ADMINISTRATIVE POLICY TEMPLATE

Policy Title	**Clinical Data and HIPAA Covered Information Systems Policy**
Policy Subtitle/Subject	Click or tap here to enter text.
Responsible Executive(s) (RE)	**Victoria Johnson, General Counsel**
Responsible Office(s) (RO)	**Privacy Office and Information Security Office**
Primary Point of Contact from RO	**Elizabeth Davis**
Contact Information (email and phone)	**edavis23@tulane.edu**
Date Proposed	**12/9/25**
Reviewed	**12/9/25**
Last Updated	**12/9/25**
Effective Date	**4/16/26**

☒Permanent ☐Temporary

1.0 POLICY STATEMENT

Tulane University (Tulane or University) provides accounts to access HIPAA-Covered Information Systems and Protected Health Information (PHI) for clinical treatment, payment, research, and associated healthcare operations. This document outlines the rules, regulations, and procedures for provisioning and deprovisioning accounts and access rights to PHI on the University's HIPAA-Covered Information Systems.

2.0 PURPOSE AND SCOPE

The purpose of this policy is to define the parameters for user access issuance, modification, or revocation to HIPAA-Covered Information Systems and PHI.

3.0 APPLICABILITY OF THIS POLICY

This policy applies to faculty, staff, students, contractors, consultants, affiliates, and all others granted access to Tulane HIPAA-Covered Information Systems and PHI.

4.0 WEBSITE ADDRESS FOR THIS POLICY

Enterprise Risk Services will add the web address of the policy after it is added to the policy library.

5.0 CONTACTS

Identifies persons or departments that should be contacted if there are any questions or concerns regarding the policy.

Subject	Contact	Telephone	E-mail/Web Address
Questions or clarifications regarding this policy	Elizabeth Davis	504-988-0500	edavis23@tulane.edu
Report an actual or suspected security incident	IT Service Desk	504-988-8888	help@tulane.edu

6.0 CONTENT

The table of contents identifies the pages to find relevant information in the policy.

7.0 DEFINITIONS

Clinical Data: Clinical Data are information, records, and tangible products created or collected by the Tulane HIPAA Component during the course of patient care or as part of a formal clinical trial program. Clinical data would include electronic health records, clinical administrative data, claims data, patient/disease registries, health surveys, and clinical trials data. Clinical data is subject to all requirements documented within this policy as well as any additional requirements found within the **Governance and Retention of Research Data**, if applicable, and/or any other clinical policies.

Deprovisioning: The suspension or disabling of account access to an information system.

HIPAA: The Health Insurance Portability and Accountability Act of 1996. It primarily focuses on protecting the privacy and security of individually identifiable health information, known as Protected Health Information (PHI), and on ensuring the portability of health insurance coverage. HIPAA sets national standards for how PHI is used and disclosed, and it applies to healthcare providers, health insurance plans, and healthcare clearinghouses.

HIPAA-Covered Information System: Any information system used by the Tulane HIPAA Component in the creation, storage, receipt, or transmission of PHI. Examples of HIPAA-Covered Information Systems are included in Exhibit A.

Information Systems: Information systems are any and all computer or electronic resources that are used in the search, access, acquisition, transmission, storage, retrieval, or dissemination of data. In addition, Tulane information systems are any technology or services that are owned or managed by Tulane University, that connect to the Tulane network, connect to another Tulane technology or service, or store Tulane data or information.

NetID: An account that identifies a person and provides access to Tulane information systems and data. This account may be called electronic identity, NetID, or Tulane user account. This account provides access to information systems such as email, wireless networking, and VPN. NetID is not the same as a Tulane University email address.

Protected Health Information (PHI): PHI or Protected Health Information has the meaning assigned to such term in Tulane's Confidentiality of Protected Health Information Policy.

Provisioning: To create or provide specific accounts and applicable access to an information system.

Single Sign-On (SSO) and Federation: Enabling seamless access to multiple Tulane information systems and data with a single authentication process, often using federated identity systems (e.g., eduroam, InCommon).

Sponsor: A Tulane employee who sponsors an Affiliate's access to PHI.

System Owner: The official responsible for the overall procurement, development, integration, modification, or operation and maintenance of a HIPAA-Covered Information System.

Tulane HIPAA Component: Those components of Tulane University designated as its health care component in accordance with 45 C.F.R. §§ 164.103 and 164.105.

Tulane Users: Persons affiliated with Tulane University, including students, faculty, staff, affiliates, vendors, third-party consultants, etc. who utilize Tulane information systems or data.

Workforce Members: Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for the Tulane HIPAA Component, is under the direct control of such entity, whether or not they are paid by the Tulane HIPAA Component.

8.0 POLICY AND PROCEDURES

8.1 **Requirement to Use HIPAA-Covered Information Systems**.

The Privacy Office maintains a list of authorized HIPAA-Covered Information Systems and their System Owners. All Tulane Workforce Members are required to use authorized HIPAA-Covered Information Systems for all communication, collaboration, use, retention, storage, and/or access of Clinical Data. The HIPAA-Covered Information System(s) used for Clinical Data must meet all compliance, regulatory, and/or other legal obligations. Any HIPAA-Covered Information System must be vetted and authorized by the Security Officer, the Privacy Officer, and Office of General Counsel. For clarity, this Policy applies to, but is not limited to, the following HIPAA-Covered Information Systems:

a. **Email and message services**.

Workforce members are strictly prohibited from using non-authorized email and messaging services such as Gmail, Hotmail, Signal, SMS, and WhatsApp for Clinical Data, the transmission of Tulane information, and/or the conduct of Tulane business. Tulane provided email must be used for communications, the transmission of Tulane information, and/or the conduct of Tulane business. Use of non-sanctioned messaging services such as text messaging is strictly prohibited for Clinical Data, the transmission of Tulane information, and/or the conduct of Tulane business.

b. **Digital Storage**.

All Tulane Workforce members must use University-authorized HIPAA-Covered Information Systems (e.g., Tulane servers, Box as provided by Tulane, eClinical Works, and/or other approved University data storage systems) to store Clinical Data. Important written correspondence (including traditional mail and electronic mail, reports, analyses, and/or progress reports) related to Clinical Data also must be stored in such University-authorized data storage systems or servers.

8.2 **New HIPAA-Covered Information Systems.**

Any HIPAA-Covered Information System may become authorized upon satisfaction of the following requirements:

a. The legal contracts relating to such proposed HIPAA-Covered Information System, as well as the identity of the proposed System Owner, are provided to the Privacy Officer, the Security Officer, and the Office of General Counsel.

b. Appropriate IT review is performed. The process requires production of dataflow diagrams, information security review of new solutions, and IT assessment of integration feasibility into the Tulane environment.

c. The Office of General counsel shall have given its approval.

d. The Privacy Officer and the Security Officer shall have confirmed the following:

i. The System Owner shall have arranged for the proposed HIPAA-Covered Information System to be included in Tulane's risk assessment process and shall mitigate identified risks.

ii. Written agreements associated with the proposed HIPAA-Covered Information System with third parties contain language that Tulane PHI receives appropriate safeguards.

iii. A Business Associate Agreement shall be executed if required.

iv. The System Owner shall have confirmed that Clinical Data are backed up daily and protected sufficiently enough to re-establish the entire working environment for the Clinical Data, consistent with the Data Backup Plan Policy and any other applicable policies.

v. The System Owner shall have ensured that Clinical Data are available to the University on an as-needed basis during and after the lifecycle of the HIPAA-Covered Information System so that the University may respond to federal audits or other official requests, respond to subpoenas or other document demands, and conduct other internal and external oversight activities.

vi. The System Owner shall have ensured that Clinical Data will be retained in accordance with University policy and applicable laws and regulations.

vii. The System Owner shall have submitted satisfactory policies and procedures governing access to and auditing of the HIPAA-Covered Information Systems.

viii. The HIPAA-Covered Information System shall generate and maintain detailed logs of system activity which will allow Tulane to monitor access and shall otherwise meet the requirements of the HIPAA Security Rule.

ix. The arrangement complies with the information blocking provisions of the 21st Century Cures Act.

8.3 **Authorized Access.**

Only Workforce Members or Affiliates who have been authorized to have access to specified PHI in accordance with Tulane's Minimum Necessary Standard Policy may access HIPAA-Covered Information Systems and work with such PHI.

8.4 **Access Control Management.**

The System Owner of a HIPAA-Covered Information System is responsible for access control management. The System Owner, or designee, will serve as:

a. Access Granting Authority – the person(s) having authority to approve requests for access rights to the HIPAA-Covered Information System.

b. Access Control Administration – the person(s) or group (e.g., access control group) responsible for creating, modifying, and terminating a user's ability to access the HIPAA-Covered Information System or PHI.

For multi-user HIPAA-Covered Information Systems, if the System Owner delegates access granting responsibility it shall do so in a written policy or procedure.

8.5 **Access Rights.**

The System Owner will only grant access rights to those persons (e.g., Workforce Members, authorized Affiliates, and other legally authorized Users) or automated processes (e.g., an interface between two Systems) that have a legitimate need based on their current responsibilities or function to access the HIPAA-Covered Information System and in accordance with Tulane's Minimum Necessary Standard Policy and other applicable Tulane policies. The System Owner will verify that Users have completed any HIPAA training as required by the University Privacy Officer, and that any other necessary requirements have been met to establish that a user is authorized to access PHI prior to granting access rights. The System Owner shall consider the following in determining whether to grant access rights:

a. The individual's current functional need for access to the HIPAA-Covered Information System, as confirmed by the individual's supervisor or Sponsor, as appropriate;

b. Whether the requested access is at an appropriate level for the User's job and position, , as confirmed by the individual's supervisor or Sponsor, as appropriate;

c. Whether the request will give the User access to a range of data that is necessary and appropriate for their duties , as confirmed by the individual's supervisor or Sponsor, as appropriate;.

8.6 **Affiliate Access.**

a. Affiliate accounts and associated access rights will be granted only if the following requirements are met:

   a. A Sponsor recommends providing such accounts and associated access rights. Such Sponsor shall be responsible for safeguarding the information or information system and notifying the System Owner when the Affiliate no longer requires access to the HIPAA-Covered Information System or requires modified access rights to perform required functions (e.g., change in job duties); and

   b. Privacy Officer approval is obtained. The Privacy Officer shall be responsible for determining whether a business associate agreement is required and ensuring that any applicable HIPAA training has been completed.

b. Access to HIPAA-Covered Information System by Affiliates shall be subject to the requirements in this policy and have a lifecycle no longer than 12 months, after which they must be re-approved by the Sponsor.

8.7 **User Account Maintenance.**

The System Owner shall establish and maintain a User account for each user of a HIPAA-

Covered Information System to control authentication and access rights.

a. Setup Requirements.

User accounts may only be created and maintained for users whose access requests have been approved by the System Owner as outlined above.

b. Access Rights.

Each User account will carry with it access rights to the data within the HIPAA-Covered Information System. Access rights determine what data sets (e.g., which patients, accounts, records) the User may view, copy, create, update, or delete within the information system. Whenever technologically possible, access should be as granular as feasible; Users should only have read or write access to the specific PHI data required for performing their appropriate function.

8.8 Deprovisioning.

The System Owner shall revoke a User's access to Clinical Data and HIPAA-Covered Information Systems their affiliation with the institution ends. This includes the conclusion of employment, academic enrollment, or training programs. Graduating medical students, for example, will have their access removed as part of the graduation process

8.9 User Identification and Authentication.

Access to a HIPAA-Covered Information System requires the use of a unique user identifier (e.g. NetID) in conjunction with an associated password or other type of authenticator that has been approved by the HIPAA Security Officer.

8.10 **Access Control Administration**.

The System Owner is responsible for:

a. Assigning each authorized User of the HIPAA-Covered Information System a unique NetID. A User may be assigned the same NetID to access multiple information systems.

b. Providing Users a secure mechanism to create a password or other authenticator that will be used to verify that the User seeking access to the HIPAA-Covered Information System is the one claimed. Except where not supported by the HIPAA-Covered Information System, Tulane Single Sign-On (SSO) authentication must be used.

8.11 **Responsibilities of Users.**

Users are required to:

a. Use only their unique NetID and authenticator(s) to access the HIPAA-Covered Information System. Use of another User's NetID and/or credentials to access a HIPAA-Covered Information System is prohibited.

b. Change their authenticator (excluding only biometric authenticators, where applicable) on a regular basis. Where Tulane SSO is not used, the System Owner will determine frequency of change prompts based on risks associated with the HIPAA-Covered Information System.

c. Change their authenticator whenever there is reason to suspect that it has or may have become known to another person or otherwise compromised.

d. Password length will adhere to current standards as adopted by Tulane University for their primary NetID.

8.12**Modification and Termination.**

a. Tulane managers and supervisors will immediately notify the appropriate System Owner whenever a User of an information system no longer requires access to a HIPAA-Covered Information System (such as due to termination of employment) or requires modified access rights in order to perform required job functions (such as due to change in job duties).

b. Sponsors will immediately notify the appropriate System Owner whenever an Affiliate who is a User of an information system no longer requires access to a HIPAA-Covered Information System (such as due to termination of employment) or requires modified access rights in order to perform required job functions (such as due to change in job duties).

c. The Office of Human Resources shall circulate to each System Owner a weekly list of employees transferred, terminated, or otherwise separated from the University during the previous week.

d. The System Owner will modify or terminate the User account access as appropriate based on receipt of the communications described above.

8.13 Other Deprovisioning Requirements.

a. Access rights removed or adjusted should include those of physical and logical access. Removal or adjustment can be done by removal, revocation, or replacement of keys, identification cards, information processing facilities, or subscriptions.

b. The System Owner shall maintain records of the removal or adjustment of access rights.

8.14**Access Monitoring.**

a. Each System Owner shall periodically review User access to ensure that each person's access privileges are appropriate.

b. Each System Owner will periodically review HIPAA-Covered Information System activity reports, including audit logs, access reports, and security incident tracking reports to ensure that implemented security controls are effective and that PHI has not been potentially compromised. Measures should include enabling logging on HIPAA-Covered Information System, developing a process for the review of exception reports and/or logs, developing and documenting procedures for the retention of monitoring data, and periodically reviewing compliance to Tulane policies and procedures.

8.15 **Emergency Procedures.**

The System Owner shall establish procedures for obtaining necessary PHI during an emergency as required by 45 CFR § 164.312(a)(2)(ii).

8.16 **Procedures**.

Each department or program included in the Tulane HIPAA Component will develop, document, implement, and train its Workforce Members on the procedures necessary to comply with this policy. Departmental or program procedures will include identification by title of the person(s) responsible for complying with the required activities and provisions.

9.0 CONSEQUENCE OF VIOLATING THE POLICY

Violation of this policy may result in disciplinary action, up to and including termination and/or criminal prosecution.

Failure to comply with the standards outlined here and in related policies may result in harm to individuals, organizations, or the University. Violations of this policy or any laws related to the use of a Tulane information system, including HIPAA, may result in penalties and disciplinary action under rules established by the University.

APPENDIX I

Related Policies:

- Identity and Access Policy (pending)
- **Data Management Policy**

- **Data Classification Policy**
- **Governance and Retention of Research Data**
- **Confidentiality of Protected Health Information Policy**
- **Minimum Necessary Standard Policy**
- **Tulane IT Policy Library**
- **Tulane Policy Library**
- Data Backup Plan Policy

APPENDIX II

Exhibit A

HIPAA-Covered Information Systems include, but are not limited to:

- eClinicalWorks (eCW)
- IDX
- Box
- REDCap
- IMPower
- Zoom
- Laserfiche
- MEDITECH
- Medicap
- Microsoft Office