Name of Policy: **HIPAA IT Policy** **Policy Number:** 3364-65-19 **Approving Officer:** Executive Vice President of Finance and Administration **Responsible Agent:** Vice President of Information Technology **Scope:** All campuses – all institutional members see section (C)	**Original effective date:** July 18, 2014

x	New policy proposal	____	Minor/technical revision of existing policy
____	Major revision of existing policy	____	Reaffirmation of existing policy

(A) Policy statement

The University of Toledo strives to ensure the *confidentiality*, *integrity*, and *availability* of *electronic protected health care information* (*EPHI*) by implementing reasonable policies, procedures, and controls to prevent, detect, contain, and correct security violations; and by taking reasonable and appropriate steps to establish and implement the HIPAA Privacy Rule. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), is a law designed to provide privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals and other health care providers. The University of Toledo is required under the *HIPAA Security Regulations* to implement a security management process. This policy reflects The University of Toledo's commitment to comply with such regulations.

(B) Purpose of policy

This policy establishes safeguards to protect the confidentiality, integrity, and availability of Electronic Protected Health Information (EPHI) to address the requirements set forth by HIPAA.

(C) Scope

Affected by this policy are *all covered* components that may be designated by the University from time to time, including the UT College of Medicine & Life Sciences, UT College of Nursing, and the Student Health Center, and areas designated part of the healthcare component of the University, but only to the extent that each component performs activities that would make such component a *business associate* of a component of the University that performs covered functions if the two components were separate legal entities (*i.e., support components*). These support components include the Office of the Bursar, Controller's Division, including Accounts Payable, Information Technology Services, Office of Insurance and Risk Management, Internal Audit, Office of Compliance and Risk Management, Office of General Counsel, Office of Sponsored Programs, University Relations and Public Affairs, Public Safety, and University Development and Alumni Relations. The UT College of Medicine & Life

Sciences follows HIPAA-related policies and procedures created specifically for its environment; College of Medicine & Life Sciences compliance with HIPAA is coordinated through UTMC Medical Center. These policies affect all UT workforce members in covered components.

(D) Procedure

(1) Enforcement

All university policies shall be adhered to in order to maintain HIPAA compliance. In addition, the following policies have specific information and guidance contained within them as they relate to HIPAA Security Regulations.

3364-65-01 Electronic mail services policy
3364-65-02 Access control policy
3364-65-03 Transmission control policy
3364-65-07 Password security policy
3364-65-12 Workstation policy

(2) Exceptions

(a) Requests for exceptions to this policy must be submitted to information technology security and compliance.

(i) Each request for exception will be handled on a case-by-case basis;

(ii) Each exception approval will be documented by information technology security and compliance.

(3) Definitions

(a) Authentication: Act of proving an identity's authenticity or validity.

(b) Authorization: Act of validating the resources an identity is permitted to access.

(c) Administrators: Are designated by management and/or information technology to manage, process, or store information assets.

(d) Availability: Assurance that information, the computing systems used to process the information, and the security controls used to protect the information are all available and functioning correctly when the information is requested.

(e) Confidentiality: Assurance that information is accessible only to those authorized to have access.

(f) Data custodian: Are designated by management (data owners) to authorize users who may have access to particular information in a system or to reports for a specific area.

(g) Identification: Unique credential that identifies somebody or something.

(h) Information assets: Systems or repositories containing sensitive information or proprietary information.

(i) Institutional members: Anyone who participates in university activities, or has an affiliation with The University of Toledo. Includes, but is not limited to general staff, managers, medical staff, contractors, vendors, students, alumni and others involved in treatment, payment, or other normal operations of the university, whether or not they are paid by the university.

(j) Integrity: Assurance that information has not been modified or destroyed in an unauthorized manner.

(k) Management: Includes senior management, department chairpersons, directors and managers with responsibility for any employees. When management is not clearly implied by institutional design, the chief information officer will make the designation.

(l) Users: Are the individuals, groups, or institutions authorized to access information assets.

Approved by:	Superseded policies:
David R. Morlock Executive Vice President of Finance and Administration 7/22/14 Date *Review/Revision completed by: Vice President, Information Technology; HIPAA Leadership Committee; JCAHO IM Chapter Committee; IT Leadership; IT Administration*	None Initial Effective Date: July 18, 2014 Review/Revision Date: Next Review Date: July 18, 2017