Information Security Plan for Financial Information
Texas Tech University Health Sciences Center El Paso

1. Introduction

This Information Security Plan ("Plan") describes Texas Tech University Health Sciences Center El Paso (TTUHSC EP)'s safeguards to protect *covered data and information*. [1] These safeguards are intended to:

- Promote security and confidentiality of covered data and information;
- Protect against anticipated threats or hazards to the security or integrity of such information; and,
- Protect against unauthorized access to or use of covered data and information that could result in substantial harm or inconvenience to any individual who has provided covered data and information.

This Plan also provides mechanisms to:

- Identify and assess the risks that may threaten covered data and information maintained by TTUHSC EP;
- Develop written policies and procedures to manage and control these risks;
- Implement and review this Plan; and,
- Adjust this Plan to reflect changes in technology, the sensitivity of covered data and information and internal or external threats to information security.

2. Identification and Assessment of Potential Risks to Covered Data and Information

TTUHSC EP recognizes that both potential internal and external risks exist. These potential risks include, but are not limited to the following:

- Unauthorized access of covered data and information by someone other than the owner of the covered data and information;
- Compromised system security as a result of system access by an unauthorized person;
- Interception of data during transmission;
- Loss of data integrity;
- Physical loss of data in a disaster;
- Errors introduced into the system;
- Corruption of data or systems;
- Unauthorized access of covered data and information by employees;
- Unauthorized requests for covered data and information;

---

[1] *Covered data and information,* for the purposes of this Plan, means *nonpublic personal information* that is obtained from *financial activities* and that is required to be protected under the Gramm-Leach-Bliley Act (GLBA) of 1999, 15 U.S.C. 6801, *et seq*., implemented by 16 CFR Part 314. For definitions of *nonpublic personal information* and *financial activities*, refer to 16 CFR 313.3(n), 16 CFR 313.3(o), and 12 USC 1843(k), respectively. *Nonpublic personal information* includes, but is not limited to, the awarding and issuance of student loans to students, receiving income tax information from a student's parent when offering a financial aid package, and other miscellaneous financial services. Examples of personal information could include addresses, phone numbers, bank and credit card account numbers, income and credit histories, payment histories, and Social Security numbers, in both paper and electronic format. However, the Federal Educational Rights and Privacy Act of 1974 does allow for disclosure of "directory information" in certain circumstances. 34 CFR Part 99. *Directory information* is information that relates to students including, but not limited to, name, address, degrees and awards received 20 U.S.C. § 1232g(a)(5)(A).

- Unauthorized access through hardcopy files or reports; and,
- Unauthorized transfer of covered data and information through third parties.

TTUHSC EP recognizes that this may not be a complete list of the potential risks associated with the protection of covered data and information. Since technology growth is not static, new risks may occur periodically. Accordingly, the Information Technology Division of TTUHSC EP will actively participate and monitor advisory groups such as the Educause Security Institute, the Internet2 Security Working Group and SANS for identification of new risks.

TTUHSC EP Information Technology Division's current safeguards are reasonable and sufficient to provide security and confidentiality to covered data and information maintained by TTUHSC EP. Additionally, these safeguards protect against currently anticipated threats or hazards to the integrity of such information.

3. Information Security Plan Coordinators (16 CFR 314.4(a))

a. Coordinators

The Director of Payment Services, the Institutional Security Officer, the Director of Student Financial Aid, and the Chief Information Officer (collectively referred to hereinafter as the "Coordinators") are responsible for coordination and execution of this Plan. With consultation from the Office of General Counsel when necessary, the Coordinators are responsible for assessing the risks associated with unauthorized transfers of covered data and information and implementing procedures to minimize those risks to TTUHSC EP.

b. Correspondence and Inquiries

Correspondence and inquiries regarding this Plan should be directed to the Coordinators at:

Director of Payment Services
5001 El Paso Drive
El Paso, Texas 79905
915-215-4377

Director of Student Financial Aid
5001 El Paso Drive
El Paso, Texas 79905915-215-3025

Institutional Security Officer 5001 El Paso Drive El Paso, Texas 79905
915-215-4903

Chief Information Officer
5001 El Paso Drive El Paso, Texas 79905
915-215-4047

4. Design and Implementation of Safeguards Program (16 CFR 314.4(b)-(c))

a. Employee Management and Training

TTUHSC EP areas that are covered by this policy are Business Services, Texas Tech University System Office of Development (those offices located at TTUHSC EP), Information Technology, Registrar, Student Affairs (at all campuses) and Student Financial Aid and any other areas that work with covered data and information on a regular basis. References for potential new employees working in these areas shall be checked. During employee orientation, new employees in said areas will receive training on the importance of confidentiality of student records, student financial information, and other types of covered data and information. TTUHSC EP also will train current employees working in these areas on the importance of confidentiality of covered data and information. Training of new and current employees working in these areas will include controls

and procedures to prevent employees from providing confidential information to an unauthorized individual, including "pretext calling"[2] and how to properly dispose of documents that contain covered data and information. All new employees, whether or not they are in an area responsible for maintaining covered data and information, will receive general training in the proper use of computer information and passwords. Areas that maintain covered data and information will be responsible for maintaining records on training (names of employees receiving training and dates of training) for their respective employees. The Coordinators will review and update training materials when necessary.

Each area responsible for maintaining covered data and information is instructed to take steps to protect the information from destruction, loss, or damage due to environmental hazards, such as fire and water damage or technical failures. Faculty, employees, students and affiliates, prior to employment will complete a CONFIDENTIALITY AGREEMENT, as required by TTUHSC EP OP 52.09.

b. Physical Security

TTUHSC EP has addressed the physical security of covered data, and information shall be accessed only by those employees who have a business reason to know such information. For example, personal customer information, accounts, balances and transactional information are available only to TTUHSC EP employees with an appropriate business need for such information.

Loan files, account information, and other paper documents are kept in file cabinets, rooms, or vaults that are locked each night. Only authorized employees know combinations and the location of keys. Paper documents that contain covered data and information shall be shredded at time of disposal.

c. Information Systems

Access to covered data and information via TTUHSC EP's computer information system is limited to those employees who have a business reason to know such information. Each employee is assigned a user name and password. Databases containing personal covered data and information, including, but not limited to, accounts, balances, and transactional information, are available only to TTUHSC EP employees in appropriate departments and positions.

Static passwords used to authenticate User ID's must be changed every ninety (90) days and must meet the minimum password requirements set by Information Technology.

TTUHSC EP will take reasonable and appropriate steps consistent with current technological developments to secure all covered data and information and to safeguard the integrity of records in storage and transmission. Information Technology Division requires that all servers must be registered before being allowed through TTUHSC EP's firewall, thereby allowing Information Technology Division to verify that the system meets necessary security requirements as defined by Information Technology Division policies before covered data and information is accessed. These requirements include maintaining the operating system and applications, including application of appropriate patches and updates in a timely fashion. User and system passwords are also required to comply with the TTUHSC EP password requirements. In addition, an intrusion detection system has been implemented to detect and stop certain external threats, along with an Incident Response Policy for occasions where intrusions do occur.

When commercially reasonable, encryption technology will be utilized for both storage and transmission of covered data and information. All covered data and information will be maintained on servers that are

---

[2] *Pretext calling* occurs when an individual improperly obtains personal information of TTUHSC EP customers so as to be able to commit identity theft, 18 U.S.C. § 1028; § 523 of the GLBA (15 U.S.C. § 6828). It is accomplished by contacting the TTUHSC EP, posing as a customer or someone authorized to have the customer's information, and through the use of trickery and deceit, convincing an employee of the TTUHSC EP to release customer

identifying information behind TTUHSC EP's firewall. All firewall software and hardware maintained by Information Technology Division will be kept current. Information Technology Division has a number of policies and procedures in place to provide security to TTUHSC EP's information systems.

In order to preserve the confidentiality of privileged and/or sensitive information, email correspondences shall not contain Social Security numbers, student information, or any personal and/or confidential information. If any email correspondence contains such information, the email must be encrypted (see HSC OP 56.02), and it should also contain a disclaimer at the end of the email indicating that the information is confidential.

d. Management of System Failures

Information Technology Division has developed written plans and procedures to detect any actual or attempted attacks on TTUHSC EP systems and has an Incident Response Policy which outlines procedures for responding to an actual or attempted unauthorized access to covered data and information. This policy is available upon request from the Director of Network/Systems.

e. Reviews

Areas maintaining covered data and information (with assistance, if necessary, from the Coordinators, Office of Audit Services and/or Office of General Counsel) will be responsible for conducting annual reviews of their respective areas to assess the internal control structure and to verify that their areas comply are in compliance with requirements and applicable state and federal laws. Office of Audit Services may conduct reviews of areas maintaining covered data and information at any time and at the Office of Audit Services' discretion.

5. Selection of Appropriate Service Providers (16 CFR 314.4(d))

It may be necessary for service providers to access covered data and information and provide resources that TTUHSC EP determines not to provide on its own. In the process of choosing a service provider that will maintain or regularly access covered data and information, the evaluation process shall include the ability of the service provider to safeguard confidential financial information. In addition to the standard contract clauses, contracts with service providers shall include the following provisions:

- An explicit acknowledgement that the contract allows the service provider access to confidential information held or collected by TTUHSC EP;
- A specific definition or description of the confidential information being provided;
- A stipulation that the confidential information will be held in strict confidence and accessed only for the explicit business purpose of the contract;
- An assurance from the service provider that the provider will protect the confidential information it receives according to commercially acceptable standards and no less rigorously than it protects its own confidential information;
- A provision providing for the return or destruction of all confidential information received by the contract provider upon completion or termination of the contract;
- An agreement that any violation of the contract's confidentiality conditions may constitute a material breach of the contract and entitles TTUHSC EP to terminate the contract immediately without penalty; and
- A provision stating that the contract's confidentiality requirements shall survive termination.

6. Continuing Evaluation and Adjustment (16 CFR 314.4(e))

This Information Security Plan will be subject to periodic review and adjustment. The most frequent of these reviews will occur within Information Technology Division, where constantly changing technology and evolving risks mandate increased vigilance. Information Technology, as well as other relevant areas, will conduct an annual data and information security review. Continued administration of the development, implementation, and maintenance of the program will be the responsibility of the Coordinators who will assign specific responsibility for implementation and administration as appropriate. The Coordinators, in

consultation with the Office of General Counsel when necessary, will review the standards set forth in this policy and recommend updates and revisions as necessary. It may be necessary to adjust the plan to reflect changes in technology, the sensitivity of student/customer data and internal or external threats to information security.

7. Disciplinary Action

To enforce this Plan, TTUHSC EP may take appropriate disciplinary measures directed to TTUHSC EP employees, faculty, students or affiliates. These disciplinary measures include, but are not limited to, letters of reprimand, suspensions with or without pay, or termination.