



TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER

Operating Policy and Procedure

HSC OP: 52.09, **Confidential Information**

PURPOSE: The purpose of this Health Sciences Center Operating Policy and Procedure (HSC OP) is to identify and protect information made confidential by law or TTUHSC policy.

REVIEW: This HSC OP will be reviewed on May 1 of each odd-numbered year (ONY) by the Institutional Compliance Officer, the Assoc. VP for Human Resources, the Associate Provost for Student Affairs, the Director of Student Business Services, the Office of General Counsel, the Information Security Officer (ISO), and the VP for Information Technology and Chief Information Officer (CIO). Any substantive revisions will then be forwarded to the People and Operations Council.

POLICY/PROCEDURE:

1. Definitions.

- a. **CONFIDENTIAL INFORMATION** includes, but is not limited to, the following in any form or format:
 - i. Financial information obtained in connection with the award and issuance of student loans which is protected under the Gramm-Leach-Bliley Act of 1999 (GLBA), 15 U.S.C. 6801, *et. seq.*, implemented by 16 C.F.R. Part 314, and as may be amended.
 - ii. Private and personally identifiable information obtained in the regular course of business, such as social security numbers, driver's license numbers, unpublished home addresses or phone numbers, personal account numbers, computer passwords and accounts, biometric information, educational records, financial information, credit card information, and protected health information.
 - iii. Protected Health Information (PHI) is information protected under the Health Insurance Portability and Accountability Act (HIPAA) of 1996, 45 C.F.R. Parts 160 *et. seq.*, Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, 42 U.S.C. § 300jj *et. seq.*; 17901 *et. seq.*, as may be amended.
 - iv. Education Records has the same meaning as set forth in [HSC OP 77.13](#), Student Education Records, and is information protected under the Family Educational Rights and Privacy Act of 1974 (FERPA), also known as the Buckley Amendment, 20 U.S.C. §1232g, as may be amended.
 - v. Medical Committee and Medical Peer Review Committee records.
 - vi. Any other information made confidential by federal or state law or TTUHSC policy including, but not limited to, research information, passwords, and access codes.
- b. **Students** refers to individuals who are or have been enrolled at TTUHSC.
- c. **Volunteers** are those individuals as defined in [HSC OP 10.28](#), Volunteer Policy.

2. General Policy.

- a. Anyone who has access to CONFIDENTIAL INFORMATION regarding TTUHSC employees, Students, patients, affiliates, or any other information made confidential by

TTUHSC policies or law will take reasonable and necessary steps to maintain the confidentiality and privacy of such information.

- b. Security, access to, and use, and/or disclosure of protected health information (PHI) shall be governed by [HIPAA Privacy Policy 1.0](#) Framework of HSC HIPAA Privacy and Security Program.
- c. Security, access to, and use, and/or disclosure of certain financial information that is covered by the Gramm-Leach-Bliley Act of 1999, shall be governed by the TTUHSC INFORMATION SECURITY PLAN FOR FINANCIAL INFORMATION ([Attachment A](#)).
- d. Security, access to, and use, and/or disclosure of student education records shall be governed by Family Educational Rights and Privacy Act (FERPA) and [HSC OP 77.13](#), Student Education Records. Access to student educational records is granted on the basis of a legitimate educational interest of the employee, Student or Volunteer.
- e. Use of portable devices containing Confidential Information is subject to the requirements of [IT OP 56.20](#), Cloud Computing.
- f. TTUHSC shall require execution of a CONFIDENTIALITY AGREEMENT ([Attachment B](#)) by employees, Students, and Volunteers at the start of employment or affiliation with TTUHSC, and annually thereafter. Annual Confidentiality Agreement is executed in conjunction with annual HIPAA training administered by the Office of Institutional Compliance (IOC).
- g. Notice. Implementation shall include notifying employees, Students, and Volunteers of this policy, and when appropriate, also notifying any other individuals designated by TTUHSC Information Security Plan for Financial Information, [HSC OP 56.01- Acceptable Use of Information Technology Resources](#), [HSC OP 77.13](#), *Student Education Records*, and/or [HIPAA Privacy Policy 1.0](#) Framework of HSC HIPAA Privacy and Security Program.
- h. Procedures. Implementation shall include developing procedures to obtain a signed CONFIDENTIALITY AGREEMENT (Attachment B) from all individuals in an area of responsibility, and confirming that properly signed Confidentiality Agreements become part of an individual's employment, Student, or Volunteer record.
- i. Written agreements between TTUHSC and other parties which involve use of and/or access to TTUHSC CONFIDENTIAL INFORMATION shall require the other parties to comply with TTUHSC policies regarding confidentiality.

3. **Suggested Departmental Safeguards.**

Each School is responsible for establishing procedures necessary to implement this HSC OP. It is recommended that Schools utilize the following practice to protect CONFIDENTIAL INFORMATION:

a. **Printed Copies.**

Use. Records containing CONFIDENTIAL INFORMATION should be secured when not in use. For example, the records may be locked in a desk drawer or filing cabinet. Departments should review documents to confirm that ONLY the last four digits of the consumer credit card account number or social security number (where feasible) is readable before scanning or exporting paper documents into an electronic document management system.

Disposal. When necessary to discard documents containing CONFIDENTIAL INFORMATION, such documents should be disposed of by shredding, or using a comparable method designed to ensure privacy per [HIPAA Privacy Policy 4.12](#) *Disposal*

of PHI.

b. **Electronic Data.**

Persons with access to electronic data containing CONFIDENTIAL INFORMATION should take adequate steps to ensure that such information is not used by or made accessible or released to unauthorized sources. When it becomes necessary to erase files containing such information, the files should be erased completely so that the information contained in the files cannot be recovered by accessing undeleted programs.

c. **Review of Departmental Processes.**

Department personnel should be aware of the types of information being gathered within the department, such as sign-in sheets, forms of identification, retrieval and use of records and posting of information. Department personnel or the Information Owner should determine the necessity of obtaining private or personally identifiable information and revise processes where appropriate.

d. **Other.**

The effort to safeguard CONFIDENTIAL INFORMATION should not be limited to the above three categories. Changing technologies or laws may make additional safeguards necessary.

4. **Reporting Violations.**

a. Anyone who knows of or suspects a violation of this policy shall report that incident promptly to his/her immediate supervisor or the appropriate dean, and/or the Assistant Provost for Student Affairs, or in accordance with TTUHSC Information Security Plan for Financial Information, [HSC OP 56.01](#), Acceptable Use of Information Technology Resources, [HSC OP 77.13](#), Student Education Records, and/or [HIPAA Privacy Policy 1.0](#) Framework of HSC HIPAA Privacy and Security Program, as applicable.

i. In cases where the immediate supervisor is the known or suspected violator, employees shall report the known or suspected violation to the next higher administrative supervisor, or Institutional Compliance Officer, the VP for Human Resources, or the Title IX Coordinator, when appropriate.

ii. Reports may also be made through the anonymous Compliance Hotline at www.ethicspoint.com or through the toll-free number, 1-866-294-9352.

b. All information acquired in the investigation of any known or suspected violation of this policy shall be confidential unless disclosure is authorized or required by law.

5. **Disciplinary Action.**

a. **Employees.** Employees found to be in violation of this policy may be subject to legal action and may be disciplined in accordance with applicable policies including, but not limited to, the following:

i. Non-faculty employees. See [HSC OP 70.31](#), Employee Conduct, Coaching, Corrective Action, and Termination.

ii. Faculty employees. See [HSC OP 60.01](#), Tenure and Promotion Policy.

b. **Students.** Policies and procedures concerning students are set forth in the TTUHSC Students Handbook.

c. **Volunteers.** Violation of this policy will result in loss of privileges, removal from institutional facilities, and possible legal action.

5. **Right to Change Policy.** TTUHSC reserves the right to interpret, change, modify, amend, or rescind this policy in whole or in part at any time without the consent of employees.