5.8.4 Access Management

Chapter 5 - Information Management	Original Effective Date: June 2002
Section: 5.8 Information Security	Date Last Reviewed: October 2022
Responsible Entity: Chief Information Security Officer	Date Last Revised: October 2022

I. Purpose

The purpose of this policy is to establish standards regarding the use, access and safeguarding of UT Health San Antonio Information Resources.

II. Scope

This policy applies to all current and former faculty, staff, students, residents, healthcare providers, researchers, contractors, or any other third party entities who have direct or indirect access to Information Resources 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

The UT Health San Antonio shall adopt access management processes to ensure that access to Information Resources is restricted to authorized users with minimal access rights necessary to perform their role and responsibilities.

Appropriate security measures shall be implemented to ensure the protection of all UT Health San Antonio Information Resources and Data with respect to privacy, unauthorized disclosure, unauthorized modification, denial of service and unauthorized access.

All UT Health San Antonio schools, offices and departments that create and manage access accounts for networks, servers or applications must manage the accounts in accordance with defined processes in compliance with this policy and the requirements of the UT System Identity Management Federation Member Operating Practices (MOP).

A. Access Controls

All non-public UT Health San Antonio Information Resources must be accessed through an access control system that allows users to be individually identified and authenticated. An access management process must incorporate procedures for:

1. assigning a unique identifier for each applicant, student, employee, insured dependent, research subject patient, alumnus, donor, third-party vendor, contractor, and other individuals, as applicable, at the earliest possible point of contact between the individual and the institution;
2. assigning a Custodian for each Information Resource or Data element responsible for:
    a. defining security profiles, access entitlements for group and role membership; and
    b. account provisioning, monitoring, and review;
3. enforcing password strength (i.e., complexity) that minimally conforms to the UT Health San Antonio password standards;
4. where possible, automatic log-off or password protected screen locking should be used to prevent unauthorized persons from accessing an unattended system that is logged in with an authorized account;
5. creating uniquely identifiable accounts for all users; this includes accounts created for use by third parties and contractors;
6. disabling all generic and default accounts;
7. disabling accounts immediately upon notification of termination of employment or the third-party or contractor agreement;
    a. Temporary account access for inactive full time or part time UT Health San Antonio faculty or staff must be:
        i. approved by the Information Resource Owner and chief information security officer (CISO).;
        ii. configured minimally based on risk and least privilege;
        iii. enabled for a period not to exceed 180 days; and
        iv. comply with access controls defined by this policy and associated standards and procedures, all other UT Health San Antonio Institutional Handbook of Operating Policies (IHOP) and UT System, state, federal policies, and regulations.
    b. Delegation of access to an Information Resource account assigned to a terminated UT Health San Antonio faculty or staff must be:
        i. approved by the Information Resource Owner; and
        ii. configured minimally based on risk and least privilege.
8. reviewing, removing and/or disabling accounts at least every 180 days, or more often if warranted by risk, to reflect current user needs or changes of user role or employment status;

9. immediately disabling or de-activating an account when its password is assessed as potentially compromised or suspicious activity is associated with the use of the account;
10. expiring passwords or disabling accounts based on risk (e.g., termination with cause) and a period of inactivity not to exceed 180 continuous days; and
11. managing access from wired and wireless devices, and from remote locations.

B. Passwords

Policies, standards, and procedures defining passwords to access Information Resources shall be adopted with processes for:

1. ensuring user identity when issuing or resetting a password;
2. establishing and enforcing password strength;
3. changing passwords;
4. managing security tokens when applicable;
5. securing unattended computing devices from unauthorized access by implementing mechanisms to prevent password guessing (e.g., lockout after multiple login attempts) and to block;
6. access to idle sessions (e.g., a password protected locking screen saver, session time-outs); and
7. ensuring that passwords are only accessed by or visible to the authenticating user, device, or system.

Unless otherwise allowed by policy, users must not share passwords or similar information, or devices used for identification and authorization purposes.

C. Shared Accounts

In some cases, an application or business need will require that an account be accessible for use by multiple users. In these cases, a shared account can be created. Shared accounts must be approved by the CISO with a single user designated as the Primary Account Holder.

1. The Primary Account Holder is responsible for maintenance of the account including:
    a. granting and revoking other users access to the account;
    b. changing the account password when users with knowledge of the account ID and password terminate, transfer roles or otherwise no longer need access to the Information Resource and in compliance with the institution’s policies and standards;
    c. tracking user access; and

d. reporting problems and security incidents to the CISO.

2. If the Primary Account Holder's job function or status changes and cannot continue to be responsible for the account, it must be reestablished with a new Primary Account Holder designated. In most cases, group accounts will only be approved in situations where technological limitations of an application require group access to a single account.

D. Remote and Wireless Access

Remote and wireless access to UT Health San Antonio network infrastructure must be managed to preserve the integrity, availability, and confidentiality of the institution's information. Remote and wireless access Standards and Procedures must:

1. establish and communicate to users the role and conditions under which remote or wireless access to Information Resources containing confidential data is permitted;
2. require the use of secure and encrypted connections when accessing Information Resources containing confidential data across the Internet, or across open segments of the institution's network or wireless network (e.g., use of VPN for access, SFTP for transfers, encrypted wireless); and
3. require monitoring for identifying and disabling of unauthorized (i.e., rogue) wireless access points.

E. Access to Network Infrastructure

Through appropriate use of administrative, physical and technical controls the Department of Infrastructure and Security Engineering is required to establish processes for approval of all network hardware connected to the UT Health San Antonio network and the methods and requirements for attachment, including any non-UT Health San Antonio owned computer systems or devices, to ensure that such access does not compromise the operations and reliability of the network or compromise the integrity or use of information contained within the network.

F. Data Access Control

All Information Resource Owners and Custodians must control and monitor access to data within their scope of responsibility based on data sensitivity and risk, and through use of appropriate administrative, physical, and technical safeguards including the following:

1. Information Resource Owners and Custodians must limit access to records containing confidential data to those employees who need access for the performance of the employees' job responsibilities. An employee may not access confidential data if it is not necessary and relevant to the employee's job function;

2. Information Resource Owners and Custodians must monitor access to records containing confidential data using appropriate measures as determined by applicable policies, standards, procedures, and regulatory requirements;
3. Information Resource Owners and Custodians must establish log capture and review processes based on risk and applicable policies, standards, procedures, and regulatory requirements. Such processes must define:
    a. the data elements to be captures in logs;
    b. the time interval for custodial review of the logs; and
    c. the appropriate retention period for logs.
4. employees may not disclose confidential date to unauthorized persons, institutions, vendors, or organizations except:
    a. as required or permitted by law, and, if required, with the consent of the Information Resource Owner;
    b. where the third-party is the agent or contractor for UT Health San Antonio and the safeguards described in institutional policy are in place to prevent unauthorized distribution; or
    c. as approved by UT Health San Antonio Legal or Compliance Office or UT System Office of General Counsel.

G. Access for Third Parties
1. Third parties acting as an agent of or otherwise on behalf of UT Health San Antonio must execute a written agreement that specifies:
    a. the data and systems authorized to be accessed;
    b. the circumstances under and purposes for which the data may be used; and
    c. that the final disposition of all University data must conform to and comply with UT Health San Antonio policies and standards, including HOP Policy 5.8.18, Third-Party Management of Information Resources.
2. Access to information resources by a third-party shall be:
    a. approved by the Information Resource Owner, Custodian and CISO;
    b. enabled for a period that minimally meets the objectives of the data and systems authorization agreement between UT Health San Antonio and the third-party and is not to exceed 180 days. Continuous access by third parties must be requested by the Information Resource Owner or Custodian every 180 days; and
    c. comply with access controls defined by this policy and associated standards and procedures, all other UT Health San Antonio Institutional Handbook of Operating Policies (IHOP) and UT System, state and federal policies and regulations.

If UT Health San Antonio determines that its provision of data or access to the institution's computing environment or network infrastructure to a third-party will result in significant risk to the confidentiality, integrity or availability of such data, computing environment or network infrastructure, the agreement between UT Health San Antonio and third-party must specify terms and conditions including appropriate administrative, physical and technical safeguards for protecting the data, computing environment and network infrastructure.

H. Access to Patient Data

1. Access to Protected Health Information (PHI) is restricted to the minimum amount of data necessary for performing an individual's job responsibilities, including using patient data to address a research question.
2. UT Health San Antonio maintains multiple data sources with diverse mechanisms for data access. To meet the principle of least privilege, entitled access rights to these data sources shall be configured by default as:
    a. Read access to Epic Clarity and other source system tables granted to Health IT and Clinical Research Informatics (CRI) professionals providing institutional support for UT Health San Antonio healthcare, treatment, payment and operations (TPO) and research.
    b. Read access to Epic Caboodle (UT Health San Antonio data only) through from-based queries granted to UT Health San Antonio Physicians for healthcare TPO, including the ability to query and view aggregate data for the provider's patients.
    c. Read access to custom subsets of warehouse data in relational data mart tables.

I. Self Service Access to De-identified Data

All UT Health San Antonio faculty and research staff are offered access to de-identified data in a self-service manner through the TriNetX, Accrual to Clinical Trials (ACT) and i2b2 software platforms.

J. Clinical Specialty and Research Group Data Marts and Registries

Data marts for TPO use require construction approval by the department chair and institutional privacy officer. Individual access authorization to data marts for TPOI use is authorized by the department chair. Access to data marts for TPO use requires attestation every 6 months of continued TPO responsibilities. Construction of and access to data marts for research use requires an IRB research repository application and may require data governance approval. Each research study using the data mart will require IRB application for the specific study. Outside a HIPAA exclusion such as patient HIPAA Authorization, release of data from data marts outside UT Health San Antonio requires data governance approval.

K. Limitations on Bulk Data Access for Research Use

1. Access and use of identified data in data marts for TPO is subject to attestation and renewal every 6 months. Research access and use are permitted as long as IRB approval is active. Access and use otherwise approved through data governance are subject to the limits documented on the approved Data Acquisition, Access, Use and Release (DAUR) form.
2. Access to Epics relational data store (Clarity) and other source systems is provided to individuals in institutional operational roles requiring such access to support healthcare TPO and research. These individuals are support professionals in Health IT or Clinical Research Informatics. These individuals work within established quality management systems and according to auditable, standard procedures.

L. Release of Patient-Level Data

Release of patient-level identified or de-identified data outside UT Health San Antonio or to persons who do not otherwise have access to the data requires explicit institutional approval. Data access privileges are separate from institutional approval for data release.

M. Two-Factor Authentication

Two-factor authentication is required in the following situations:

1. when an employee or other individual providing services on behalf of UT Health San Antonio (such as student employee, contractor, vendor or volunteer) logs on to the institution's network using an enterprise remote access gateway such as VPN, Terminal Server, Citrix or similar services;
2. when an employee or other individual providing services on behalf of UT Health San Antonio (such as student employee, contractor, vendor or volunteer) who is working from a remote location uses an online function, such as a web page to modify employee banking, tax, or financial information; or
3. when an employee or other individual providing services on behalf of UT Health San Antonio (such as student employee, contractor, vendor or volunteer) working from a remote location uses administrator credentials (also referred to as "Privileged Access") to access a Mission Critical Information Resource or a server that contains or has access to confidential data.

N. Test, Development and Systems Accounts

Information Resource accounts required for its development, testing or non-privileged operations shall be:

1. configured based on risk and least privilege;
2. approved by the Information Resource Owner, Custodian and CISO;

3. enabled for a period that minimally meets the objectives of development, testing or operation and is not to exceed 180 days. Continuous access must be requested by the Information Resource Owner or Custodian every 180 days; and
4. comply with access controls defined by this policy and associated standards and procedures, all other UT Health San Antonio Institutional Handbook of Operating Policies (IHOP) and UT System, state and federal policies and regulations.

O. Least Privilege and Segregation of Duties

1. Granting access to information and information systems must be based on the principle of least privilege, allowing only authorized access for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.
2. UT Health San Antonio shall adopt adequate controls to ensure separation of duties for tasks that are susceptible to fraudulent or other unauthorized activity.

IV. Definitions

When used in this document, the following words have the meaning set forth below unless a different meaning is required by context.

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]*

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 Resources Custodian (Custodian) – an individual, department, Institution, or third-party service provider responsible for supporting and implementing Information Resources Owner defined controls to Information Resources. Custodians include Information Security Administrators, institutional information technology/systems departments, vendors, and any third-party acting as an agent of or otherwise on behalf of an Institution. [*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*]

Mission Critical Information Resources – Information Resources defined by UT Health San Antonio to be essential to its ability to meet its instructional, research, patient care, or public service missions. The loss of these resources or inability to restore them in a timely fashion would result in the failure of UT Health San Antonio's operations, inability to comply with regulations or legal obligations, negative legal or financial impact, or endanger the health and safety of faculty, students, staff, and patients.

V. Related References

Institutional Handbook of Operating Policies (IHOP)
5.8.18 Third Party Management of Information Resources

UT System (UTS) Policy
UT System Identity Management Federation Member Operating Practices (MOP)
UTS 165 Information Resources Use and Security, Standard 4: Access Management
UTS 165 Information Resources Use and Security, Standard 15: Passwords

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
6/2002	Approved		
5/2011	Reviewed/revised		
10/2016	Reviewed/revised		
6/2018	Reviewed/revised		
9/2019	Reviewed/revised		
2/2020	Reviewed/revised	Executive Committee	02/09/2021
10/2022	Reviewed/revised	Executive Committee	10/12/2022