William Osler Health System

Local Registration Authority Procedures Manual

Table of Contents

Introduction 2

1.1 Purpose 2

1.2 Scope 2

2.0 Sponsorship, Registration and Enrolment 3

2.1 Registration Roles 3

2.2 Infrastructure of Trust 4

3.0 External Organization Access Provisioning Requirements 5

3.1 Identity and Organizational Validation 5

3.2 Professional Licence Validation 6

3.3 Challenge Questions and Remote Identity Verification 6

4.0 Local Registration Authority (LRA) Role and Responsibilities 7

4.1 LRA Nomination 7

4.2 LRA Responsibilities 7

4.3 LRA Procedures 10

Introduction

The Local Registration Authority (LRA) process is used to verify the identity of external staff and grant secure access to Osler's internal digital health services and sensitive personal health information (PHI). The LRA model supports external user access to Osler's protected digital health systems by requiring each external partner organization to identify an LRA who will support onboarding and access for users at their site.

This LRA process aligns with Osler's Identity and Access Management (IAM) Policy which sets the baseline security requirements for logical access control within information systems and applications owned by, or under the control of Osler.

1.1 Purpose

This document details how LRAs verify and onboard external users and manage their access to Osler's Epic HIS Platform and other digital systems.

1.2 Scope

This document applies to external organizations, their Authorized Representatives, LRAs, external users, and designated Osler personnel involved in sponsoring, validating, provisioning, reviewing, or terminating access to Osler's digital health services.

2.0 Sponsorship, Registration and Enrolment

This section provides an overview of the LRA process key concepts:

- **An Infrastructure of Trust** – the foundation that permits the model to build a network of trust.
- **Sponsorship** - the nomination of applicants by an authorized source for access to one or more services.
- **Registration** – the process of verifying the identity of applicants and proving they are who they claim to be.
- **Service Enrolment** - the process of providing registrants with access to services.

2.1 Registration Roles

These are key roles involved in authorizing registrations:

Role	Description	Example
External Organization	The external legal entity that has entered into an agreement with Osler and is accountable for sponsoring eligible members of its workforce for access to Osler services.	External hospital, clinic, pharmacy, or organization with a designated LRA.
Legally Responsible Person (LRP)	The individual who is legally responsible and oversees the LRA registration process within their organization. The Authorized Representative has the authority to sign a legal agreement on behalf of their organization. The LRP confirms that appropriate sponsors and LRA(s) are identified and that the organization understands its access-related obligations.	External organization CEO, CAO, executive leader, or Lead Physician at a family practice clinic.
Authorized Representative	Designated individual with authority to sign agreements or confirm sponsorship arrangements on behalf of the External Organization.	CEO, CAO, clinic owner, or Lead Physician authorized to represent the external organization.
Sponsor	The sponsor is an authorized Osler representative nominated by a business unit or department who internally approves and requests for user accounts to access Osler's protected digital services. The sponsor confirms that a user has a legitimate business or clinical requirement to access specific Osler protected digital services.	Osler manager, business owner, department lead, or authorized service owner.
Local Registration Authority (LRA)	Operational role responsible for completing registration activities, validating required information, supporting onboarding, and acting as the primary liaison between Osler and the external organization for LRA-related access matters.	Designated staff member within the external organization, clinic, or hospital.

External User / Registrant	Individual who requires access to an Osler service and is submitted for registration, validation, service enrolment, and ongoing access review.	External staff member, physician, clinician, or member of a physician's care team.

2.2 Infrastructure of Trust

Infrastructure of trust refers to the LRA process model that relies on recognized, trained, and trusted individuals within an organization to verify identity and support authorized access to Osler digital information and health services for external staff and personnel. For the trust model to work, questions must be answered for all individuals requesting access to Osler services such as (a) Who are you? (b) Who provided you sponsorship and from which organization? And (c) Can you prove your identity?

An organization (e.g. Hospital, Clinic, Pharmacy or external organization) may sponsor members of their health care team or staff to access digital health services offered by Osler.

Once an individual is sponsored and registered with an Osler Credential (login ID, password and MFA), this credential has the full weight and authority of the sponsoring organization.

3.0 External Organization Access Provisioning Requirements

External organizations requesting access to Osler's Epic HIS Platform or other authorized digital systems for their users are responsible for ensuring that access is requested only for individuals who have been appropriately identified, validated, and authorized.

The organization is responsible for ensuring that the following requirements are completed before access is requested and for maintaining compliance with applicable access requirements for the duration of the individual's access.

3.1 Identity and Organizational Validation

The organization must ensure that each individual's identity is validated before access to Osler systems is requested.

For identity validation, the individual must provide identification that meets the following requirements:

- Identification must be government-issued and contain the individual's legal name, gender, and date of birth.
- At least one identity document must contain a photograph of the individual.
- Identity documents must be original documents and not photocopies.
- All identity documents must display the individual's name.
- All identity documents must be current and valid.
- The individual is legally authorized to work in Canada.
- The individual has successfully completed the background checks required by the organization.
- The individual has signed all applicable confidentiality, privacy, security, and other required agreements.
- The individual **is current with all required annual privacy and security training and remains current for the duration of their access**.
- The required user PIN and LRA PIN are used in accordance with the established identity-validation process.

The organization may designate an approved LRA to perform identity-validation activities on its behalf in accordance with Osler's established registration and access processes.

3.2 Professional Licence Validation

The external organization is responsible for ensuring that users who require professional credentials as a condition of their role or system access, hold current and valid credentials, where applicable.

Users who are licensed by an Ontario regulatory health college must have the applicable professional credentials associated with their Epic account where required for their role and access privileges.

Professional credentials must be validated using supporting documentation provided by the individual or an authoritative source, such as the applicable regulatory college's public register.

The external organization is responsible for ensuring that changes to an individual's professional status that may affect their access are identified and communicated to Osler through the established access-management process.

3.3 Challenge Questions and Remote Identity Verification

As part of the registration and self-enrolment process, individuals may be required to provide responses to predefined challenge questions. These responses may be used as an additional method of verifying an individual's identity when remote support is provided, including support by telephone or online.

The organization is responsible for ensuring that individuals authorized to perform identity verification use challenge questions and responses **solely for authorized identity-verification purposes** and in accordance with the established identity-verification process.

Challenge-question responses must be treated as confidential authentication information and must not be disclosed, shared, or used for purposes unrelated to authorized identity verification.

An individual's identity must be successfully verified using the established verification process before a request for account support is submitted to Osler.

4.0 Local Registration Authority (LRA) Role and Responsibilities

The Local Registration Authority (LRA) is a role assumed by individuals who have been nominated by their organization and approved by Osler to execute onboarding responsibilities to access Osler's Epic HIS Platform and other digital systems.

4.1 LRA Nomination

How to nominate someone to be the LRA for your organization?

1. Your organization needs to provide proof of the following information for the LRA Nominee from a trusted source within your organization:
    a. Are they legally allowed to work in Canada?
    b. Have they passed background checks before being hired to your organization?

2. The trusted source at your organization will be required to have the LRA Nominee fill out and sign the external access form that contains the following documentation:
    a. User Information
    b. Application Access requirements
    c. Statement of Accountability with LRA Nominee details
    d. Signed Confidentiality Agreement

3. Submit the completed nomination form to your organization's designated Sponsor at Osler. The Sponsor is responsible for submitting the LRA Nomination Form through the Service Desk process.

4. Successfully complete LRA training as required by Osler.

5. Once your request has been reviewed and approved, you will receive an email with instructions on the next steps.

4.2 LRA Responsibilities

All Local Registration Authorities (LRAs) are responsible for tracking their activities within their organization and **ensuring compliance with the requirements outlined in this**

document. The organization's Authorized Representative must conduct a monthly review of LRA activities to validate continued compliance.

LRAs are responsible for the following:

1. **Account Setup and MFA Support**
   Serve as the primary point of contact to assist users with **initial password setup and Multi-Factor Authentication (MFA) configuration**, in accordance with Osler's Identity and Access Management Policy.

2. **Epic CareLink Support Escalation**
   Serve as the point of contact for users and **escalate Epic CareLink application issues to the Osler Service Desk when required**.

3. **Quarterly User Attestation**
   Review and attest to the continued access requirements of **all users associated with their organization at least every 90 days**. Failure to complete the required attestation may result in the **deactivation of user accounts associated with the organization**.

4. **Monthly Access Review**
   Conduct a monthly review of user accounts to confirm that access remains appropriate for each user's current job duties and is consistent with the **principle of least privilege**.

   The review must also identify dormant or inactive accounts and users who no longer require access. **Osler must be notified within 48 hours of the LRA becoming aware that a user no longer requires access.**

5. **User Account Changes and Termination**

   For users with access to Epic Hyperspace, the LRA must **immediately notify the Osler Sponsor when a user:**

   - Changes job role; or
   - Leaves the organization.

   The Osler Sponsor must review and validate the user's continued access requirements and submit the appropriate **access modification or termination request to the Osler Service Desk**.

   Osler will deactivate user accounts that have been inactive for **six months or longer**. A deactivated account may be reinstated only where access remains appropriate for the user's current job duties and responsibilities and has been **approved by the user's manager and the Osler Sponsor**.

6. **Transaction and Record-Keeping Accountability**

   Each LRA is accountable for **the transactions they perform and for maintaining accurate records of LRA activities conducted on behalf of their organization**.

   Organizations are **required to maintain their own records of LRA activities** to support reconciliation, compliance monitoring, and audit requirements. Upon request, Osler may provide the organization with a report of users sponsored by the organization and transactions performed by its LRAs.

   At a minimum, records must include:

   - **User registrations** submitted or completed on behalf of the organization.
   - **User access changes**, including additions, modifications, and removals of access.
   - **Account termination or deactivation requests** for users who no longer require access.
   - **Supporting requests or approvals**, whether received electronically or in hard copy, associated with user registration or access changes.

7. **Privacy and Security Incident Reporting**

   LRAs must report any suspected or confirmed privacy or security incident to the Sponsor **as soon as reasonably possible, and no later than 24 hours after becoming aware of the incident**.

   Osler, in coordination with the LRA's organization, will investigate and manage the incident through the applicable incident-management process.

   Examples of privacy or security incidents include, but are not limited to:

   1. Personal Information (PI) collected or recorded during the registration process is **lost, stolen, or misplaced**.
   2. Personal Information is **accessed, obtained, or used without authorization**, including for the purposes of identity theft.
   3. An unauthorized individual **accesses or obtains registrant identity information**.
   4. Information collected for registration or identity-verification purposes is **used or disclosed for an unauthorized or unintended purpose**, such as updating an unrelated human resources database.

4.3 LRA Procedures

Request a copy of the detailed LRA user management procedures from your sponsor.

- Community User – Manage Your Clinic (EpicCare Link Homepage)
- LRA EpicCare Link User Management Procedures
- LRA Epic Hyperspace External Access Procedures