


<p>Name of Policy: <u>HIPAA organizational structure and administrative responsibilities</u></p> <p>Policy Number: 3364-15-01</p> <p>Department: Office of the President</p> <p>Approving Officer: President</p> <p>Responsible Agent: Privacy Officer, Human Resources, Information Technology and Health Information Management</p> <p>Scope: The health care components of the University of Toledo and The University of Toledo Physicians, LLC</p>	 <p>Revision date: February 18, 2020</p> <p>Original effective date: July 1, 2006</p>				
<table border="0"> <tr> <td><input type="checkbox"/> New policy proposal</td> <td><input checked="" type="checkbox"/> Minor/technical revision of existing policy</td> </tr> <tr> <td><input type="checkbox"/> Major revision of existing policy</td> <td><input type="checkbox"/> Reaffirmation of existing policy</td> </tr> </table>		<input type="checkbox"/> New policy proposal	<input checked="" type="checkbox"/> Minor/technical revision of existing policy	<input type="checkbox"/> Major revision of existing policy	<input type="checkbox"/> Reaffirmation of existing policy
<input type="checkbox"/> New policy proposal	<input checked="" type="checkbox"/> Minor/technical revision of existing policy				
<input type="checkbox"/> Major revision of existing policy	<input type="checkbox"/> Reaffirmation of existing policy				

(A) Policy statement

The University of Toledo (UToledo) and The University of Toledo Physicians, LLC, (UTP) have a long-standing commitment to protect the confidentiality, integrity, and availability of identifiable Patient Health Information (PHI) by taking reasonable and appropriate steps to address the requirements of the Health Insurance Portability and Accountability Act (HIPAA) of 1996, as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH Act), and the Privacy and Security Regulations .

(B) The purpose of this policy:

- (1) Designate UToledo as a hybrid entity;
- (2) Designate UToledo and UTP as an Affiliated Covered Entity (ACE);
- (3) Define the organizational structure and administrative responsibilities as required by HIPAA; and
- (4) Designate a Privacy Officer and Information Security Officer and identify their administrative responsibilities.

(C) Scope

This policy applies to UTP (ACE) and all UToledo health care components (Hybrid) and their respective workforce members. Health care components are designated routinely by the Privacy and Security Committee. Health care components are identified on UToledo Privacy website and include the Health Science Campus, The University of Toledo Medical Center (UTMC), the Student Health Center, and designated departments of the Main Campus that perform HIPAA covered functions. A reference in this policy to the covered entity refers to UTP (ACE) and the designated components of UToledo (Hybrid).

(D) Designation as a hybrid entity:

- (1) UToledo designates itself as a hybrid entity; a single entity that is a covered entity whose business activities include both HIPAA covered and non-covered functions, and that designates health care components.
- (2) The Privacy and Security Committee determines and maintains the list of health care components. The health care components for purposes of HIPAA compliance include UToledo's entire Health Science Campus and designated departments or units on the UToledo Main Campus
- (3) The HIPAA requirements apply only to the health care components of UToledo and UTP referred to as "covered entity" going forward in this policy.

Although UToledo is a single legal entity, the covered entity must treat units not designated as part of the covered entity as an external entity with respect to uses and disclosures of PHI.

If a person performs duties for both the covered entity and for another unit of the university such workforce member must not use or disclose PHI created or received in the course of or incident to the member's work for the covered entity.

(E) Designation as a single Affiliated Covered Entity (ACE)

- (1) UToledo and UTP are affiliated, legally separate entities under common ownership that have joined together as an Affiliated Covered Entity (ACE) for purposes of complying with HIPAA, to be known as UToledo ACE.
- (2) The UToledo ACE will name a single HIPAA Privacy Officer and Information Security Officer, adopt common HIPAA policies and procedures, and issue a single Notice of Privacy Practices. The

UToledo ACE may use a single consent form to obtain consent for uses and disclosures for treatment, payment, or health care operations.

- (3) The UToledo ACE will comply with all UToledo policies that address HIPAA Privacy and Security regulations.
- (4) PHI may be used and disclosed among the UToledo ACE for all functions of the covered entities, consistent with all UToledo HIPAA Privacy and Security policies located on UToledo website: www.utoledo.edu/policies.

(F) Administrative responsibility:

- (1) A Privacy and Security committee will meet quarterly or more frequently as needed.
 - (a) The committee will operate under a charter approved by the committee. The committee will be chaired by the Privacy Officer and the Information Security Officer. Other members will be designated from time to time by the privacy officer and approved by existing members.
- (2) A security risk assessment will be reviewed to determine the effectiveness of HIPAA privacy.
- (3) The Privacy Officer
 - (a) Chairs the Privacy and Security Committee
 - (b) Develops and implements HIPAA compliance program
 - (c) Collaborates with the Information Security Officer to ensure compliance with HIPAA Privacy and Security Regulations.
 - (d) Develops and revises HIPAA Privacy policies and procedures
 - (i) Provides a process for individuals to make complaints concerning violations of HIPAA Privacy and Security policies and regulations.
 - (ii) Provides a method for documenting complaints and the investigation in such a manner that protects the confidentiality of the reporting individual.
 - (e) Investigates all reports of an incident document the investigation response, notification, and remediation follow through.
 - (f) Incident analysis will be reviewed with Legal Counsel to determine whether a reportable incident has occurred.
 - (g) Understands the HIPAA Privacy Rule and how it applies within each health care component.

- (h) Oversees the enforcement of patient privacy rights within each health care component.
- (i) Monitors the Health care components for compliance with privacy policies and procedures.
- (j) Develops and implements HIPAA privacy training for employees.
- (k) Develop and implement any other procedures with respect to PHI that is necessary for UToledo ACE compliance with the standards, implementation specifications or other requirements of HIPAA.

(3) Information Security Officer

- (a) Vice-chair of the Privacy and Security Committee, Vice-chair will present on Security Risk Assessment on a quarterly basis.
- (b) Performs the Security Risk Assessment and develops subcommittees to ensure that the assessment is updated as needed.
- (c) Ensures all health care components secure all PHI subject to these security regulations, housed or transmitted electronically, hold reasonable protections depending on the needs and current technology in place. These reasonable protections will include:
 - (i) Develops procedures including certification, incident response and reporting, contingency planning, documented policies and procedures and training;
- (d) Provide physical safeguards, including physical access controls, workstation usage and placement, device and media disposal, re-use, and accountability;
- (e) Provide technical security services, including access, audit and authorization controls; and
- (f) Provide technical security mechanisms, including communications/network transmission controls.
- (g) Understands the HIPAA Security Rule and how it applies within each health care component.
- (h) Develops appropriate policies and procedures to comply with the HIPAA Security Rule,
- (i) Analyzes and manages reasonably anticipated threats to the security of integrity of electronic PHI (ePHI) within each covered entity.
- (j) Ensures availability of ePHI through proper storage, backup, disaster recovery plans, contingency operations, testing, and other safeguards.

- (k) Monitors workforce members in each covered entity for compliance with security policies and procedures including auditing information system activity of workforce members and access reports.
- (l) Implements ePHI access controls and termination of access.
- (m) Identifies, evaluates threats to the confidentiality and integrity of ePHI.
- (n) Protects against uses or disclosures of ePHI that are not permitted under the Privacy Standards.
- (o) Responds to security incidents and actual or suspected breaches in the confidentiality or integrity of ePHI and maintaining security incident tracking reports.
- (p) Security incidents are reported to the Privacy Officer timely to investigate and determine through incident analysis if a reportable incident has occurred as determined in collaboration with Associate General Counsel.

(H) Standards for electronic transactions

UToledo ACE must electronically bill using the standardized formats, codes, and data elements and comply with the rules governing such transactions.

(I) Workforce members

Workforce members of UToledo ACE means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such covered entity, whether or not they are paid by the covered entity.

(J) Training requirements

UToledo ACE workforce members and employees who conduct business on the Health Science Campus who have access or may be exposed to PHI will complete online HIPAA training. Business Associates who need to access electronic PHI will follow all business associate agreement terms and conditions.

All UToledo ACE Workforce members must complete HIPAA Privacy and Security Training within 30 days of date from hire and annually thereafter.

(K) Violation of policy or procedures:

The failure of a workforce member to comply with this policy or any UToledo policy or procedure that relates to HIPAA or IT Security 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. The UToledo ACE must document any sanctions applied under the disciplinary policies or collective bargaining agreements.

(L) Monitoring/Auditing

Monitoring/Auditing of compliance with UToledo policies relating to HIPAA Privacy and Security will be performed to assure compliance with HIPAA Privacy and Security regulations.

<p>Approved by:</p> <p><u>/s/</u> Sharon L. Gaber, Ph.D. President</p> <p><u>February 18, 2020</u> Date</p> <p><i>Review/Revision Completed by:</i> <i>Privacy and Security Committee Office of Legal Affairs, SLT</i></p>	<p>Policies Superseded by This Policy:</p> <ul style="list-style-type: none"> • <i>HIPAA Administrative Simplification (former Main Campus policy, previous effective date 2/26/03)</i> • <i>3364-15-01 HIPAA Administrative Simplification Policy, effective date</i> • <i>3364-100-90-10 Privacy and Security Office Designation</i> • <i>3364-15-07 Compliance with privacy and security of protected health information (PHI)</i> • <i>3364-15-08 Health Insurance Portability and Accountability Act (HIPAA) compliance training policy.</i> <p>Initial effective date: July 1, 2006</p> <p>Review/Revision Date: Reviewed effective July 1, 2009; September 23, 2011; January 20, 2016, February 18, 2020</p> <p>Next review date: February 20, 2023</p>
--	---