

Name of Policy: [HIPAA Administrative Simplification](#)
(Health Insurance Portability and Accountability Act of 1996; Administrative Simplification incorporating the Security, Privacy, and Electronic Transaction Standards).

Policy Number: 3364-15-01

Issuing Office: Office of the President

Responsible Agent: Compliance Officer and Security Officer

Scope: All University of Toledo Campuses

OFFICIAL POLICY



Effective Date: July 1, 2006

(A) The purpose of this policy:

To set forth the compliance program, policy and practices of The University of Toledo for developing and maintaining reasonable and appropriate administrative and physical safeguards to ensure the confidentiality of identifiable health information as required by "HIPAA." "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, Public Law 104-91, enacted August 21, 1996, codified at 42 U.S.C. §1320d, the administrative simplification regulations found at Parts 160 through 164 of Title 45 of the Code of Federal Regulations, as may be amended.

(B) Administrative responsibility:

The President of The University of Toledo directs the HIPAA committee chaired by the privacy officer, or his or her designee, to take the steps necessary for HIPAA compliance, including:

- (1) Developing, implementing and maintaining a HIPAA compliance program,
- (2) Designating the health care components,
- (3) Approving and maintaining the privacy and security office,
- (4) Approving all HIPAA policies and procedures and their respective revisions,
- (5) Providing oversight to ensure the security and safety of certain health information, and
- (6) Developing, implementing and monitoring all other obligations required of the University under HIPAA.

(C) Designation as a hybrid entity and of University health care components:

- (1) The University designates itself as a hybrid entity.
- (2) The University designates the entire Health Science Campus in addition to certain departments or units on the Main Campus of the University as health care

components, which are covered entities for purposes of HIPAA compliance. The privacy officer maintains the list of the University health care components.

(3) Although compliance may not be required under the privacy regulations for departments other than the University health care components, all employees should maintain the privacy and confidentiality of any individual's health information that may be subject to other components of HIPAA, the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g (FERPA) and other applicable federal and state law.

(D) Business associate arrangements:

(1) The University may share protected health information with external parties, referred to as business associates, who are contracted specifically to provide the University services using health information. The University may only share protected health information with business associates pursuant to an approved business associate agreement.

(2) Conversely, University employees should use care when asked to enter into business associate agreements with third parties involving the receipt or disclosure of health information from an outside party. The University may only execute a business associate agreement for the receipt of health information pursuant to an approved business associate agreement.

(E) Privacy regulations:

(1) Only the University's designated health care components must comply with this part E. The privacy regulations and this part E only apply to protected health information, which is individually identifiable health information transmitted, maintained or received by a University designated health care component. The privacy regulations exempt from protected health information employment records and student health records under FERPA (including both FERPA education records and student health records not disclosed).

(2) Generally, University health care components may use or disclose protected health information to the individual who is the subject of the information or for purposes related to treatment, payment or health care operations, or as specifically permitted under HIPAA. University health care components may share protected health information within its own department only to those employees who have a valid business or medical need for the information and only where necessary to accomplish the intended purpose of the approved use, disclosure or request.

(3) Access to any protected health information stored in a file or depository, stored electronically, or that exists in any medium must be protected with sufficient protocols, procedures and practices and in compliance with law.

(4) The University is obligated to change its policies and procedures as necessary and appropriate to comply with changes in the law, including the standards, requirements, and implementation specifications of HIPAA. A University health plan that is part of a designated health care component may amend its plan documents to reflect the uses of protected health information if it wishes to obtain protected health information for any reason without an authorization.

(5) If a health care component wishes to use or disclose protected health information not otherwise permitted by HIPAA, the health care component must obtain an authorization from the individual that complies with applicable regulations.

(6) Health care components must maintain in written or electronic form the following procedures, which will be subject to approval by the University privacy officer:

(a) A procedure that documents disclosures made on a routine and recurring basis and that outlines the permitted and required disclosures of protected health information or when an authorization is necessary, and that also limits the disclosure of protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure or request for information.

(b) A procedure that outlines the University's application of appropriate administrative, technical and physical safeguards protecting the privacy of protected health information, and reasonably safeguarding this protected health information from any intentional or unintentional disclosure prohibited by HIPAA.

(c) A procedure outlining an individual's rights with respect to protected health information including providing a notice of privacy practices, providing access to an individual's protected health information, providing an accounting of disclosures, amending incorrect health information and providing the right to request additional protections. The procedure should also contain a directive for mitigating, to the extent practicable, any harmful effect known to the health care component of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of HIPAA.

(d) A procedure that provides a process for individuals to make complaints concerning this HIPAA policy and procedures of the University or the University's compliance with the HIPAA policy or procedures, including a method for documenting such complaints in a manner that maintains the confidentiality of the reporting individual. The procedure should also contain a prohibition on retaliatory or intimidating acts in response to an

individual exercising his or her rights under HIPAA or the complaint process.

(e) A procedure designating and documenting the privacy official who is responsible for implementing and maintaining the procedures of each health care component of the University and designating a person for receiving complaints in violation of HIPAA policies or procedures.

(f) A procedure setting forth the required initial and continued HIPAA training for University employees within the timeframes as required by the applicable regulations, including a directive for documenting this training.

(g) Any other procedures with respect to protected health information that is necessary for University compliance with the standards, implementation specifications or other requirements of HIPAA.

(7) Health care components must comply with the record keeping requirements under the applicable regulations.

(F) Security regulations:

Health care components must ensure that all health information subject to these security regulations, housed or transmitted electronically, holds reasonable protections depending on the needs and current technology in place. These reasonable protections will include:

(1) Administrative procedures including certification, incident response and reporting, contingency planning, documented policies and procedures and training;

(2) Physical safeguards, including physical access controls, workstation usage and placement, device and media disposal, re-use, and accountability;

(3) Technical security services, including access, audit and authorization controls; and

(4) Technical security mechanisms, including communications/network transmission controls.

(G) Standards for electronic transactions:

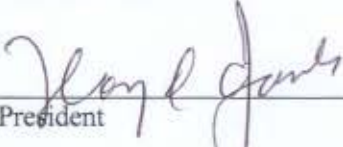
All University departments or units must electronically bill using the standardized formats, codes and data elements and comply with the rules governing such transactions.

(H) Violation of policy or procedures:

The failure of an employee to comply with this policy or any University HIPAA procedures will be grounds for discipline under the applicable disciplinary policies or collective bargaining agreement. These disciplinary proceedings shall not apply to workforce member "whistleblower" activities, crime victims or complaints, investigations or opposition as set forth in the applicable regulations. Health care components must document any sanctions applied under the disciplinary policies or collective bargaining agreements.

(I) Further guidance:

Employees of the University, including employees of the designated health care components, should refer to the University HIPAA procedures required by part E above, or under the respective privacy, security or transaction and code set regulations kept with the privacy officer for further compliance guidelines.

<p>Approved by:</p>  <hr/> <p>President</p> <p><i>Review/Revision Completed by: President's Senior Leadership Team HIPAA Committee Office of Legal Affairs</i></p>	<p>Policies Superseded by This Policy:</p> <p><i>3360-15-02 HIPAA Administrative Simplification (former Main Campus policy, previous effective date 2/26/03)</i></p> <p>Review/Revision Date:</p>
--	---