5.8.22 Data Protection

Chapter 5 - Information Management	Original Effective Date: October 2004
Section: 5.8 Information Security	Date Last Reviewed: October 2022
Responsible Entity: Chief Information Security Officer	Date Last Revised: October 2022

I. Purpose

The UT Health San Antonio Policies, Standards and Procedures must describe and require steps to protect University data using appropriate administrative, physical and technical controls in accordance with the Information Security Program, Institutional Handbook of Operating Policy (IHOP) policy 5.8.21 (*Data Classification*), UT System Policy 165 (*Information Resources Use and Security*), and its associated Standards, and any federal or state law and regulation that may apply to the data's classification.

II. Scope

This policy applies to all faculty, staff, students, residents, healthcare providers, researchers, contractors, or any other third party entities who have direct or indirect access to data created, held or maintained by any UT Health San Antonio controlled affiliate, including, but not limited to its clinics, hospitals, and research operations.

III. Policy

A. Password and Encryption Protections

1. All high-risk desktop computers, laptop computers and mobile devices, including but not limited to, smartphones and tablet computers, which are owned, leased, or controlled by UT Health San Antonio must be encrypted using methods approved by the chief information security officer. Access to these devices must be password protected in compliance with UT Health San Antonio policy.
2. USB and similar removed storage devices owned, leased, or controlled by UT Health San Antonio must be encrypted before confidential data is stored on the device.
3. All personally owned computing devices, mobile devices, USB storage devices or similar devices must be password protected and encrypted using methods approved by the chief information security officer if they contain any of the following types of data:

a. information classified as "Confidential";

b. federal, state, university or privately sponsored research that requires confidentiality or is deemed sensitive by the funding entity; or

c. any other information that has been deemed by UT Health San Antonio as essential to its operations to the extent that its integrity and security should be maintained at all times.

B. **Assured Access to Encrypted Data**

1. For all computing devices owned, leased, or controlled by the UT Health San Antonio, standards and/or procedures shall be defined and documented to ensure accessibility of encrypted data in the event that an encryption key becomes corrupted or unavailable.

2. For personally owned devices protected by provisions described in this and other UT Health San Antonio policy, the device owner is responsible for ensuring that encrypted data is backed up to UT Health San Antonio owned or sanctioned storage.

C. **Data in Transit**

UT Health San Antonio shall adopt and document policies, standards, and/or procedures and implement appropriate administrative, physical, and technical safeguards necessary to adequately protect the security of data during transport and electronic transmissions. Each of the following controls shall be addressed:

1. Prior to disposal or repurposing storage media, original records subject to retention requirements must be copied to an alternative storage device. Original records must be accessible and retrievable for mandated retention periods, as documented in the institution's "Record Retention Schedule". The alternative data device and all other removable media must be protected commensurate with the data stored on them.

2. Information Resource Owners must remove all data contained on storage media prior to transferring it to the UT Health San Antonio warehouse for disposal or repurposing. Prior to disposal of data storage media, the Information Resource Owner must certify that no data remains on the media or device. For common rotating magnetic media (hard drives), the departmental Technical Support Representative (TSR) is authorized to use software designated by the chief information security officer that will destroy all data on the drive.

3. Prior to repurposing a storage device or media that previously contained "Confidential" or "Confidential/High Risk" information, the data on the media must be completely destroyed using a process approved by the chief information security officer.

D. **Storage and Transport of Electronic Media**

Information Resource Owners, in coordination with the chief information security officer, shall adopt and document physical and technical controls for securing storage devices and removable media that contain Confidential data. These Standards and Procedures should include, but are not limited to, movement of the media, access to the media, its storage, and its transfer to other parties.

E. **Patient Data Governance**

1. Requests for acquisition, access, use, external release and/or destruction of Protected Health Information (PHI) must be submitted to the Patient Data Governance Sub-committee for consideration and decision. These requests must meet the following criteria:
    a. data acquisition, access, use or release that will be outside of Treatment, Payment or Operations (TPO) or Health Insurance Portability and Accountability (HIPAA) Authorization;
    b. data acquired from, stored on or released to servers outside the UT Health San Antonio network. Unless covered by HIPAA Authorization, data acquired from, stored on or released to servers outside the University network require a Business Associate Agreement (BAA) or Data Use Agreement (DUA);
    c. the data does not meet the definition of TPO and has been classified as or received a non-research/non-human subjects research determination from the UT Health Institutional Review Board;
    d. epic access for non-TPO purposes and otherwise not covered by a HIPAA Authorization, e.g., for chart review, or slicer-dicer access;
    e. data acquisition, access, use, or release requests involving individuals without an official UT Health San Antonio affiliation, i.e., individuals other than UTHSA students, trainees, employees, and faculty; or
    f. data acquisition, access, use, or release requests referred to the Patient Data Governance Committee by a Department Chair or their designee.
2. Previously approved requests require re-review if the following occur:
    a. There is a change in access, use or release of one or more of the HIPAA 18 identifiers or information such as free text fields, narrative text or images of free text fields or narrative text that may contain information that could indirectly identify an individual;
    b. Addition of a new data source (acquisition or use of a new data source);
    c. Addition of a new external data release;
    d. Extension of the project period documented on the approved Data Acquisition, Access, Use and Release (DAUR) Request Form; or
    e. Changes, beyond those administrative in nature, in organizational agreements such as contracts, DUAs, BAAs or MTAs covering the data.

3. An internal Data Use Agreement (iDUA) is required by the data requestor at the time of the request for patient-level data acknowledging their understanding of their responsibilities under HIPAA (regardless if the data is classified as PHI or is de-identified patient-level data), including, but not limited to:
    a. Control access to the data according to UT Health San Antonio policy;
    b. Refrain from and take reasonable actions to prevent unauthorized disclosure of data;
    c. Refrain from and take reasonable actions to prevent use of data for purposes other than those approved by the IRB, Privacy Board or data governance process;
    d. Maintain data on the UT Health San Antonio network unless a project or services contract specifies further release;
    e. Encrypt data at rest and in transit according to UT Health San Antonio policy;
    f. Refrain from linking received data with other data unless approved by the IRB, Privacy Board or data governance process; and
    g. Refrain from contacting patients unless patient contact is approved by the IRB, Privacy Board or data governance process.

IV. Definitions

When used in this document with initial capital letter(s), the following words have the meaning set forth below unless a different meaning is required by context.

Confidential Data – data that is exempt from disclosure under applicable State law, including the Texas Public Information Act, and Federal laws. Data or information meeting these criteria are designated with the classification of "Confidential" within the U. T. System Data Classification Standard. [*as defined by UT System policy 165*]

Data – elemental units, regardless of form or media, which are combined to create information used to support research, teaching, patient care, and other University business processes. Data may include but are not limited to written, electronic video, and audio records, photographs, negatives, etc. [*as defined by UT System policy 165*]

HIPAA– Health Insurance Portability and Accountability Act (HIPAA) as specifically set forth in Title II, Subtitle F of the Health Insurance Portability and Accountability Act of 1996 as the Administrative Simplification provisions and the regulations adopted by the U.S. Department of Health and Human Services (HHS) to implement HIPAA which give HHS the authority to establish standards and requirements for the electronic transfer of health care information, and for the privacy and security of PHI.

Information Resources – any and all computer printouts, online display devices, mass storage media, and all computer-related activities involving any device capable of

receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting data including, but not limited to, mainframes, servers, Network Infrastructure, personal computers, notebook computers, hand-held computers, pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and Data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information. [*as defined by UT System policy 165*]

Information Resource Owner – the manager or agent responsible for the business function that is supported by the Information Resource or the individual upon whom responsibility rests for carrying out the program that uses the resources. The Owner is responsible for establishing the controls that provide the security and authorizing access to the Information Resource. The Owner of a collection of information is the person responsible for the business results of that system or the business use of the information. Where appropriate, ownership may be shared. [*as defined by UT System policy 165*]

Protected Health Information (PHI) – individually identifiable health information that is transmitted or maintained in any medium or form that is subject to HIPAA. PHI excludes individually identifiable health information in education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended; in records described at 20 U.S.C. §1232g(a)(4)(B)(iv) (student treatment records excepted from FERPA); and in employment records held by a covered entity in its role as an employer.

V. Related References

Institutional Handbook of Operating Policies (IHOP)
2.2.1 Records and Information Management and Retention
5.8.21 Data Classification

University of Texas System (UTS) Policies
UTS165 Information Resources Use and Security Policy, Standard 11: Safeguarding Data

Federal Law & Statute
HIPAA Security Rule 164.312(a)(2)(iv)
HIPAA Security Rule 164.312(e)(2)(ii)

VI. Review and Approval History

A. The approving authority of this policy is the University Executive Committee.

B. The review frequency cycle is set for three years following the last review date, a time period that is not mandated by regulatory, accreditation, or other authority.

Effective Date	Action Taken	Approved By	Date Approved
10/2004	Policy Origination		
01/2021	Policy Revision/technical edit		
10/2022	Policy Review/revision	Executive Committee	10/12/22