85 Health Insurance Portability and Accountability Act (HIPAA)

Approved by President
Effective Date: __________, 2017
Responsible Division: Business and Finance
Responsible Office: Compliance and Enterprise Risk Management
Responsible Officer: Assistant Vice President for Compliance and Enterprise Risk Management

I. Purpose

This policy ensures Middle Tennessee State University’s (MTSU or University) compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA or the Act). The Campus Pharmacy is covered under the Act as a covered entity and healthcare provider.

II. Background

HIPAA (Pub. L. 104-191) sets forth national standards to protect individually identifiable health information by certain covered entities. The Act additionally requires information technology security protections for electronically stored and transmitted healthcare data sets and provides certain patient protections and rights regarding access to individual health information.

III. Scope

As a healthcare provider and HIPAA covered entity, the staff, student workers, interns, part-time employees, and healthcare business associates of Campus Pharmacy are covered under this policy. Additionally, the policy covers all areas of the University for which healthcare documentation is transmitted to external agencies for healthcare operations or treatment purposes including, but not limited to, University Counseling services, the University Speech Clinic, and the Dyslexia Center.

IV. Definitions

A. Breach Log. A log of all breaches of unsecured protected health information (PHI).

B. Business Associate. A person or entity contracted by covered entities to provide certain health care activities or functions on behalf of the covered entity including, but not limited to, the use and disclosure of protected health information for healthcare billing
services; benefit management services; consulting; repricing; practice management; quality assurance; and utilization review; and claims processing. Business Associates are covered under the HIPAA privacy rule and must provide assurances to covered entity that protected health information will be safeguarded from misuse and will not be used for the business associate’s independent purposes.

C. Covered Entity. A healthcare provider, health plan, or healthcare clearinghouse. A healthcare provider includes: doctors, clinics, psychologists, dentists, chiropractors, nursing homes, and pharmacies that transmit healthcare information in an electronic format in connection with a Department of Health and Human Services (HHS) adopted standard. Health plans include: health insurance companies, health maintenance organizations (HMOs), company health plans, and government funded healthcare programs, such as Medicare, Medicaid, and the military and veterans’ health care programs. Healthcare clearinghouses are entities that process nonstandard health information, received from another agency, into standard, electronic data or content.

D. Protected Health Information (PHI). The most common protected health information includes the following:

1. Name
2. Street address
3. Zip code
4. Date of birth
5. Patient age
6. Telephone number (home, work, mobile)
7. Fax number
8. E-mail address
9. Health Plan, Medicare, or Medicaid number
10. Diagnosis or diagnosis code
11. Social Security Number
12. Medication and any health or allergy information
13. Patient video recordings from therapy and/or counseling and psychotherapy sessions.

V. Policy

All covered entities are required to provide written notice to patients affected by a breach of unsecured PHI. (45 C.F.R. § 164.408).

A. Breaches Affecting Fewer than 500 Individuals. For breaches affecting fewer than 500 individual, notifications must be made to the federal Department of Health and Human Services (HHS) within sixty (60) days of the end of the calendar year in which the breach was discovered. Notifications to HHS must be submitted electronically on the agency’s Health Information Privacy Web portal (Web Portal). Covered entities are not required
to wait until the end of the calendar year to report a breach of PHI and may, instead, report the breach at the time of occurrence. Separate notices also must be completed for each breach incident.

B. Breaches Affecting 500 Individuals or More. For breaches affecting 500 individuals or more, notification must be made to HHS without reasonable delay and in no case later than sixty (60) calendar days from the discovery of the breach. Notification to HHS must be submitted electronically by utilizing the HHS Web portal. In addition, all affected individuals must be notified of the breach and should describe the PHI involved and the method by which the PHI was stolen (e.g., missing laptop, non-shredded PHI in a trash container). For a breach affecting 500 or more individuals, notification must also be provided to a major media outlet within the state. The Secretary of HHS will post, online, breaches affecting 500 individuals or more at www.hhs.gov/ocr/privacy.

C. Breach Log. A log of all breaches of PHI must be maintained by the Covered Entity and reported to the Secretary of HHS by March annually.

D. Acknowledgment of Receipt. The Act requires that notification of the Covered Entity’s privacy practices be provided to all patients. For example, patients who receive or pick up prescriptions must be provided notice of the Campus Pharmacy’s privacy practices. Patients should be asked to sign electronically, or in writing, to acknowledge receipt of the Covered Entity’s practices. Where a patient refuses to acknowledge receipt of the privacy practices, the Covered Entity shall document the refusal of its good faith effort to provide the patient with its notice of privacy practices.

E. Minimum Necessary. The Covered Entity shall maintain, and implement, practices, policies and procedures to limit unnecessary or inappropriate access to, and disclosure of, protected health information. Only the minimally necessary information should be shared regarding the patient’s health record or healthcare data set to accomplish a specific function or for a particular purpose. The Covered Entity should rarely need to share the whole patient record for a prescriber to provide proper care or for a third-party to process a claim. The Minimum Necessary standard does not apply to the following types of disclosure and information:

1. Disclosures or request by a healthcare provider for treatment purposes.
2. Disclosures to the individual (patient) who is the subject of the information.
3. Uses or disclosures made pursuant to an individual’s authorization.
4. Uses or disclosure required for compliance with HIPAA’s Administrative Simplification Rules.
5. Uses or disclosure that are required by law enforcement agencies.

The Covered Entity’s procedures must identify the Pharmacy staff, business associates, student workers, or other individuals who need access to PHI to perform their job duties.

F. Patient Authorization. Patient authorization provides covered entities with permission to utilize or transmit PHI for specific purposes.

1. The authorization must be in writing and must contain the following elements:
   a. A description of the PHI to be used and or disclosed.
   b. The individual authorized to make the disclosure or use of PHI.
   c. An expiration date of the authorization.
   d. The purpose for which the PHI can be used or disclosed.

2. Patient authorization also is expressly required for uses and disclosures of PHI for all marketing communications with the exception of:
   a. Communication that occurs face-to-face between the covered entity and the individual (such as across the Campus Pharmacy counter); and
   b. Communication that involves a promotional gift of nominal value.

G. Patient Consent. Patient consent may be obtained for uses and disclosures of PHI for healthcare treatment, payment, and healthcare operations but is not required under the HIPAA Privacy Rule.

H. Patient Rights. Under HIPAA’s Privacy Rule, patients have certain rights for which covered entities must comply. The patient, or the patient’s personal representative (45 CFR § 164.502(g)), has the right to:

1. Ask to see his/her health records.
2. Ask to obtain a copy of his/her health records.
3. Have corrections made to an individual’s health records.
4. Receive a notice that tells the patient how their health information can be used or shared for certain purposes.
5. Receive a report on when and why the patient’s health information was used or shared.

6. Receive notification of a breach of their protected health information.

7. Request to review health records of the patient used for treatment, payment, or healthcare operations.

8. File a complaint with HHS if the patient is denied their rights under HIPAA, or if it is believed their information is not being protected.

I. Security Rule. The HIPAA Security Rule sets forth a national set of security standards for protecting certain health information that is maintained or transferred in electronic format. Both the technical and non-technical safeguards of the Security Rule requires protections of PHI, electronic protected health information (e-PHI), and such clinical applications as computerized physician order entry (CPOE). The Security Rule additionally specifies a series of administrative, technical, and physical security procedures that must be utilized by covered entities and their business associates to assure the integrity, privacy, and availability of e-PHI, as well as to protect against any anticipated cyber-threats involving e-PHI and electronic health records.

Minimally, Covered Entities must have the following HIPAA Security Safeguards in place:

1. Authorized access and control of the physical facility.

2. Workstation, device, and electronic media security, as well as written policies and procedures on the proper use of, and access to, workstations and devices containing e-PHI.

3. Technical safeguards, in collaboration with the University’s Information Technology Division, that assure: access control; audit controls; integrity controls; and transmission security (including electronic network security and dedicated facsimile or email).

Such technical safeguards must also comply with the Health Information Technology for Economic and Clinical Health Act of 2009. (HITECH, Pub. L.111-5)

J. Government Resources. If a patient wishes to file a healthcare information privacy or security complaint, the Campus Pharmacy shall provide information about the HHS website and direct them to the Office of Civil Rights Complaint Portal for instructions on how to complete the complaint. The Department of HHS also provides a Breach of
Unsecured Protected Health Information Portal (Breach Portal) of providers and other Covered Entities who have notified the OCR of HIPAA breaches. The HHS and OCR Breach Portal can be found at [https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf).

VI. Training

Training of all Campus Pharmacy employees, including student workers, interns, and part-time employees, shall occur annual during as part of the Fall Semester Faculty meeting. New hires of Campus Pharmacy shall receive HIPAA training within thirty (30) days of hire. Refresher training also shall be conducted, as needed, to ensure employee compliance with HIPAA practices.

VII. Annual Review

This Policy shall be reviewed for expansion and/or revision annually by University Health Services; Campus Pharmacy; the Office of University Counsel; and the Office of Compliance and Enterprise Risk Management.

Forms: none.

Revisions: none.