3364-15-10 Confidentiality of patient information.

(A) Policy statement

The university of Toledo "UT" requires that all workforce members that 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 policies.

(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 and all updates 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 (See rule 3364-70-05, protections of human subjects in research for confidentiality of research information.)

(C) Procedure

Organizational structure and administrative responsibilities rule 3364-15-01 designated "UT" and "UTP" as an affiliated covered entity "ACE" and designated "UT" as a hybrid entity. The entire health science campus in addition to certain departments or units on the main campus of "UT" are designated as health care components and "UTP" as an "ACE" which are covered entitles 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) Patient information may be accessed by the university 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. Examples of those who can have access to confidential patient information include, but are not limited to:

(a) Employees

(b) Faculty
(c) Volunteers and trainers
(d) Medical staff members
(e) Residents
(f) Students

(2) Affiliates who are provided access for the purpose of continuity of care must maintain the confidentiality of patient information in compliance with the privacy and security regulations and university policies. Those persons who are considered affiliates are but not limited to:

(a) Residents from other affiliated hospitals
(b) Hospice
(c) Physicians and their staff from other affiliated hospitals and/or clinics that refer patients to the university of Toledo medical center
(d) Cancer registry

(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.

(4) Access to use and disclosure of patient information shall be limited to the minimum necessary to perform a specific task or provide a specific service except when a heathcare provider accesses for treatment purposes.

Minimum necessary requirements to patient health information must follow rule 3364-100-90-2.

(5) Release of health information must be safeguarded by following the "HIPAA" regulations and university rules. As well as taking reasonable effort to maintain the confidentiality by using appropriate physical, technical and administrative safeguards, including but not limited to:

Selecting private settings to conduct interviews, refraining from discussing patient information in public area, assuring location of records and files in non-public area, and placing computers and electronic devices in appropriate locations and positions.

(a) 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.

(b) When accessing patient information computers should not be left unattended, if one must leave their computer unattended, it should be locked or logged off.

(c) Use of electronic mail system for patient information must follow electronic mail services rule 3364-100-50-32.

(d) Voice messages containing confidential patient information 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. Protected patient information in regards to additional copy print outs is limited by function through "UT's" information system. Additional copies generated must follow the disposal of protected health information rule 3364-15-09.

(6) A confidentiality statement acknowledging that an individual is aware of and understands the university's confidentiality policy shall be signed prior to any person obtaining access or exposure to patient information**.**

(7) 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 access control rule 3364-65-02.

(8) Breaches and other incidents involving patient confidentiality must be reported to and investigated by the privacy officer in accordance with institutional corrective action/disciplinary policies.

(D) Definitions

(1) 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 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 and "UTP" as an "ACE" will be designated as a covered entity. See rule 3364-15-01.

(2) 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.

(3) Health care 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 health care in the normal course of business.

(4) Health information is any information, including genetic information, whether oral or recorded in any form or medium, that (45 CFA 160.103):

(a) Is created or received by a health care provider, health plan, public health authority, employer, lifer insurer, school or university of heath care clearinghouse.

(b) Related to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

(5) Health information technology means hardware, software, integrated technologies or related licenses, intellectual property, upgrades, or packaged solutions sold as services that are designed for or support the use by health care entities or patients for the electronic creation maintenance, access, or exchange of health information [HITECH act, section 3000(5)].

(6) 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.

(7) 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;
(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”.

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.

(8) Workforce member is 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.

Effective: 07/11/2016

CERTIFIED ELECTRONICALLY

Certification

06/30/2016

Date

Promulgated Under:	111.15
Statutory Authority:	3364
Rule Amplifies:	3364