3364-15-01 HIPAA organizational structure and administrative responsibilities.

(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 ~~"HIPAA." "HIPAA" means~~ the Health Insurance Portability and Accountability Act ("HIPAA") 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 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 ~~"~~UT~~"~~oledo as a hybrid entity;

(2) Designate ~~"~~UT~~"~~oledo 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~~"~~ affiliated covered entity ("ACE") and all ~~"~~UT~~"~~oledo ~~covered~~ health care components (hybrid) and their respective workforce members. ~~Covered~~Health care components are designated ~~from time to time~~routinely by the privacy and security committee. ~~Covered~~Health care components are ~~identified in the addendum to this policy~~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 ~~"~~UT.~~"~~oledo hybrid.

(D) Designation as a hybrid entity:

(1) ~~"~~UT~~"~~oledo 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 ~~covered~~health care components. The health care components for purposes of ~~"~~HIPAA~~"~~ compliance include ~~"~~UT~~P,"~~oledo's ~~the~~ 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 ~~"~~UT~~"~~oledo and ~~"~~UTP~~"~~ referred to as "covered entity" going forward in this policy.

Although ~~"~~UT~~"~~oledo 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 protected health information ("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 ~~protected health information~~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) ~~"~~UT~~"~~oledo 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 signal consent form to obtain consent for uses and disclosures for treatment, payment, or health care operations.

(3) The ~~"~~UToledo ACE~~"~~ will comply with all ~~"~~UT~~"~~oledo 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 ~~"~~UT~~"~~oledo website: https://www.utoledo.edu/policies/.

(F) Administrative responsibility:

(1) A privacy and security committee will ~~consist of the following representatives and operate under a plan developed by the committee:~~meet quarterly or more frequently as needed.

~~(a) Privacy officer~~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.

~~(b) Information security officer~~

~~(c) Legal counsel~~

~~(d) "UTP" designee~~

~~(e) Compliance officer, "UTP"~~

~~(f) Chief medical information officer~~

~~(g) Chief operating and clinical officer~~

~~(h) Director of information management~~

~~(i) "UTMC" clinic representative~~

~~(j) Director of internal audit and chief compliance officer~~

~~(k) Director of nursing~~

~~(l) Clinical trial division chief~~

(2) A security risk assessment will be reviewed to determine the effectiveness of HIPAA privacy.

(3) The privacy officer

(a) C~~o-c~~hairs 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 ~~breach and works with legal counsel to perform breach analysis,~~ document the investigation response, notification, and remediation follow through.

(f) Incident analysis will be reviewed by legal counsel to determine whether a reportable incident has occurred.

(g) Understands the ~~"~~HIPAA~~"~~ privacy rule and how it applies within each covered component.

(h) Oversees the enforcement of patient privacy rights within each covered component.

(i) Monitors the ~~covered~~ health care components for compliance with privacy policies and procedures.

(j) Develops and implements ~~"~~HIPAA~~"~~ privacy training for employees ~~within each covered component~~.

(k) Develop and implement any other procedures with respect to ~~protected health information~~PHI that is necessary for ~~"~~UToledo ACE~~"~~ compliance with the standards, implementation specifications or other requirements of~~"~~ HIPAA.~~"~~

(3) Information security officer

(a) ~~Co~~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 that all health care components secure all ~~health information~~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:

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 covered 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 ePHI ("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.

(G) 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.

(H) Workforce members

Workforce members of ~~"~~UToledo ACE~~,"~~ ~~including~~ 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. ~~of the designated health care components who have access or may be exposed to "PHI "will complete "HIPAA" training conducted by the privacy and security officer or their designee(s). Business associates who need to access electronic protected health information will follow all business associate agreement terms and conditions.~~

(I) 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" ~~P~~privacy and security training ~~upon hiring or prior to exposure to "PHI."~~within thirty days of date from hire and annually thereafter.

(J) Violation of policy or procedures:

The failure of a workforce member to comply with this policy or any "UT"oledo 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.

(K) Monitoring/auditing

Monitoring/auditing of compliance with "UT"oledo policies relating to "HIPAA" privacy and security will be performed to assure compliance with "HIPAA" privacy and security regulations.

~~(K) Definition~~

~~Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for the "UT ACE" or its healthcare components is under the direct control of the "UT ACE" or its healthcare components regardless of whether or not they are paid by the "UT ACE" or its healthcare components.~~

Effective: 4/2/2020

CERTIFIED ELECTRONICALLY

Certification

03/23/2020

Date

Promulgated Under:	111.15
Statutory Authority:	3364
Rule Amplifies:	3364
Prior Effective Dates:	04/25/2016