TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER EL PASO

Operating Policy and Procedure

HSCEP OP: Data Minimization & Retention (DM)

Policy Statement:

TTUHSC El Paso shall implement data minimization and retention controls applicable to the collection, use, and retention of Personally Identifiable Information (PII) in order to ensure PII is relevant and necessary for the specified purpose for which it was originally collected.

Reason for Policy:

The purpose of the Data Accountability, Audit & Risk Management (AR) policy is to enhance public confidence through effective governance, monitoring, risk management, and assessments to demonstrate that TTUHSC El Paso is complying with applicable privacy and security protection requirements and minimizing overall risk.

Entities Affected by this Policy are any and all users of Information Resources at TTUHSC El Paso.

What is covered in this Policy?

The overall policy addresses the Institutional stance as it applies to data minimization & retention minimization of PII, Data Retention & Disposal, Data Collection, Sensitive Data Storage, Data Masking, and minimization of PII used in testing, training & research.

It is the stance of TTUHSC El Paso to ensure that there are safeguards in place aligned with NIST 800-53 and TAC 202 to ensure the protection, integrity, and confidentiality of information resources at TTUHSC El Paso

Who Should Read this Policy?

All individuals accessing, storing, viewing any TTUHSC El Paso information resources.

What happens if I violate this policy?

Any person(s) violating TTUHSC El Paso Information Technology policies are subject to penalty under federal, state, and local legislation. Disciplinary actions are further outlined in HSCEP OP 56.50, Sanctions Policy.

DM-01: Minimization of Personally Identifiable Information (PII)
TTUHSC El Paso;

- Identifies the minimum PII elements (e.g., name, address, date of birth) that are relevant and necessary to accomplish the purpose of collection; and
- Limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent.

Where feasible and within the limits of technology, data/process owners are responsible for locating and removing/redacting unnecessary PII through the use of anonymization and de-identification techniques.

DM-02: Data Retention & Disposal
TTUHSC El Paso:

- Retains PII for an organization-defined time period to fulfill the purpose(s) identified in the notice or as required by law;

- Disposes of destroys, erases, and/or anonymizes the PII, regardless of the method of storage; and
- Uses organization-defined techniques or methods to ensure secure deletion or destruction of PII (including originals, copies, and archived records).

Data/process owners are required to:

- Define retention periods for PII; and
- Dispose of, destroy, erase, and/or anonymizes the PII once the PII is no longer necessary for business purposes.

Data Retention & Disposal includes:

Data Collection
Data/process owners are required to implement limitations on the collection, use, and disclosure of personal information.

Sensitive Data Storage
TTUHSC El Paso limits storing sensitive data to explicit business requirements.3 Personally Identifiable Information (PII) is prohibited from being stored for any longer than the legitimate business need exists to retain the data.

Data Masking
TTUHSC El Paso applies data masking to sensitive information that is displayed or printed. Sensitive information that is displayed or printed is required to be masked. This includes but is not limited to:

- Financial account numbers;
- Social Security Numbers (SSN); and
- Credit or debit Primary Account Numbers (PANs) (no more than the first six and the last four digits allowed).

DM-03: Minimization of PII Used In Testing, Training, & Research
TTUHSC El Paso:

- Develops policies and procedures for the use of PII for testing, training, and research; and
- Implements controls to protect PII used for testing, training, and research.

The use of PII is prohibited for research, testing or training.

All other IT Policies can be found at https://ttuhscep.edu/it/policies/

TTUHSCEP Sanctions Policy 56.50
UK Data Protection Act of 1998 (Chapter 20-Schedule 1-Part1-Principle3)
UK Data Protection Act of 1998 (Chapter 29-Schedule1-Part1-Principle 5)
PCI DSS 3.2 & 3.2.1-3.2.3
PDI DSS 3.3
TAC §202.74, §202.75

Revised May 2018