3359-11-19 Policies and procedures for release, privacy and security of selected health information.

(A) Definitions.

(1) "HIPAA." "HIPAA" is the "Health Insurance Portability and Accountability Act of 1996" and the "Administrative Simplification" regulations found in title 45 of the Code of Federal Regulations.

(2) Protected health information. Protected health information is individually identifiable health information as defined and protected under "HIPAA."

(B) Privacy official.

(1) The director of health services shall act as the university's privacy official and in that capacity shall coordinate the university's compliance with "HIPAA," including, but not limited to, gathering information sought by a requester, providing for the inspection of such information by the requestor, furnishing copies to the requestor, receiving complaints, establishing an internal privacy and security audit system, coordinating privacy and security training for affected areas of campus, coordinating with the university's information technology security officer, and attending and briefing the information technology security policy as necessary regarding "HIPAA" privacy and security issues. In order for the university to comply fully with "HIPAA," the university privacy official shall have full authority to gather such information as is necessary to comply with the request.

The university privacy official shall have the authority to designate an individual or individuals to assist with "HIPAA" compliance obligations.

(2) The university privacy official shall keep the office of general counsel informed with respect to all "HIPAA" requests and complaints and shall obtain advice and counsel with respect to compliance requirements.

(3) All university employees, students, and members of the workforce, as that term is defined by "HIPAA," shall cooperate fully with the university privacy official in "HIPAA" compliance efforts, including, but not limited to, providing the records requested, allowing for proper inspection and copying of the records, attending trainings, and conducting inspections and audits as necessary to conform with the requirements of the law.

(4) The university privacy official shall designate those academic and administrative health care units covered by "HIPAA" as part of the covered health care component of the university. The university privacy official shall maintain a list of all units covered by "HIPAA" and of all other units included within the covered health care component of the university, which serve as business associates within the university covered health care component for "HIPAA" purposes.

(5) The university privacy official shall have the authority to review all privacy, confidentiality and security standards and procedures created by academic and administrative departments that are part of the covered health care component of the university and to direct changes to such standards and procedures as necessary.

(C) Unit requirements.

(1) Academic and administrative departments determined by the university privacy official to be part of the covered health care component of the university shall:

(a) Develop unit specific standards and procedures to protect the privacy, confidentiality and security of protected health information that comply with "HIPAA" and with this rule.

(b) Train all unit employees, students, and members of the workforce, as that term is defined by "HIPAA," who have access to records protected by "HIPAA" on the "HIPAA" requirements, the university policies and procedures for release, privacy and security of selected health information, and the unit standard and procedures for privacy, confidentiality and security of records protected by "HIPAA." Such training must be conducted as the university privacy official deems necessary and within a reasonable period of time after a new individual joins one of the covered health care components.

(c) Coordinate distribution of a notice of privacy practices as necessary under "HIPAA." The notice of privacy practices must contain all "HIPAA" required elements and be approved by the university privacy official prior to being distributed.

(d) Document compliance efforts as required by "HIPAA."

(e) Comply with all federal, state, and local laws and regulations related to the privacy, confidentiality, and security of medical information.

(D) Business associates.

(1) Units within the covered health care component of the university may share protected health information with third parties, referred to as business associates, who provide the units within the covered component with services that use or involve health information. These units shall only share such information with business associates pursuant to a business associate agreement approved by the office of general counsel.

(E) University employees, students, and members of the workforce. University employees, students, and members of the workforce, as that term is defined by "HIPAA," in "HIPAA" covered components shall:

(1) Limit uses and disclosures of all health information to the minimum necessary to complete the assigned task.

(2) Upon discovery, report all incidents of misuse or improper disclosure of protected health information to the university privacy official.

(F) Retaliation.

(1) The university shall not tolerate nor engage in retaliation against any employee, student, or member of the workforce, as that term is defined by "HIPAA," who reports an incident of misuse or improper disclosure of protected health information to the university privacy official or to the secretary of the department of health and human services.

(G) Discipline for violations of "HIPAA," rule 3359-11-19 of the Administrative Code, or unit standards and procedures.

(1) All employees, students, or members of the workforce, as that term is defined by "HIPAA," who use or disclose protected health information contrary to unit standards and procedures, rule 3359-11-19 of the Administrative Code, or "HIPAA" shall be subject to discipline, which may include, but is not limited to, verbal and written warnings, suspension without pay, and termination.

(2) Covered components shall document any sanctions imposed for violations of "HIPAA," rule 3359-11-19 of the Administrative Code, or unit standards and procedures, as required by "HIPAA." and provide all documentation relevant to such sanctions to human resources for inclusion in the employee's personnel record.

Replaces:	3359-11-19
Effective:	01/31/2015
Certification:	_____ Ted A. Mallo Secretary Board of Trustees
Promulgated Under:	111.15
Statutory Authority:	3359.01
Rule Amplifies:	3359.01
Prior Effective Dates:	04/17/03, 11/06/06