UTHealth
The University of Texas Health Science Center at Tyler

Origination Date:	*12/2005*
Last Approved:	*04/2017*
Last Revised:	*04/2017*
Next Review:	*04/2020*
Owner:	*Donna Martin: Director Compliance*
Policy Area:	*Information Resources*
References:	

Confidential Information

Scope

All University of Texas Health Science Center at Tyler (the "University") faculty, staff, students, volunteers, and any other contractors or agents granted access to confidential information.

Purpose

To provide guidance for accessing confidential information, including Protected Health Information (PHI).

POLICY

There may be times when University employees, contractors, consultants, students, interns, volunteers or others have knowledge of confidential information regarding patients, fellow employees, passwords or other sensitive information. Confidential information regarding patients includes, but is not limited to, all PHI, medical records, personal data and/or health status data (see HIPAA Privacy section below.). The privacy of others must be respected and, except in the line of duty, this information must not be discussed.

Sharing of computer passwords and/or IT data, as outlined in the IHOP Information Resources Acceptable Use, is prohibited. All employees, contractors, consultants, students and volunteers are required to comply with any departmental policies related to protection of confidential information. Unauthorized release of confidential or sensitive information will result in disciplinary action, including termination. For contractors and consultants, this may include termination of the work engagement. For interns and volunteers, this may include dismissal. Any student violating this policy will be referred to student judicial services at the student's home campus. All individuals are subject to possible civil and criminal prosecution.

HIPAA CONFIDENTIALITY GUIDELINES

The Health Insurance Portability and Accountability Act ("HIPAA") has established privacy and security standards with mandatory guidelines for protecting PHI. This policy states the levels of Breach of Confidentiality and guidelines for further corrective action.

University staff, contractors, consultants, students, interns and volunteers are expected to maintain patients' confidentiality of PHI and follow the privacy and security standards set by federal and state regulations. Breach of Confidentiality, Privacy and/or Security from inappropriate access to use or release confidential information will lead to corrective action (sanctions), which may include termination of employment.

Staff, contractors, consultants, students, interns and volunteers may only access patient PHI on a "need to

know" basis when directly involved in the treatment, payment, or health care operations for that patient.

PHI disclosed to a University employee under any other circumstance, including when authorization has been given by the patient, must be obtained through the standard process using the HIM Release of Information Office. An employee must not use online access to an electronic health record (EHR) to access patient PHI when this access is not directly related to his/her job function. This includes, but is not limited to, inquiries on family members. It is permissible to use the approved patient portal to access one's own medical information residing there or for those patients who have given the user authorization to access their information via the patient portal.

Employees working on specific projects and investigations in areas such as Internal Audit and Compliance will be authorized to view relevant PHI under the provision of health care operations with prior supervisory approval.

Level of Breach

Breaches of confidentiality/privacy and/or security have been divided into three (3) levels:

Level I. Carelessness/Not Following Procedures

This level of breach occurs when a person carelessly or inappropriately accesses, reviews or reveals information to him/herself or others without a legitimate need to know. Examples include, but are not limited to:

a. Discussing patient information in a public area;
b. Leaving a copy of patient information in a public area;
c. Leaving a computer unattended with patient information unsecured;
d. Accessing one's own medical information.

Level II. Curiosity or Concern (No Personal Gain)

This level of breach occurs when a person intentionally accesses or discusses patient information for purposes other than the care of the patient or hospital operations, but for reasons unrelated to personal gain. Examples include, but are not limited to:

a. Review of a public personality/high profile personality record;
b. Use of another's password to access computerized patient information;
c. Accessing the medical record of relatives, neighbors, coworkers, friends or any others out of curiosity or concern;
d. Discussing confidential information with those who do not have a need to know;
e. Obtaining medical information under false pretenses such as a forged authorization.

Level III. Personal Gain or Malicious Intent

This level of breach occurs when a person accesses, reviews or discusses patient information or sensitive information for personal gain or with malicious intent. Examples include, but are not limited to:

a. Review of a medical record of a patient with whom the person has a relationship;
b. Compiling a patient list for personal use or to be sold;
c. Releasing patient information to the media regarding a public personality.

Enforcement

Violation of this policy may result in disciplinary action that may included termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or explusion in the case of a student. Addtiitonally, individuals are submjtect to loss of University Information Resosources access privileges, civil, and criminal prosecution.

References

Federal and State Privacy laws including:
HIPAA - Health Insurance Portability and Accountability Act;
HITECH Act (42 USC §17921 et. seq.)
Texas Administrative Code 202.70;
UTS-165 UT System Information Resources Use and Security Policy (includes Confidentiality of Social Security Numbers and confidentiality and integrity of Digital Research Data

Attachments:

No Attachments

Approval Signatures

Step Description	Approver	Date
	Kirk Calhoun: President/Prof of Medicine	04/2017
Executive Cabinet	Carol Davis: Executive Assistant, Senior	04/2017
Office of Legal Affairs	Terry Witter: VP, Legal Affairs/ChiefLegalOf	03/2017
Faculty Senate	Julie Philley: Assoc Prof Of Medicine	03/2017
	John Yoder: VP, Information Technology/CIO	03/2017

Applicability

UTHealth