DI-r Process:	**DIR Non-Privileged Access Management Process**		
DI-r Process No.:	**DIR-PRC-002**		
Owner of Process:	**Coordinator, DIPACS ITS Department**		
SLT Sponsor:	**Manager, DIPACS ITS Department**		
Approval Date: **TBD**	**Effective Date:** TBD	**Reviewed Date:** -	**Revised Date:** -
Parent Standard:	ITS-STD-###	Identity and Access Management Standard	
This process applies to:	Any individual or organization that users the DI-r Systems with a non-privileged account.		

1. PURPOSE

Non-Privileged access provides the ability to view patient information within and outside of their local hospital. There are over 74 hospitals and independent health facilities patient records in the Diagnostic Imaging Repository. The patient information includes: demographics, orders, reports and diagnostic images.

The purpose of this process is to reduce organizational risk and ensure the appropriate management of non-privileged access. Such risks include, but are not exclusive to:

- Unauthorized access to financial, personal health information, personal information or corporate information for personal benefit
- Privacy breaches, possible IPC orders, fines, investigations and / or prosecutions
- Identity theft
- Attack on systems i.e. denial of service
- Legislative and Regulatory non-compliance
- Legal action against the hospital
- Disruption to clinical care processes or business functions of the hospital
- Reputational damage to the hospital in the event of privacy and / or security breach, theft, or other adverse effect
- Financial exposure, including but not limited to, insurance coverage, liabilities, claims, losses, damages, expenses, legal fees

2. VALUE TO ORGANIZATION

The value of the non-Privileged Access Management Process is to:

- Establish a standard consistent approach to manage non-privileged access
- Mitigate risk to the organizations services, systems, confidential information and processes
- Maintain the security, integrity and availability of hospital systems
- Provide an auditable process to the management of non-privileged access
- Reduce non-privileged level access to only those that require such access based on the authorized job function or business needs
- Educate business, system and ITS service owners of their accountability and responsibilities for managing non-privileged access
- Develop accountability to business, system, and ITS service owners to manage non-privileged access

3. PROCESS PRINCIPLES

Principle 1: A standard, consistent approach to manage non-privileged access is to be used across the Southwester Ontario Diagnostic Imaging Network.

Principle 2: All non-privileged access management activities must be appropriately documented within the local hospital of the Local Regional Authorities.

Principle 3: Authorization of non-privileged access is the responsibility of the Local Regional Authority and/or ITS service owner.

Principle 4: Approvals and authorizations for non-privileged accounts must not be delegated.

Principle 5: Non-Privileged access to systems is granted on a least-privilege basis.

Principle 6: Non-Privileged access account passwords are in compliance with the corporate password standard, subject to any system limitations or if user is at a local hospital it is the corporate password standard for that users. If the hospital does not have a password standard, the hospital is recommended to use the eHealth policies to set a standard.

Principle 7: System and service owners perform a quality review and assessment of non-privileged access as part of their role responsibilities.

4. ROLES AND RESPONSIBILITIES

4.1.Local Regional Authorities

- Approve creation of, modifications to, or the disabling / deactivation of accounts
- Ensure only authorized individuals can create accounts
- Ensure only authorized individuals are create or have privileged accounts
- Review and revise access to users when users change roles or departments, take extended leaves or end employment.
- Monthly review of reports, provided by SWODIN, containing user name, ID, title, and last login date and time
- Follow local policies, standards and processes for maintaining access control.
- Ensure accounts are designed with least-privileged access possible
- Local Privacy Office to regularly review audit logs for inappropriate access, failed access attempts and situations where access is questionable.
- Local Privacy Office attends regularly to Regional Privacy Meetings
- A local regional authority or site administrator attends the hub collaboration call regularly to obtain any new information from SWODIN or guest speakers

4.2.SWODIN Service Owners

- Reinforce importance for protection of information resources through access control management; in privacy message pop up every quarter upon OneView login, yearly during hub collaboration call.
- Export user activity report from OneView and provide on a monthly basis to Local Regional Authority for review.
- SWODIN team access approvals follow the LHSC policies, standards and processes.
- Review eHealth's policies for any recommendations to implement for the DI-r systems on an annual basis.
- Set a password standard based on eHealth's recommended policies.

5. PROCESS

There are four processes involved in managing access:

1. Assessing, Authorizing, Authenticating, Granting and Altering Access – A non-privileged request must be submitted by the user or manager of user and approved by a Local Regional Authorities. The LRA reviews what access provides the least privilege and the user is associated to that specific access group. A privileged user who manages creation of accounts grants or modifies access based on the Local Regional Authority.

2. Terminating access – A request must be approved by a Local Regional Authority, and follow the local hospital policies and standards for account suspension. A non-privileged user who manages deactivation of accounts on behalf of the Local Regional Authority.
3. Auditing: Attestation and Privacy – Local Regional Authorities are to review non-privileged access accounts monthly to ensure all non-privileged access, at the local site, is appropriate based on the users job responsibilities. The regional privacy office is responsible for reviewing audits of inappropriate access, failed access attempts and situations where access is questionable.
4. Monitoring/Reviewing/Managing access – Local Regional Authorities will be responsible to ensure the appropriate mechanisms are in place to review and identify the appropriate users have access to the DI-r systems. The Local Regional Authorities will use the activity logs to review last log in date, access privileges, password expiry timeframes, and if user should have access and resides in their hospital or independent health facility. SWODIN team will provide monthly activity logs for every user at their facilities.

5.1.Process Roles and Responsibilities RACI

Process Activity	SWODIN	Local Regional Authority	Privileged User
Requesting new, modifications to, disabling or removal of privileged access accounts	R	A	R
Approving new, modifications to, disabling or removal of privileged access accounts	R	A	R
Creating, modifying, disabling/deleting privileged access accounts	R	A	R
Pulling and providing lists to system owners for access management	R	A	I
Review of non-privileged access accounts	C	A	R
Post-access management modifications and documentation	R	I	I
Monitoring of non-privileged access accounts	A	R	R
Record and store review of access management results at Local Site	A	I	R
Record and store review and attestation results ITS	R	-	-

DEFINITIONS

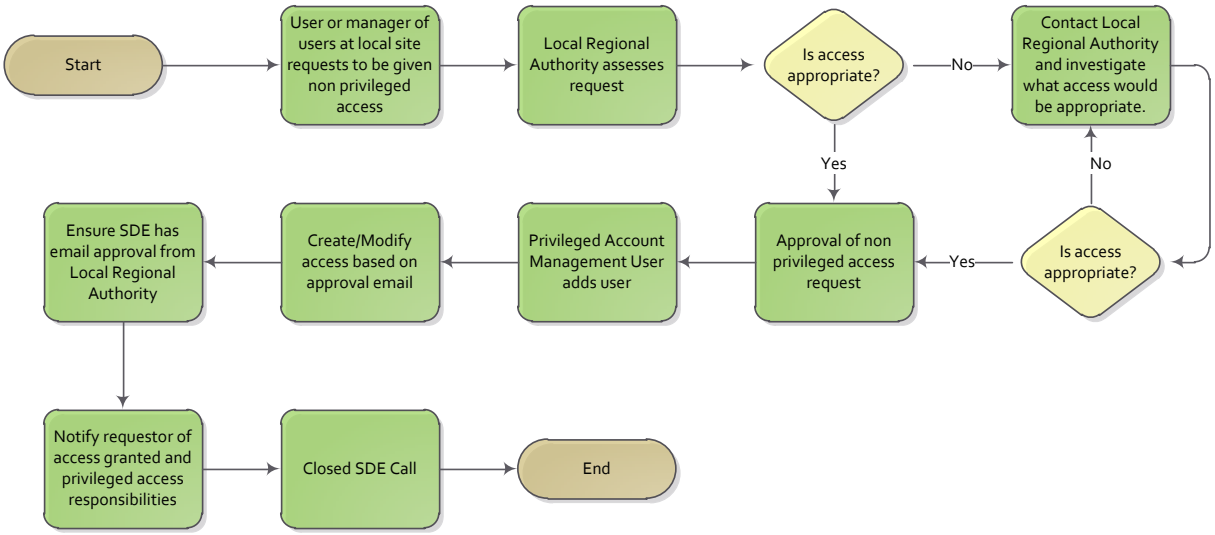
A: ACCOUNTABLE *- The accountable person is the individual who is ultimately answerable for the activity or decision. This includes "yes" or "no" authority and veto power. Only one "A" can be assigned to an action.*

R: RESPONSIBLE – *The "doer." This is the individual(s) who actually complete the task. The "doer" Is responsible for action/implementation. Responsibility can be shared. The degree of responsibility is determined by the individual with the "A".*

C: CONSULTED *- The consulted role is the individual(s) (typically subject matter experts) to be consulted prior to a final decision or action.*

I: INFORMED *- This is the individual(s) who needs to be informed after a decision or action is taken. They may be required to take action as a result of the outcome.*

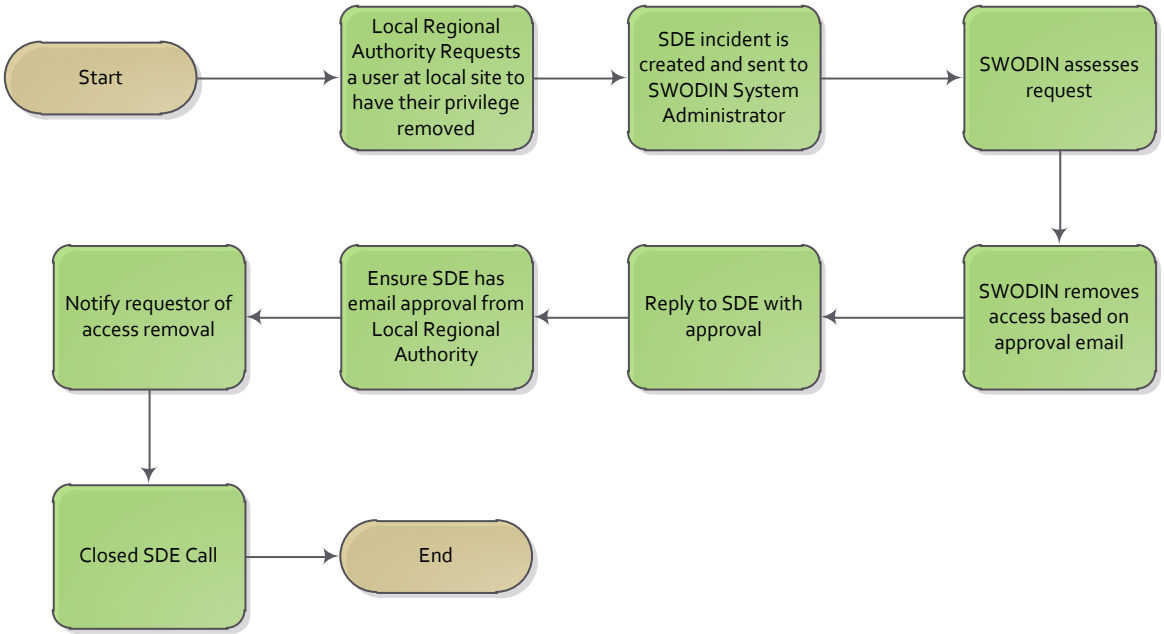
5.2.Granting and Modifying Access



5.3.Terminating Access

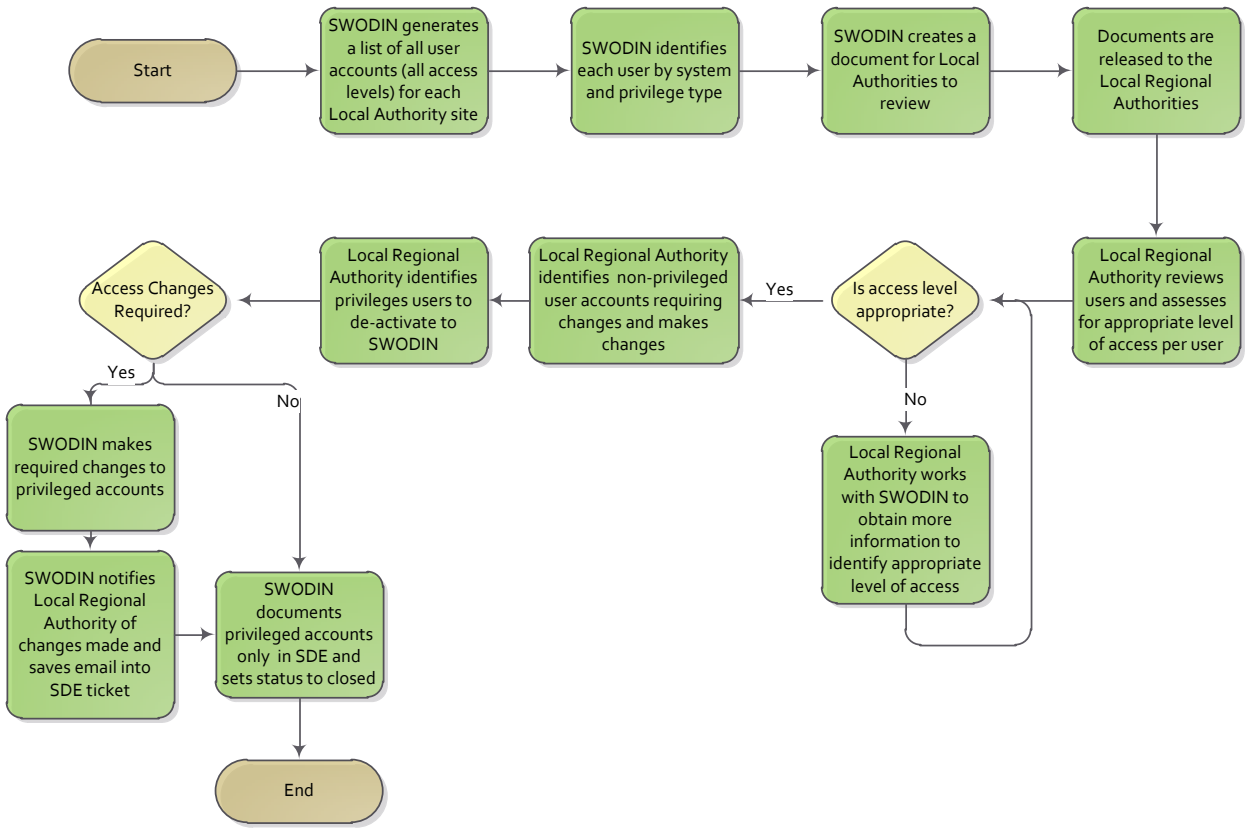
Local Site Workflow

SWODIN Workflow



5.4.Managing Access

Review is required on a monthly basis.



6. Definitions

Least Privilege – a security principle requiring that each user in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.

Access Controls – In the fields of physical security and information security, access control is the selective restriction of access to a place or other resource. The act of accessing may mean consuming, entering, or using. Permission to access a resource is called authorization.

Local Regional Authorities: Manager PACS/DI-r - PACS and DI-r systems. Is the clinical or business person, at a partnered hospital or independent health facility, whether corporate or departmental, with the authority to send information from the local site to the DI-r system, use the DI-r system and approving addition or removal of user accounts.

System - A system includes all of the layers that comprise it: the application, the database, the operating system and the server or servers they are installed on.

SWODIN Administrator: One whose role is to perform activities which may affect applications and / or systems, servers, network communications, end-user accounts, files, data, or processes of users. A system includes all of the layers that it comprises: the application, the database, the server, and the infrastructure to connect to it.

Document Revision History

Revision	Author	Date	Comments
1.0	Arielle Fuller	Aug 30, 2016	Original draft