

# eHealth Identity Federation User Authorization Summary

Access management within the eHealth Identity Federation requires coordination between Health Information Custodians (HICs) and eHealth Ontario. HICs verify that prospective users have met all eligibility criteria for the service while eHealth Ontario executes the technical steps required to grant users access on the HICs' behalf.

This document provides an overview of the processes by which a HIC should inform eHealth Ontario of new user authorizations and changes to existing user authorizations.

## Local Registration Authorities

Local Registration Authorities (LRAs) perform Identity and Access Management on behalf HICs. Specific responsibilities may vary depending on the eHealth Service(s) being supported and/or the Identity Provider(s) being leveraged but all LRAs must:

- Be registered in eHealth's ONE ID Identity Management system at Assurance Level 2.
- Be nominated by the HIC's Signing Authority or Authorized Representative; the LRA Nomination Form should be sent to [eHealthOntario-ONEIDBusinessSupport@ehealthontario.on.ca](mailto:eHealthOntario-ONEIDBusinessSupport@ehealthontario.on.ca).

## Individual Authorization/Revoke Requests

To grant an individual access to a Federated Service, the LRA should email a request to [registration.agents@ehealthontario.on.ca](mailto:registration.agents@ehealthontario.on.ca). Requests must include:

- The individual's Login ID
- A clear statement of which HIC has authorized or revoked the individual for access. This must be explicitly stated in the email body; an implicit statement (e.g. the name of the organization in the email signature) cannot be relied upon for authorization.
- The name and contact information of the LRA (may be included in the email signature)
- Example email text: "Please grant JANE.DOE@ABCHOSPITAL.CA access to the ConnectingOntario Clinical Viewer as per authorization from ABC Hospital."

Authorization and revoke requests will be completed in 5 business days or less, in accordance with eHealth Ontario's standard registration and enrolment service levels. In the event that an authorization/revoke is needed more urgently, this should be indicated in the email body. Best efforts will be made to accommodate such requests.

LRAs will receive notification via email after the Authorization/Revoke Request is completed.

## Bulk Authorization/Revoke Requests

LRAs should contact the Business Delivery Team at [eHealthOntario-ONEIDBusinessSupport@ehealthontario.on.ca](mailto:eHealthOntario-ONEIDBusinessSupport@ehealthontario.on.ca) in circumstances where individual email requests are impractical (e.g. during service implementation when the initial

---

user group must be added). Users can be authorized or revoked in bulk according to a mutually agreed upon schedule.

## Authorization Tracking

LRAs are expected to maintain a record of who has been authorized to access Federated Services under the authority of their organization. At a minimum, this record should include:

- The Login ID of the user
- The Login ID of the LRA who requested their access
- The date on which they were granted access (as per the confirmation email from eHealth Ontario)
- The date on which the authorization was revoked (if applicable)

To support this process, eHealth Ontario can produce a report of authorized users at the request of an organization's LRA. Please submit requests to [Registration.Agents@chealthontario.on.ca](mailto:Registration.Agents@chealthontario.on.ca).

## ONE® ID as Identity Provider

The individual Authorization/Revoke process described above corresponds with the Email Request Process described in the LRA and ERA Procedures Guides with the following exceptions:

### Suspending Access

“Suspended” is not a valid state for Federated Authorizations; users are either authorized or they are not. If a user must lose access temporarily (e.g. during a leave of absence), a revoke request should be submitted, followed by a new authorization on the appropriate date (e.g. when the user returns to work).

### Tracking Authorizations

Authorizations for Federated Services will not be displayed in the “Enrolments” or “Event Log” tabs of the user's profile in ONE® ID Web. Because Authorizations are managed outside of the ONE® ID System, there is no facility to display this information in the ONE® ID Web Interface. LRAs & ERAs should track authorizations by following the same protocol described above.