


Name of Policy: Confidentiality of patient information Policy Number: 3364-15-10 Approving Officer: President Responsible Agent: Compliance and Privacy Officer Scope: “Covered Entities” of The University of Toledo		 Initial Effective date: November 18, 2008	
	New policy proposal	<input checked="" type="checkbox"/>	Minor/technical revision of existing policy
	Major revision of existing policy	<input type="checkbox"/>	Reaffirmation of existing policy

(A) Policy statement

The University of Toledo requires that all workforce employees employed in a designated “covered entity” and have access to patient information be committed to ensuring that patient information is protected and kept confidential. Patient information shall be used and disclosed in accordance with applicable laws and university policy.

(B) Purpose of policy

The purpose of this policy is to outline the appropriate use of confidential patient information consistent with the Health Insurance Portability and Accountability Act (HIPAA) privacy rule allowing for the use and disclosure of patient information for treatment, payment, or health care operations. Patient information includes all health and financial information pertaining to a patient and the relatives or household members of the patient.

(C) Procedure

HIPAA Administrative Simplification policy 3364-15-01 designated the university as a hybrid entity. The entire health science campus in addition to certain departments or units on the main campus of the university are designated as health care components, which are covered entities for purposes of HIPAA compliance.

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

- (1) Access to patient information is limited to University of Toledo workforce who is directly or indirectly involved in a patient’s care or finances and who have a need to know the information to perform specific tasks or provides specific services.

Examples of those who can have access to confidential patient information include but are not limited to:

- (a) Employees,
- (b) Faculty
- (c) Volunteers and trainees
- (d) Medical staff members
- (e) Residents
- (f) Students
- (g) Business associates who are directly or indirectly involved in a patient's care or finances and who have a need to know the information

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.

- (2) Access to patient information shall be limited to the minimum necessary to perform a specific task or provide a specific service.
 - (a) Minimum necessary requirements to patient health information must follow policy 3364-100-90-2.
- (3) Release, use or disclosure of patient health information must follow university policy. Release of health information must be safeguarded by instituting the following:
 - (a) Each department shall develop and implement appropriate physical, technical and administrative safeguards to protect the confidentiality of patient information.
 - (b) Reasonable efforts to maintain patient confidentiality may include selecting private settings to conduct interviews, refraining from discussing patient information in public areas, location of records and files in non-public areas, appropriate location and position of computers and electronic devices.
 - (c) PDAs that contain PHI must incorporate the use of password protection. The physical security of the device must always be maintained by the user.
 - (d) Use of electronic mail system for patient information must follow electronic mail services policy 3364-65-01.
 - (e) Facsimile transmission of patient information must follow policy 3364-100-50-32.
 - (f) Voice 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.

- (4) Protected patient information in regards to additional copy print outs is limited by function through the university information system. Additional copies generated must follow the disposal of protected health information policy 3364-15-09.
- (5) A confidentiality statement acknowledging that an individual is aware of and understands the university confidentiality policy shall be signed prior to any person obtaining access or exposure to patient information.
- (6) Individuals with access to patient health information are educated about confidentiality during orientation and during training on the hospital information system with an annual review.
 - (a) Access to the hospital information system requires identification and password as defined by access control policy 3364-65-02.
- (7) Breaches of confidentiality will be reported to and investigated by the privacy officer in accordance with institutional corrective action/disciplinary policies.

(D) Definitions

- (1) Covered Entity –An organization that routinely handles protected health information in any capacity is in all probability a covered entity. See 45 CFR 160.103 for the few statutory exemptions. The health science campus is considered a covered entity and specific departments on the main campus will be designated as a covered entity.

Covered Entity further defined by HIPAA regulations directly cover three basic groups of individuals or corporate entities: health plans, health care providers, and health care clearinghouse. Each of these in turn is given an expansive regulatory definition, summarized as follows:

- (a) Health plan means 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 it to provide or pay for health care services.
- (b) Health care provider means a provider of medical or health services, and any other person or organizations who furnishes, bills, or is paid for health care in the normal course of business; and

- (c) Health care clearinghouse means a public or private entity, including a billing service repricing company, community health information system, and “value-added” networks and switches, that either processes or facilitated the processing of healthcare information.
- (2) Patient information -includes all health information and financial information pertaining to a patient and the relatives or household members of the patient.
- (3) Health information is defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and includes any information, whether oral or recorded in any form or medium, that is created or received by a health care provider and relates to the past, present or future physical or mental health or condition of an individual, the provision of health care services to an individual, or the payment for the provision of health care services.

Health information may be found in medical records, patient information stored in computerized data bases, patient census lists, operating room schedules, "white patient boards" and admission/discharge lists.

- (4) Financial information for the purpose of this policy includes but is not limited to:
 - (a) health care 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.

Financial information may be information generated by the university or received from other parties, such as third party payers. (See 3364-70-05 Protections of human subjects in research for confidentiality of research information.)

- (5) Protected health information is health information that identifies or can be used to identify an individual is considered protected health information (PHI) under HIPAA. Any of the following information pertaining to a patient or the relatives, employees or household members of the patient can be used to identify a patient which include but is not limited to:
 - (a) name;

- (b) street address;
 - (c) city;
 - (d) county;
 - (e) precinct;
 - (f) zip code;
 - (g) genocide;
 - (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 number;
 - (s) account number;
 - (t) certificate/license number;
 - (u) vehicle ID number and license plate;
 - (v) device identifier;
 - (w) web location, Internet Address;
 - (x) biometric identifier;
 - (y) photographs; or
 - (z) any unique ID.
- (6) Workforce - 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 entity, whether or not they are paid by the covered entity.

<p>Approved by:</p> <p><u>/s/ laj</u> Lloyd A. Jacobs, M.D. President</p> <p><u>November 18, 2008</u> Date</p> <p><i>Review/Revision Completed by:</i></p> <p><i>Compliance and Privacy Officer, Office of Legal Affairs</i></p>	<p>Policies Superseded by This Policy:</p> <ul style="list-style-type: none"> • <i>01-063 Confidentiality of patient information (former Health Science Campus policy reviewed 07/01/03)</i> <p>Initial Effective Date: November 18, 2008</p> <p>Review/Revision date:</p> <p>Next review date: November 18, 2011</p>
--	--