



# **Handbook of Operating Procedures**

**Section:** 4.11.1  
Originally Approved: 09/16/2005  
Last Amended:  
Last Reviewed:  
Page: 1 of 4

---

## **PRIVACY AND SECURITY OF PERSONAL INFORMATION**

### **A. Purpose**

The purpose of this policy is to clarify The University of Texas-Pan American's commitment to maintaining the privacy and security of personal information for both students and non-students by identifying the general personal information security programs in place at the University.

### **B. General Personal Information Security Program**

#### 1. Requirements

The University safeguards against inappropriate disclosure and abuse of personal information that the University holds, as required by applicable laws and regulations which may include:

- [The Privacy Act of 1974](#)
- [Family Educational Rights and Privacy Act \(FERPA\)](#)
- [Gramm-Leach-Bliley Act \(GLBA\)](#)
- The University of Texas System [Business Procedures Memorandum 66 \(BPM 66\)](#)

#### 2. Basis

The University's general personal information security program includes:

- a. Identification and prioritization of personal information data elements subject to protection under state and federal law;
- b. Application, where applicable, of FERPA privacy standards and GLBA safeguarding standards to student and non-student records; and
- c. Application of medical privacy standards to campus clinical health records for both students and non-students.

#### 3. Prioritization of Personal Information Data Elements

- a. Highest Risk Personal Identifiers (HRPIS)



## ***Handbook of Operating Procedures***

**Section:** 4.11.1  
Originally Approved: 09/16/2005  
Last Amended:  
Last Reviewed:  
Page: 2 of 4

---

### **PRIVACY AND SECURITY OF PERSONAL INFORMATION**

Identifiers through which the personal information can be accessed, and identity theft crime may occur includes:

- Credit Card Numbers (CCNs)
- Social Security Numbers (SSNs)
- Drivers License Numbers (DLNs)
- Automatic Clearing House information (such as bank account numbers)
- Certificate/License Number
- Credit Reports/Histories
- Electronic Signatures
- Passwords
- PIN Numbers

Measures to be taken with respect to HRPIS include:

- 1) To the extent appropriate, minimizing the number of offices, computers, and databases on campus that collect and/or store HRPIS. Offices, individuals, or departments planning upon storing CCNs on servers or other computers or transmitting them over networks must have plans for securing those numbers approved by the Chief Information Security Officer (CISO) prior to beginning storing or transmitting the numbers.
- 2) Requiring submission of SSNs and DLNs only where required or authorized by law. Requiring submission of CCNs only for purposes of payment. (Note: This does not preclude the University's requesting that individuals provide these data elements in the ordinary course of its business, but the University may not refuse service based on a refusal to provide them except in cases required or authorized by law.)
- 3) Providing for the delivery of campus services in ways that do not **require** submission of SSNs or DLNs except where authorized or required by law.



## ***Handbook of Operating Procedures***

**Section:** 4.11.1  
Originally Approved: 09/16/2005  
Last Amended:  
Last Reviewed:  
Page: 3 of 4

---

### **PRIVACY AND SECURITY OF PERSONAL INFORMATION**

- 4) Providing all required notices to the individual of the purpose for collecting SSNs and DLNs when and where they are collected.
- 5) Controlling the use of SSNs and DLNs to be consistent with the use that has been disclosed to the individual or to other usage required by law or policy.
- 6) Avoiding disclosure of SSNs and DLNs except with written authorization of the individual involved or when required or permitted by law or policy.
- 7) Providing affected individuals with written notice upon discovery by the University of theft, accidental disclosures, or breaches of security that create a high risk of disclosure or compromise of protected information.
- 8) Entering into confidentiality and non-disclosure agreements, with third parties with whom the University shares HRPIS that hold the third party accountable for safeguarding HRPIS.
- 9) Applying the safeguarding measures described below in Subsection B.4.
- 10) Avoiding external disclosure except with written authorization of the individual involved or as may be required by law, policy, or legitimate University business.

The CISO shall develop and implement such additional rules and procedures to secure HRPIS as changing technologies and threats may require. In this policy, the term “credit card” includes debit and other transaction cards and instruments as may be deemed appropriate.

- b. Personally Identifiable Health Information. The University is not a covered entity for purposes of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or the HIPAA Privacy and Security regulations (42 CFR parts 160 and 164). The University shall therefore endeavor to avoid entering into any business relationship that would involve the collection, maintenance or use of information by the University that meets the definition of personally identifiable health information as described in 42 CFR 160.103. However, if the University enters into an agreement pursuant to 42 CFR 164.504(e) to act as the Business Associate of a covered entity that is subject to HIPAA, the University will take all steps necessary to comply with the requirements applicable to any personally identifiable health information that it collects, maintains or uses on behalf of the covered entity pursuant to the terms of the Business Associate agreement.



## **Handbook of Operating Procedures**

**Section:** 4.11.1  
Originally Approved: 09/16/2005  
Last Amended:  
Last Reviewed:  
Page: 4 of 4

---

### **PRIVACY AND SECURITY OF PERSONAL INFORMATION**

4. Safeguarding Measures for Personal Information subject to the Gramm-Leach-Bliley Act (GLBA)

Safeguarding measures as defined in [Part VII Federal Trade Commission 16 CFR Part 314, Standard for Safeguarding Customer Information](#), as required by the GLBA, 15 U.S.C. § 6801 et seq., should be applied for all personal information that is subject to the GLBA.

5. Safeguarding Personal Information

The University shall make tools and information available to members of its community to assist in applying appropriate measures.

These tools may include the following or such others may be developed or required from time to time:

- a. Departmental Personal Identifiable Information Risk Assessment and Security Plan
  - To be completed and identified measures implemented.
  - To be updated annually and identified changes implemented.
- b. Online access to general information and to sample text for disclosure notices
- c. Identification of University Social Security Number (SSN) Coordinator, HIPAA Coordinator, Chief Information Security Officer, and Records Manager, and other positions of responsibility as may be required or useful.
  - To aid in answering questions and learning approaches that have proven to be efficient and effective at the University.

The CISO may perform risk analysis, intrusion testing, and other testing, and take other appropriate actions related to analyzing, reviewing, or strengthening security measures applicable to the security of data referenced in this policy on the University's application systems, servers and networks.

#### **C. Review**

This policy shall be reviewed every three years or as laws and rules change by the Chief Information Officer.