TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER EL PASO

Operating Policy and Procedure

HSCEP OP: 77.21 **FERPA Breach Policy**

PURPOSE: The purpose of this Texas Tech University Health Sciences Center El Paso (TTUHSC El Paso) Operating Policy and Procedure (HSCEP OP) is to provide an institutional process to investigate and report, where required by state or federal law, suspected breaches and accidental disclosures of student information that is electronically or physically stored. Federally funded higher education institutions must protect student data from internal and external unauthorized disclosures under the Family Educational Rights and Privacy Act (FERPA), 34 Code of Federal Regulation Part 99.

REVIEW: This HSCEP OP will be reviewed by May 1 of each odd-numbered year (ONY) by the Vice President for Academic Affairs, Vice President for Information Technology, Assistant Vice President for Student Services and Student Engagement, and Vice President for Institutional Compliance, with recommendations for revisions submitted to the Office of General Counsel and the President or designee by June 15.

I. Definitions:

Student Personally Identifiable Information (PII) under FERPA: Student PII, under FERPA, generally refers to identifiable information that is maintained in education records and includes direct identifiers: a student's name or identification number, indirect identifiers, such as a student's date of birth, or other information which can directly or indirectly distinguish the identity of a student.

Breach of System Security: An incident in which student information and other PII that is sensitive, protected, or confidential, as provided by federal and state law, is inadvertently disclosed, stolen or copied, transmitted, viewed, or used by a person or entity unauthorized to engage in that action.

II. Breach Classification:

The severity of a breach that compromises student PII stored in an IT system or physical storage (i.e., printed records) and subject to unauthorized verbal disclosure, is classified according to the overall impact it had, or is expected to have, on TTUHSC El Paso. Throughout the investigation and response process, each breach is subject to re-classification, depending on the context of the incident and discoverable facts. Some breaches will not require a formalized investigation due to the low impact of the incident. The impact of a breach may be classified as low and inadvertent, moderate, or high, as follows:

A. Low Impact and Inadvertent Breaches are common, primarily accidental, unintentional disclosures of student PII to an unauthorized source and there is minimal chance of harm to the student.

B. Moderate Impact Breaches are the intentional and unauthorized acquisition of at least one student's PII. Such breaches may be subject to state and federal notification laws.

C. High Impact Breaches are the intentional unauthorized acquisitions of student PII that affect 250 or more individuals. Such breaches may be subject to state and federal notification laws.

III. Breach Investigation and Breach Response Team:

A. Obligation to report: If a business associate/contractor, faculty member, staff, or student suspects an inadvertent, unlawful and/or unauthorized breach of electronic system or digital system student PII, they are expected to report that concern to the Vice President for Information Technology or their designee as soon as possible, within 24 hours, by email at it-academics@ttuhsc.edu or phone at 915-215-4111. Suspected inadvertent, unlawful, and/or unauthorized breach of physically stored student PII by physical removal, copying, or verbal disclosure should be reported as soon as possible, within 24 hours, to the Registrar's Office at epregistrar@ttuhsc.edu or phone at 915-215-4370. The Vice President for Information Technology and the Registrar, or their designees, shall forward all breach reports to the chair of the Breach Response Team within 24 hours. TTUHSC El Paso will comply with all required state and federal breach notification laws.

B. Breach Response Team: The Breach Response Team shall be designated to investigate and determine the level of any student PII breach and TTUHSC El Paso's duty to provide breach notifications to individuals and government agencies under applicable federal and state notification laws. The specific and technical responses for moderate or high impact breaches will vary depending on the details of each incident.

1) The Breach Response Team shall be chaired by the Chief Information Officer (CIO), and shall be comprised of the following members: Information Security Officer (ISO), Vice President for Academic Affairs, Vice President for Institutional Compliance, Vice President for Institutional Advancement, Office of General Counsel, and Chief of Texas Tech El Paso Police Department, or their designees.

2) The duties of the Breach Response Team shall include:
   a. Determining how the student PII breach occurred
   b. Determining the level of the breach (low and inadvertent, moderate, high)
   c. Determining the number of students affected.

3) The Breach Response Team shall investigate potential PII breaches to determine if the incident resulted in a moderate or high impact breach of student PII. The Breach Response Team shall produce a report for each investigation that shall answer the following questions:
   a. On what date and in which department did the incident occurred?
   b. In what form was the student PII disclosed?
   c. What was the nature and extent of the breach: was the disclosure of student PII a low and inadvertent impact breach, a moderate impact breach, or a high impact breach?
   d. Who or what entity is responsible for the breach?
   e. If inadvertent, what were the circumstances and causes of the disclosure(s)/breach?
   f. What happened to the unauthorized accessed student PII?
   g. What additional controls are recommended to mitigate the damage and the potential for similar incidents in the future?

4) If the compromised PII is accessed through an IT system or program, then the incident report shall be retained by the Office of Information Technology (with copies retained by the Registrar's Office) for six years. Breach reports involving the unlawful accessing or disclosure of student PII not stored in an IT system or program shall be retained by the Registrar's Office for six years.

5) Low Impact and inadvertent incidents may not necessitate significant investigations; however, the chair of the Breach Response Team, or their designee, will provide a written, signed report describing their findings and their rational for labeling the breach as “Low Impact” to the Vice President for Institutional Compliance and the Vice President for Academic Affairs or their designees. Affected students shall be notified of the incident by the Vice President for Institutional Compliance and/or the Vice President for Academic Affairs or their designees, and be informed of steps the institution will take to better track student PII.

6) If a Breach Response Team investigation determines that engagement with a law enforcement agency is required or advisable, local law enforcement agencies or the FBI shall be notified as soon as possible. If a law enforcement agency requests a delay in required breach notifications, the request must be documented in writing by the requesting law enforcement agency and provided to TTUHSC El Paso. The delay request must be provided to the affected individuals as part of the notification process.

7) The Breach Response Team shall review TTUHSC El Paso IT Policies and Procedures: OP 56.01 – 1.4.7, Incident Management; OP 56.50, Incident Response; OP 56.50, Data Security (SE) and; OP 56.90, IT Event Management/Response. These four OPs, with guidance from the Office of Information Technology, shall inform the Breach Response Team of the technical processes required to secure the affected computer systems and data after a student PII breach is confirmed.

8) The Breach Response Team shall prepare a report to be presented to the President by the Vice President for Information Technology and/or the Vice President for Academic Affairs. In addition, the Breach Response Team’s report shall be disclosed to the Office of General Counsel prior to any notifications being sent to the affected individuals as required under section II above.

9) Should a breach require notification to the public and the media, those notifications will be managed by the Vice President for Institutional Advancement, or their designee, in consultation with the Vice President for Institutional Compliance and the Office of General Counsel.

10) Reports to government agencies shall be made by the Vice President for Institutional Compliance in consultation with the Office of the President, the Office of Institutional Research and Effectiveness, and the Office of General Counsel. The Breach Response Team will provide a written, signed report detailing the investigation and all findings to the Vice President for Institutional Compliance.