

Communication of Health Information - HIPAA General Operating Policy

I. POLICY STATEMENT

It is the policy of Mercer University (Mercer) to inform individuals about the institution's privacy practices as they relate to protected health information that may be stored in any Mercer file or depository, or stored electronically or that exists in any recording device or in any clinical or research data base, hereafter collectively referred to as the "health record", to safeguard health information in our possession, and, to the extent practicable, to protect the communication of health information, including oral information, from intentional or unintentional use or disclosure. It is further the University's policy to accommodate, to the extent practicable, the requests of individuals regarding the place, time, and method of communicating to them their own health information. For purposes of HIPAA compliance, employee records and student records subject to FERPA are specifically excluded from the definition of "health record".

II. POLICY PURPOSE

The purpose of this policy is to assure that all individuals are provided with adequate notice of Mercer's privacy practices and that Mercer employees treat health information to which they have access and the communication of that health information, whether in oral, written or electronic form, confidentially within the institution as well as when communicating health information to individuals outside the institution, including to the individuals themselves.

III. POLICY STANDARDS

Patients at Mercer, including those who are participants in treatment-oriented research, as well as participants in non-treatment-oriented research studies conducted at Mercer and from whom protected health information will be obtained will be provided the Mercer Notice of Privacy Practices and a good faith effort made to receive an acknowledgement of such receipt prior to the date of the first service delivery. Mercer will not knowingly use or disclose health information in a manner inconsistent with its privacy notice, except to the extent that emergency patient care would be compromised. Mercer reserves the right to amend the Notice of Privacy Practices as deemed necessary or advisable and, to the extent and in a manner practicable, will inform patients of material changes to the notice. The Mercer Notice of Privacy Practices constitutes an official University form and may not be amended, or otherwise altered, by any area of the University.

Health information that is communicated in any form is to be treated as confidential and in a manner that reasonably protects the communication from being intentionally or unintentionally overheard or intercepted by those who do not have a need or right to know the information. All procedures developed to support these policies must be approved by and be on file in the University HIPAA Privacy Officer's office. Each department must provide the Privacy Office with its procedures for securing information.

Mercer recognizes that in the treatment setting, communications must occur freely and quickly and there can be no assurance of absolute privacy. It is also recognized that the physical layout of the treatment area impacts the degree of confidentiality that may be achieved. However, it is the responsibility of each department, division or unit to implement procedures to achieve a reasonable degree of confidentiality within their respective areas and to establish operating policies and procedures that reasonably protect the confidentiality of oral, written and electronic communications.

Written communications that include identifiable health information, medical charts, files, electronic storage devices, fax machines, and other electronic equipment over which protected health information may be received or transmitted are to be maintained in secure sites and/or away from public access. Computer screens containing protected health information are to be inaccessible to public view. Computers that store

protected health information are to be secured before being left unattended.

Protected health information stored in computers is to be password protected. Passwords are individual specific and are not to be shared by or accessible to more than one individual. Each department is to advise Human Resources of all transfers and of all terminated employees so that Human Resources can arrange to have that employee's access to personal identifiable information removed.

As part of patient directory information, Mercer will communicate a patient's name, location in a Mercer in-patient facility, a patient's religious affiliation, and a patient's general condition to clergy, family, friends, and other interested parties. Mercer will, however, provide patients the opportunity and will honor their requests to have their information excluded from these patient directories if they so wish.

To the extent practicable, Mercer will accommodate the written request of an individual to have their health information communicated to them at a time, place, and in a manner of their choosing. If the request is impractical or impossible for the University to accommodate, this will be clearly communicated to the individual requesting the accommodation.

Mercer will recognize personal representatives authorized by our patients, by the courts, or by state law for purposes of communicating health information. Personal representatives may be parents or legal guardians of minor children or persons who are legally authorized or specifically identified by the patient themselves, such as a close friend or family member, to act on behalf of the patient. Mercer may, without prior authorization of the patient, and where necessary due to emergency or other professionally sound reason, communicate health information with persons directly involved in the care of a patient. Mercer may also refuse to provide information to personal representatives, or to the patient themselves, where it is determined that access to the information may be detrimental to or otherwise not in the best interest of the patient, may endanger or breach the confidentiality of a third party or is precluded by statute.

Violation of this policy or negligence on behalf of any Mercer employee, student or trainee resulting in or having the potential to result in the unauthorized release of identifiable health information may result in disciplinary action up to and including termination of employment or suspension or expulsion from a student or trainee program. Any Business Associate who violates this policy understands that the violation will result in the immediate termination of its underlying business contract with Mercer.

The above represents a general statement of Mercer operating policy. For further details regarding this statement, see Statutory Requirements 45 CFR Sections 164.510, 164.520 and 164.522.

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

Issued:
RMP/ogc