MERCER UNIVERSITY

UNIVERSITY POLICIES

Title:	Uses and Disclosures of Health Information Policy (HIPAA General Operating Policy)
Effective Date:	July 1, 2025
Issuing Authority:	Senior Vice President for Finance and Administration
Policy Contact:	University HIPAA Officer, 478-301-2300

Purpose

The purpose of this policy is to assure that identifiable health information contained in any Mercer health record is only used or disclosed for its intended purpose and in accordance with general and/or specific patient notifications and permissions, except where permitted or required by law.

Scope

This policy applies to all employees, students, and patients of Mercer University.

Exclusions

None

Policy Statement

It is the policy of Mercer University (Mercer) that an individual's identifiable health information may only be used within the University or disclosed to entities outside the University after notification to and/or with the expressed permission of the patient, except in cases of emergency or where specifically permitted or required by law. Access to health information stored in any Mercer file or depository, stored electronically, or that exists in any recording device or in any clinical or research data base, collectively hereafter referred to as the "health record", is limited to those who have a valid business or medical need for the information or otherwise have a right to know the information. With the exception of purposes related to treatment, access to an individual's health information or the use or disclosure of an individual's health information must, to the extent practicable, be limited to only that necessary to accomplish the intended purpose of the approved use, disclosure or request. For purposes of HIPAA compliance, employee records and student records subject to FERPA are specifically excluded from the definition of "health record".

An individual's health information may be used by Mercer for treatment, payment, and healthcare operations (routine purposes), after Mercer has provided to the individual its Notice of Privacy Practices and has made a good faith effort to obtain an acknowledgement of its receipt. Additionally, Mercer may use an individual's health information for other (non-routine) purposes or may disclose an individual's health information to external entities for non-routine

purposes upon obtaining a valid authorization from the individual giving permission for that stated use or disclosure. Further, Mercer may use and disclose an individual's health information without prior permission or authorization where the health information has been sufficiently "de- identified", so as to hide the identity of the individual(s), is part of a "limited data set", or for other uses where allowable by statute. Where authorization is required, the requirement to obtain authorization may only be waived by the University's Institutional Review Board (IRB).

Health information may be used or disclosed without a patient's acknowledgement of receipt of the Notice of Privacy Practices in the event of an emergency or where a communications barrier makes prior permission or notification impossible. Mercer health professionals may, at their discretion, use or disclose an individual's protected health information without prior notification of privacy practices or without acknowledgement where providing or obtaining such would compromise patient care.

From time to time, Mercer may disclose identifiable health information to other entities for use by the recipient for treatment. Further, Mercer may disclose identifiable health information to other entities to assist the recipient in obtaining payment and, under limited circumstances, may disclose identifiable health information to other entities for purposes associated with healthcare operations.

Health information may only be accessed, used or disclosed by authorized personnel. With the exception of the use and disclosure of health information directly related to treatment and to the extent practicable, access to health information by Mercer employees or other authorized personnel is restricted to the minimum necessary to execute their job responsibilities. It is the responsibility of each department, division or unit to identify those persons or classes of persons who are authorized to access, use or disclose health information and specifically to identify what health information they may have access.

Physical access to controlled areas and user accounts that provide access to protected health information are to be revoked upon the termination of an employee, student, or trainee or when others, such as contractors and vendors, no longer require access. All protected health information in the possession of these individual or entities is to be returned to Mercer or an attestation provided that such information has been destroyed or if that is not possible due to the nature of an on-going research effort, a statement attesting that the information will remain confidential and safeguarded as long as it is in the possession of the third party.

The unauthorized access to or unauthorized use or disclosure of health information that exists in any Mercer health record may subject the responsible employee, student, or trainee to disciplinary action up to and including termination of employment or suspension or expulsion from a student or trainee program. This extends to the unauthorized use or disclosure of health information that is overheard during the course of business or health information that is otherwise learned or secured by any Mercer employee, student or trainee by virtue of their employment or academic training association with Mercer.

Departments that become aware of the unauthorized use or disclosure of protected health information that causes or reasonably could cause harm should immediately report the incident to any University HIPAA privacy official. To the extent practicable, Mercer will attempt to minimize the known harmful effects and/or correct known instances of harm.

All Mercer employees who may use, disclose, or have access to identifiable health information contained in any health record must, as a condition of continued employment, complete an institutionally-sponsored training program that outlines employee responsibility and patient rights under the statutory privacy regulations contained in the Health Insurance Portability and Accountability Act (HIPAA). Additionally, all students or trainees who may use, disclose, or have access to any health information contained in any health record must complete an institutionally-sponsored training.

Mercer will, from time to time, disclose identifiable health information to business associates who have been contracted to provide services to the University. Health information provided to a business associate must be pursuant to an assurance that the business associate, and its sub-contractors, will use the information only for the purpose(s) intended, will restrict access to the information on a "need to know" basis only, and will otherwise take appropriate measures to safeguard the information in its possession. There must be a valid, signed business associate agreement in place before identifiable health information may be provided.

Except to the extent that patient care might be compromised, the use or disclosure of health information must comply with the University approved and published Mercer Notice of Privacy Practices. In addition, except to the extent that patient care might be compromised, the use and disclosure of an individual's health information must comply with any restrictions requested and subsequently agreed to by Mercer.

Additional Resources

The above represents a general statement of University operating policy. For further detail regarding this statement, see Statutory Requirements 45 CFR Sections 164. 502, 164.508, 164.512 and164.520.

Employees of the Mercer Health System should reference the Mercer Health System Policies and Procedures for HIPAA compliance guidelines.

History

Revised June 2003
Revised July 1, 2025