


<b>Name of Policy:</b> Confidentiality of patient information			
<b>Policy Number:</b> 3364-15-10		<b>Effective date:</b> August 14, 2023	
<b>Approving Officer:</b> President		<b>Original effective date:</b> November 18, 2008	
<b>Responsible Agent:</b> Privacy Officer			
<b>Scope:</b> Covered entities of the University of Toledo			
<b>Keywords:</b>			
	New policy	X	Minor/technical revision of existing policy
	Major revision of existing policy		Reaffirmation of existing policy

(A) Policy statement

The university of Toledo (UToledo) requires that all workforce members with access to protected health information (PHI) be committed to ensuring that PHI is protected and kept confidential. PHI shall be used and disclosed in accordance with applicable laws and UToledo policies.

(B) Purpose of policy

The purpose of this policy is to outline the appropriate use of PHI consistent with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and all updates allowing for the use and disclosure of PHI for treatment, payment, or health care operations. PHI includes all health and financial information pertaining to a patient and the relatives or household members of the patient (UToledo Policy: 3364-70-05 Protections of human subjects in research for confidentiality of research information.)

(C) Scope

This policy applies to all UToledo covered components (hybrid) and university of Toledo physicians (ACE) and their respective workforce members. Healthcare components are determined by the privacy and security committee as outlined in UToledo policy 3364-15-01 HIPAA organizational structure and administrative responsibilities. The hybrid list is maintained on the UToledo health care compliance and institutional privacy website.

- (D) Definitions for the purposes of UToledo HIPAA privacy policies
- (1) Affiliate: a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. A covered health care provider, health plan, or health care clearinghouse can be a business associate of another covered entity.
  - (2) Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under HIPAA Privacy Rule which compromises the security or privacy of the PHI based on a risk assessment conducted by the UToledo privacy office.
  - (3) Covered entity: a health plan, a healthcare clearinghouse or a healthcare provider who transmits any health information in an electronic form in connection with a transaction. See CFR 45 160.103 for the few statutory exemptions. See policy 3364-15-01.
  - (4) De-identification: in accordance with the HIPAA Privacy Rule, requires that the expert determination method be used or the following identifiers of the individual or of relatives, employers, or household members of the individual are removed:
    - (a) name;
    - (b) street address;
    - (c) city;
    - (d) county;
    - (e) precinct;
    - (f) zip code; all geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP code, and their equivalent geocodes, except for the initial three digits of the ZIP code if, according to the current publicly available data from the Bureau of the Census:
      - (i) The geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people; and
      - (ii) The initial three digits of a ZIP code for all such geographic units containing 20,000 or fewer people is changed to 000.
    - (g) gender;
    - (h) birth date;
    - (i) admission date;
    - (j) discharge date;
    - (k) date of death;
    - (l) age;
    - (m) telephone number;
    - (n) fax number;
    - (o) e-mail;
    - (p) Social Security number;

- (q) medical record number;
- (r) health plan beneficiary number;
- (s) account number;
- (t) certificate/license number;
- (u) vehicle ID number and license plate;
- (v) device identifier and serial number;
- (w) web universal resource locators (URLs);
- (x) internet protocol address (IP address);
- (y) biometric identifier, including finger and voice prints;
- (z) photographs; or
- (aa) any other unique identifying number, characteristic or code.

Note: ages over eighty-nine and all elements of date (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age ninety or older. Please seek assistance and/or approval from the privacy officer prior to de-identification.

- (5) Financial information: for the purpose of this policy includes but is not limited to:
  - (a) healthcare claims information (including diagnostic and procedure codes, services rendered, and charges associated with those services);
  - (b) insurance or other payment information;
  - (c) payment activity;
  - (d) coordination of benefits;
  - (e) claim status;
  - (f) referral certifications and authorizations;
  - (g) health claim attachments; and
  - (h) collection activity documentation.
- (6) Health plan: any individual or group that provides or pays the cost of medical care, including public and private health insurance issuers, HMOs, or other managed care organizations, employee benefit plans, the Medicare and Medicaid programs, military/veterans plans, and other policy, plan or programs for which a principal purpose is to provide or pay for healthcare services.
- (7) Healthcare provider: (as defined in section 1861(u) of the Social Security Act, 42 USC 1395x(u)): a provider of medical or health services, as defined in this section (as defined in section 1861(u) of the Social Security Act, 42 USC 1395x(u)), any other person or organizations who furnishes, bills, or is paid for healthcare in the normal course of business.
- (8) Workforce member: an employee, volunteer, trainee, and other person whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

(E) Procedure

All patient information that identifies or can be used to identify an individual is confidential and must be safeguarded.

- (1) PHI may be accessed by the UToledo workforce members who are directly or indirectly involved in the patient's care or finances and those who have a need to know the information to perform specific tasks or provides specific services.
- (2) Affiliates must maintain the confidentiality of patient information in compliance with the privacy and security regulations and UToledo policies.
- (3) Persons not involved with a patient's care or finances and/or who do not have a specific need to know patient information for the performance of specific tasks or to provide specific services shall neither have nor seek access to patient information. Unauthorized access to PHI is prohibited and upon discovery, sanctions may be applied to the employee up to and including termination, as deemed appropriate given the circumstances.
- (4) Access to use and disclosure of PHI shall be limited to the minimum necessary to perform a specific task or provide a specific service except when a healthcare provider accesses for treatment purposes. See UToledo policy minimum necessary guidelines for use/disclosure of protected health information requirements to protected health information (3364-90-02).
- (5) Release of health information must be safeguarded by following the HIPAA regulations and UToledo policies.
- (6) Covered entity should limit uses, disclosures and requests for patient information to the minimum necessary and it is good practice to de-identify (45 CFR Section 164.514).
- (7) Reasonable effort must be taken to maintain the confidentiality of PHI, by using appropriate physical, technical and administrative safeguards, including but not limited to:
  - (a) Selecting private settings to conduct interviews, refraining from discussing patient information in public areas, assuring location of records and files in non-public areas, and placing computers and electronic devices in appropriate locations and positions.
  - (b) Electronic devices that contain PHI must incorporate the use of password protection. The physical security of the device must always be maintained by the user.

- (c) When accessing patient information, computers should not be left unattended. If one must leave their computer unattended, it should be locked or logged off.
  - (d) Use of electronic mail system for PHI must follow electronic communication policy 3364-65-07.
  - (e) Voice mail messages containing PHI generally should not be left on recorders. Messages to patient should be messages containing confidential patient information generally should not be left on recorders. Messages to patient recorders should be limited to pre-registration information, confirmation of appointments, or to solicit a return call, unless otherwise agreed or requested by a patient.
  - (f) PHI must be appropriately disposed of, See UToledo policy 3364-90-16 medical record retention and destruction; disposal of protected health information.
  - (g) To mitigate security risks to individuals for the secondary use of data, for example: comparative studies, policy assessment, and research, patient information should be de-identified. The Privacy Rule does not restrict the use or disclosure of de-identified health information, as it is no longer considered protected health information, see UToledo policy 3364-90-05 de-Identifiable and re-identifiable health information, limited data set and data use agreement policy.
- (8) A confidentiality statement acknowledging that an individual is aware of and understands UToledo's confidentiality policy shall be signed prior to any person obtaining access or exposure to patient information.
- (9) Individuals with access to patient health information are educated about confidentiality during orientation and during training on the hospital information system. Access to the hospital information system requires identification and password as defined by UToledo's policy information security and technology administrative safeguards policy 3364-65-02.
- (10) Breaches of unsecured PHI and other incidents involving PHI must be reported to and investigated by the privacy officer in accordance with institutional corrective action/disciplinary policies.

<p><b>Approved by:</b></p> <p>/s/</p> <hr/> <p>Gregory Postel, MD President</p> <p><b>Date:</b> August 14, 2023</p> <p><b>Review/revision completed by:</b></p> <ul style="list-style-type: none"><li>• <i>Compliance and Institutional Privacy Office</i></li></ul>	<p><b>Policies superseded by this policy:</b></p> <ul style="list-style-type: none"><li>• <i>01-063 Confidentiality of patient information (former Health Science Campus policy reviewed July 1, 2003)</i></li></ul> <p><b>Original effective date:</b> <i>November 18, 2008</i></p> <p><b>Review/revision date:</b> <i>June 27, 2016</i> <i>February 18, 2020</i> <i>August 14, 2023</i></p> <p><b>Next review date:</b> <i>August 14, 2026</i></p>
--	--