

6.1 PHI must not be accessed from a public computer, private computer or other electronic device that is not owned by CMU or the Workforce member.

6.2 The Workforce member must follow all CMU security requirements, which includes keeping any computer or other electronic device utilized to access PHI up to date with current anti-virus software and patches and following CMU protocols for secure remote access to CMU information systems.

6.3 The Workforce member must not allow the computer or other electronic device to be used in ways that would compromise the security and confidentiality of the computer, device, the information stored on the device, or to CMU information systems.

7.0 While working in a remote locations, PHI should not be printed or photocopied unless absolutely necessary.

8.0 All PHI taken from CMU to an offsite location must be returned to CMU on the Workforce member's next scheduled work day. CMU-owned media containing PHI that are no longer needed must be returned to CMU and "scrubbed" or disposed of appropriately. This includes but

is not limited to, printed information, faxes, hard drives, diskettes, CDs and thumb drives. Media owned by the Workforce member and used to access PHI must be "scrubbed" and otherwise disposed of according to standards established by CMU.

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.