UT Health San Antonio
Joe R. & Teresa Lozano Long School of Medicine

Department of Population Health Sciences
Clinical Research Informatics Division

STANDARD OPERATING PROCEDURE

SOP Number: CRI.SOP. SDLC-005	**Title: Access Control**	
Version No.: 1.0	**Effective Date: February 28, 2023**	**Page 1 of 4**
Supersedes Version: N/A **Dated:** N/A	REQUIRED APPROVALS BELOW	
CRI Director:	DocuSigned by: Bill Sanns FB861DB144CF4B1...	**Date:** 3/1/2023
CISIL Approver 1:	DocuSigned by: Becki Gerwitz 0C0BFDB1724D1...	**Date:** 3/1/2023
CISIL Approver 2:	DocuSigned by: Stephen Hargrove 5AEBB2C5776E46A...	**Date:** 3/1/2023

1.0 Purpose

This Standard Operating Procedure (SOP) establishes processes to manage access control to CRI-managed systems, applications, and data.

2.0 Scope

This procedure applies to all users, staff, personnel, faculty, etc., that are in any manner accessing or using CRI-managed systems, applications, and data whether or not they are university employees. Access controls generally refer to both authentication (proving who you are) and authorization (what permissions you have); however, this SOP will defer to UT System and UT Health San Antonio authentication protocols and will focus on local system authorization and need to know.

3.0 Responsibility

3.1 Technical Director: role bears responsibility for assuring any software written complies with this SOP.

3.2 Senior Manager: role performs all functions related to tracking activities, managing resource allocation required for the software development process, and is the Technical Director's primary backup.

3.3 System Administrator: role performs all functions related to establishing, managing, and maintenance related to Population Health Sciences' managed servers, software, network, and security.

3.4 Software Developer Senior/Team Lead: role assures each developed application follows the application owner's authorization requirements

3.5 Data Warehouse Developer Senior/Team Lead: role assures that warehouse programmers who access the data warehouse have proper authorization to do so.

3.6 System Owner: role defines access requirements to the software system.

3.7 Data Owner: role defines access requirements to specific data

4.0 References

4.1 UT System: UTS 165 Information Resources Use and Security

4.2 UT Health San Antonio Handbook of Operating Policy 5.8.4: Access Management

4.3 21 CFR Part 11, Electronic Records; Electronic Signatures, March 20, 1997

4.4 General Principles of Software Validation: Final Guidance for Industry and FDA Staff, January 11, 2002, FDA

4.5 CRI.SOP.SDLC-001 - External Software Installation and Verification

4.6 CRI.SOP.SDLC-003 - Software Development

5.0 Acronyms and Definitions

Term	Definition
Authentication	Proving you are who you say you are
Authorization	Granting permissions to do something
COTS	Commercial Off the Shelf Software/System
CRI	Clinical Research Informatics
DUA	Data Use Agreement: a contract that governs the exchange of specific data between two parties
IMS	Information Management Services: UTHSA's central IT Operations
Least Privilege	When a user is given the minimum levels of access – or permissions – needed to perform his/her job functions.
Need to Know	limiting access to the information that a job function requires, regardless of their security clearance level or other approval
PHI	Protected Health Information
SOP	Standard Operating Procedure
SOW	Statement of Work: a document within a contract that describes the work requirements for a specific project along with its performance and design expectations.
System Owner	The term used to identify the primary point of contact for any server, resources, system, or application deployed by CRI staff and factulty.
UTHSA	University of Texas Health Science Center San Antonio
VM	Virtual Machine: Used as a generic term to describe a server-based container that will host the software application or service.

6.0 Procedure

PHS CRI access control relies on the following three concepts

6.1 Authentication:

6.1.1 You are whom you claim to be generally done through two mechanisms

6.1.1.1 Multi-factor authentication: using more than one of the following

6.1.1.1.1 What you know: usernames, passwords, PINs, etc

6.1.1.1.2 Who you are: biometrics

6.1.1.1.3 What you have: cellphone verification, Computer Access Cards, etc.

6.1.1.2 Multi-mode authentication: Using one factor more than once such as knowing a username, password, and/or PIN to gain access to systems or data.

6.1.2 PHS CRI defers to and will follow all UTS and UT Health SA HOP authentication policies and guidelines.

6.2 Authorization

6.2.1 Given who you are, you may have specific system or data access rights operating directly under the concept of "least privilege".

6.2.1.1 Systems that interact with one specific set of data: authorization determined by the system owner

6.2.1.2 Systems that interact with more than one set of data: authorization determined by the data owner.

6.3 Need to Know

6.3.1 Ensures any single person only has rights to systems or data for which there is a direct and documented need regardless of authentication or authorization levels.

6.3.2 Defined by the system and/or data owner and managed through either role-based (what type of position a user holds) or individual-based (individual-specific) rights determined by project need and/or system capabilities.

6.4 Mechanism and Process to define and implement access controls based on CRI Resources

6.4.1 **Externally Managed Systems**: Externally managed systems (e.g., Epic, Peoplesoft, etc.) do not fall under this SOP. All CRI staff and faculty will submit to and follow the rules and requirements of those systems; however, it is CRI's responsibility to assure access controls and documentation requirements are met, properly managed, and up to date.

6.4.2 **COTS/Open Source Systems:** Access to CRI deployed and managed systems are based on the criteria specified within this SOP, and is managed at a level determined by the features built into these systems.

6.4.3 **CRI Developed Software:** Access to CRI deployed and managed systems are based on the criteria specified within this SOP, and is managed at a level determined by the requirements as defined by the CRI.SOP.SDLC-003 - Software Development SOP.

6.4.4 **Servers and Server Resources:** Access to CRI servers or VMs are based on the criteria specified within this SOP, is approved by either the Technical Director or Senior Manager and is implemented by CRI's System Administrators.

6.4.5 **External Data:** Any data residing on a CRI server, resource, system, or application that was not collected by a CRI-managed or CRI-developed system is considered External Data and will be managed in accordance with its associated Data Use Agreement (DUA), contract, Statement of Work (SOW), or research protocol.

7.0 SOP Deviations

Deviations from this and all SOPs are handled according to CRI.POL.001 *Clinical Research Informatics Quality Management System (QMS)*.

8.0 Review & Revisions

Review and revisions of this and all SOPs are handled according to CRI.POL.001 *Clinical Research Informatics Quality Management System (QMS)*.

9.0 Attachments

10.0 Revision History

Version No.	Revision Date	Description of Revision