TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER

Operating Policy and Procedure

HSC OP: 56.04 Data Security and Privacy

PURPOSE: This policy applies to TTUHSC data generated by or for, owned by, or otherwise in the possession of TTUHSC and that is related to TTUHSC activities. The purpose of this policy is to ensure that such data is categorized, properly handled, and protected. Data is protected in accordance with its regulatory status and the potential impact to Texas Tech University Health Sciences Center (TTUHSC) if the data is compromised through a loss of confidentiality, integrity, or availability.

Security and privacy categorization ensures that data being processed, stored, or transmitted is properly protected. The data classification scheme summarized in this policy is intended to inform the implementation of the safeguards, precautions, and handling requirements necessary to prevent accidental data disclosure.

The Information Security Officer (ISO) in consultation with the TTUHSC Office of Institutional Compliance will recommend, in accordance with Texas Administrative Code, Title 1, Chapter 202 (1 TAC 202), appropriate standards, guidelines, and training regarding Data Security and Privacy to the Information Resources Manager (IRM) for approval.

REVIEW: This IT Policy will be reviewed annually in August by the IT Executive Management Team and the Office of Institutional Compliance.

TABLE OF CONTENTS

SCOPE

This policy applies to

a. TTUHSC data. Information generated by or for, owned by, or otherwise in the possession of TTUHSC that is related to TTUHSC's activities. TTUHSC Information may exist in any format (e.g

electronic, paper) and include, but not be limited to, all academic, administrative, clinical, and research data,

b. TTUHSC Information Systems that support the business of the institution by storing or transmitting TTUHSC Information, and;

c. TTUHSC employees, students, contactors, volunteers, and any other users authorized to access TTUHSC Information and information systems. In addition, third parties may be subject to this policy through contractual obligations with TTUHSC.

POLICY

1. Data Security and Privacy Principles

Data, regardless of the form or format, which is created or used in support of TTUHSC business activities, is owned by TTUHSC. TTUHSC-owned information is an asset and must be protected from its creation, through its useful life, to its timely and authorized disposal. TTUHSC-owned Information should be maintained in a secure, accurate, and reliable manner and be readily available for authorized use.

Proper data security must

a. be based on the value and associated risks of managing the Information,

b. meet the appropriate levels of protection as required by state and federal laws,

c. account for ethical, proprietary, and privacy considerations,

d. recognize that data classifications are contextual, subject to change and should therefore be periodically reviewed, and

e. follow approved storage guidelines as described in the TTUHSC IT Data Storage Standard.

2. Management Roles for Data Security and Privacy

The ISO is responsible for managing the planning and tool implementation used to secure TTUHSC data. The ISO develops, maintains, and disseminates information security policies, procedures, standards, and guidelines regarding data security.

The following data security management roles should be established for each TTUHSC business unit or department that stores, processes, or transmits data:

a. Data Owner: Individuals, often department heads or similar, who have direct responsibility for the information that resides in and/or is primarily used within their department. The owner is accountable for classifying and reviewing the information according to the designations defined in the Security Categorization of Information and Information System Impact Standard, and for ensuring that policies, standards, and internal controls established by the ISO and the Office of Institutional Compliance are executed in a reliable and consistent manner.

b. Data Custodian: Individuals who implement the policies, standards, and internal controls established by the ISO and the Office of Institutional Compliance and as required to do so by the Data Owner. The data custodian ensures that users are trained and that they are monitored for compliance.

c. Data User: Authorized individuals who access information at any point during its lifecycle. Anyone within TTUHSC can be a data user. Users are responsible for identification, labeling, and proper disposal of information in accordance with relevant TTUHSC policies.

3. Data Classification Principals and Schema

TTUHSC-owned data is classified both in terms of regulated privacy standards and based on its sensitivity, legal status, and retention requirements, as well as according to the type of access required by TTUHSC users.[1] TTUHSC-owned information can be classified as follows:

a. Privacy Compliance-based Definitions

(1) Personally Identifiable Information (PII)

Information or data about an individual that may be used to distinguish or track the individual's identity or that may be linked to the individual, including, but not limited to, the individual's name, social security number, date of birth, location of birth, mother's maiden name, biometric records, medical information, educational information, financial information, and employment information.

(2) Protected Health Information (PHI)

PHI is defined in 45 CFR § 160.103 and in TTUHSC HIPAA Privacy Policy HIPAA 1.1 Glossary of HIPAA Terms, as individually identifiable health information created, maintained or transmitted by TTUHSC or any other covered entity in any form or medium, including information transmitted orally, or in written or electronic form.

b. Data Security-based Definitions (in order of security required from lowest to highest)

(1) Public Data

The Public label is used for Information such as published reports, press releases, and Information published to the university's public website. Such public-related materials require no authentication and are freely distributable by all university personnel and are available for public access without requiring intervention by TTUHSC employees.

(2) Sensitive Data

The Sensitive label is used for Information that may be subject to disclosure under the Texas Public Information Act, but should be vetted/verified before it is released. While these records and information are considered "Public" under the Texas Public Information Act, they should still be afforded a higher level of protection to ensure Confidential Data (e.g., net salary information) is not comingled. Sensitive Data may include Confidential Data that has not yet been classified as such. Examples of Sensitive Data may include but are not limited to:

- Operational information
- Personnel records
- Information security procedures
- Unpublished research information
- Internal communications
- Gross salary information

(3) Confidential Data

The Confidential label is used to identify information that TTUHSC collects and maintains that is protected from disclosure either through a codified exception to the Public Information Act, Texas Government Code Ch. 552 or through the opinions or decisions of the Attorney General's Public Information office. Such information may also be subject to

[1] For a more thorough discussion of data classification and risk impact, see the Security Categorization of Information and Information System Impact Standard.

breach notification requirements under Texas law. Examples of Confidential Information may include but are not limited to:

- Attorney-client communications
- Computer Vulnerability Reports
- Protected draft communications
- Net salary information

(4) Regulated Data

The Regulated label is used to identify Information that TTUHSC collects and maintains that is controlled by state or federal law, and other constitutional, statutory, judicial, and legal agreements and requirements. Authorized disclosure or release of Regulated Data is governed by applicable statutes.

Examples of Regulated Data may include but are not limited to Compliance-based Personally Identifiable Information (PII) and Protected Health Information (PHI) as defined in the following:

- Patient Protected Health Information as defined by HIPAA 45 CFR § 160.103
- Education records as defined by FERPA 34 CFR § 99.3
- Cardholder Data governed by PCI DSS
- Data that meets the definition of SPI under the Texas Business and Commerce Code 521.002(a)(1) and 521.002(a)(2)
- Controlled Unclassified Information as defined by Federal Executive Order 13556

4. Data Life Cycle

a. Data Creation

Data Owners who oversee data creation as part of their authorized duties or receive legitimate data from an outside source must classify and protect the data in accordance with this policy. Data Owners should consult with TTUHSC General Counsel, TTUHSC Office of Institutional Compliance or TTUHSC IT GRC regarding any questions on the proper classification or disclosure of data. Data Owners, Custodians, and Users are prohibited from improperly receiving or sharing data that is protected under applicable copyright and trademark laws.

b. Document Retention and Disposal

Documents or media that contain Sensitive Information or higher must be retained, disposed of, or destroyed in a secure manner as outlined in TTUHSC OP 10.09 Records Retention and its accompanying schedule. Documents that contain Protected Health Information must be disposed of appropriately in accordance with TTUHSC HIPAA Privacy Policy 2.12 Retention and Destruction of PHI.

c. Lifecycle Changes

The classification of a data item can change over the course of its lifecycle. For example, data may start as Confidential Data during its draft phase and may become Public Data once it is publicly available. The Information Owner or their designee remains responsible for the proper classification of data over the course of its lifecycle.

5. Data Encryption

a. All electronically stored or transmitted data classified as Sensitive Data or higher, including information identified as PII or PHI, must be encrypted while it is either transmitted across networks, or stored or transported on approved computing devices, using an approved Cryptographic Algorithm.

b. The Information System Owner must contact TTUHSC IT to obtain approved encryption tools. Minimum requirements for TTUHSC data encryption can be found in the Encryption Standard.

c. All Cryptographic Keys (except for Public Asymmetric Keys) as well as the resources used to generate and store Cryptographic Keys themselves shall be considered Confidential Data. Public Asymmetric Keys may be considered public data.

d. Exportation of cryptographic technologies outside of the United States is restricted by federal regulations. See the Foreign Travel Standard for requirements related to TTUHSC travel and encrypted devices.

e. All data classified as Sensitive Data or higher, including PII/PHI that is sent over email, must follow the email encryption procedure as described in TTUHSC IT Policy 56.22 Email.

f. All data classified as Sensitive Data or higher, including PII/PHI, must be digitally stored as described in the Data Storage Standard .

6. Approval for Release of TTUHSC-Owned Data

a. Data identified as Sensitive, Confidential, or Regulated shall not be released outside of TTUHSC without prior approval of the TTUHSC General Counsel.

b. Regulated Data (including PII/PHI) may only be released as authorized by the applicable regulations.

7. Violations

Any violation of this policy may result in disciplinary action, up to and including fines to both the individual and the institution, investigation by the TTUHSC Institutional Privacy Officer and or/ Information Security office and may result in termination of employment. TTUHSC reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity.

a. Disciplinary Repercussions

Misuse of TTUHSC Information or Information Systems is a violation of the policies contained herein and can result in disciplinary action in accordance with, but not limited to, TTUS Regulations 07.07 Employee Conduct, Coaching, Corrective Action, and Termination and TTUHSC OP 77.05 Suspension and Retention, TTUHSC HIPAA Privacy Policy 1.10 HIPAA Sanctions as well as the Student Handbook.

Related Statutes, Policies, and Requirements

- Computer Fraud and Abuse Act
- Computer Security Act
- Copyright Act of 1976
- Family Education Rights and Privacy Act
- Federal Executive Order 13556, Controlled Unclassified Information
- Federal Information Processing Standards (FIPS) Publication 199
- Federal Information Security Management Act (FISMA)

- Gramm-Leach-Bliley Act
- International Standards Organization 27001:2005
- State of Texas Executive Order RP58
- Texas Business and Commerce Code, Chapters 48 and 521
- Texas Government Code, Chapters 441 and 2054
- Texas Penal Code, Title 7, Chapter 33 and 33A
- Uniform Trade Secrets Act

Digital Millennium Copyright Act
Digital Millennium Copyright Act of 1998

Health Insurance Portability and Accountability Act of 1996
HIPAA, Title 45, Subchapter C, Part 164

Payment Card Industry (PCI) Data Security Standard (DSS)
PCI-DSS: 12.3 Acceptable Usage

Texas Administrative Code
TAC 202, Subchapter C, 70-76

Texas Public Information Act
Texas Public Information Act

Texas Security Control Standards Catalog
Texas DIR Security Control Standards Catalog

Texas Government Code
Texas Government Code Chapter 552

TTUHSC IT Areas of Responsibility
Information and Information System Roles and Responsibilities

Approval and Ownership

Approved By	Vince Fell
Title	Vice President for Information Technology, CIO
Approval Date	12/15/2023
Owner(s)	IT Executive Management Team

Revision History

Version	Description	Date Reviewed	Date Submitted for Publishing	Reviewer(s)
1.0	Initial Version	05/20/2023	12/18/2023	Office of Institutional Compliance, ISO, IT Executive Management
1.1	Annual Review	09/10/2024		Office of Institutional Compliance, ISO, IT GRC
1.2	Annual Review			Office of Institutional Compliance, ISO, IT Executive Management