

Guide for Legal Signing Authorities Using AGS

**ACCESS
GOVERNANCE
SYSTEM**

**HITS
eHealthOFFICE**
Innovating & Transforming
eHealth Solutions

This guide reviews the Access Governance System (AGS) functionality specifically for Legal Signing Authorities of ClinicalConnect Participant Organizations.

May 2020

The contents of this document are confidential and proprietary to the HITS eHealth Office at Hamilton Health Sciences, and are meant for private circulation only. No part of this document may be disclosed, shared, reproduced, transmitted, made public or copied in any form or by any means without the express written permission of the HITS eHealth Office at Hamilton Health Sciences © 2020

Contents

Getting Started	2
Support Contacts & Resources	2
Highlights of Organization's Participation in ClinicalConnect	3
Ways to Access ClinicalConnect.....	4
Overview of "Under the Authority Of" (UAO) Selector and AGS	5
Assurance Levels for ClinicalConnect or AGS Users	6
How are Assurance Levels defined?.....	6
How are Assurance Levels Assigned?.....	7
The Access Governance System	8
Legal Signing Authority's Use of AGS.....	8
Logging into AGS.....	9
'My Profile' Menu	11
Edit My Profile	11
'Submit Request' Menu	12
Modifying Sites.....	12
Appointing a New LRA.....	13
Adding the LRA Role to an Existing User.....	15
Revoking an LRA Appointment	16
Appointing a New Privacy Contact	17
Adding a Privacy Contact Role to an Existing User.....	19
Appointing a New Legal Signing Authority	20
Adding Agreement Signatory Role to Existing User	21
Delegating Tasks to Your Privacy Contact.....	22
Appointing a New Information Security Contact.....	23
'My Actions' Menu.....	25
Completing Pending Attestations.....	25
Other Attestation Tips.....	26
'My Activity History' Menu.....	28

Getting Started

This guide provides an overview of the Legal Signing Authority's responsibilities, with detailed instructions of how to use the Access Governance System (AGS) to support those responsibilities. The guide also reviews the Assurance Level identity verification process required by Ontario Health (Digital Services) for any user who will be provisioned with access to ClinicalConnect, or accessing Personal Health Information (PHI) through other ancillary systems used to support the operation of ClinicalConnect. Links to supporting resources and contact support are included in this guide.

As a Legal Signing Authority, your key responsibilities associated with your participation in ClinicalConnect are:

- Ensuring organization upholds the ClinicalConnect Terms & Conditions
- Revoking and appointing new Privacy Contact, Information Security Contact and Local Registration Authority (LRA) if required
- Performing semi-annual attestations of Privacy Contact and LRA(s)
- Adding/removing sites/programs covered by ClinicalConnect Terms & Conditions
- Notifying change in Legal Signing Authority if required
- Terminating Participation Agreement if required. Note that for Sole Practitioners, this includes notifying the CCPO if the physician no longer practices medicine in south west Ontario, or is no longer an active member of the College of Physicians & Surgeons of Ontario (CPSO).

Please note, for physicians who are Sole Practitioner Participants in ClinicalConnect reading this Guide, you are by default your office's one and only Local Registration Authority and Information Security Contact. You cannot replace yourself in these roles, but you can change who represents your organization as Privacy Contact as is explained in this Guide.

Support Contacts & Resources

Access Management Team

If you require assistance with your access to AGS, please contact the Access Management team at the ClinicalConnect Program Office.

Email: cc-lra@hhsc.ca

Phone: **905-521-2100 ext. 46727**

HITS Helpdesk:

If you are having technical issues with AGS or Self-Service Password Manager (SSPM) please contact the helpdesk.

Email: helpd@hhsc.ca

Phone: **905-521-2100 ext. 43000**

Training Support

If you would like additional training about how to use AGS, please email training@clinicalconnect.ca.

Highlights of Organization's Participation in ClinicalConnect

The **ClinicalConnect Participation Agreement**, and associated **Terms & Conditions**, have been designed to accommodate the changing provincial eHealth landscape, be consistent with current privacy law, and also work to align more closely with terms and conditions being utilized by Ontario Health Digital Services (OHDS) and other operators of Electronic Health Records (EHRs) in Ontario.

ClinicalConnect Agreement Framework

Three core documents comprise the framework:

1. **Participation Agreement**
2. **ClinicalConnect Terms & Conditions (T&Cs).**
3. **ClinicalConnect User Agreement (UA)**

These documents are located on the ClinicalConnect Information site and can be accessed by visiting <https://info.clinicalconnect.ca/CC/healthcare/participants>.

As the Legal Signing Authority (LSA) for your organization you signed your Participation Agreement (PA). The PA binds your organization to the Terms & Conditions that it incorporates by reference. In completing the PA, you identified the **Identity, or Account, Provider (iDP)** for your organization as one of three options:

- Hamilton Health Sciences
- Ontario Health Digital Services' ONE ID Services
- Your organization, as an Ontario Health Digital Services' federated Identity Provider




Know Your iDP

A summary of iDP options is presented here. The appointed LRAs for your organization will need to be aware of who your organization's iDP is as it determines how ClinicalConnect accounts get created and are managed for your authorized staff in your organization.

- **If Hamilton Health Sciences (HHS) is your iDP**, then HHS authorizes individuals' access to ClinicalConnect based on your LRAs' requesting accounts for your authorized users using AGS. Users can access ClinicalConnect from <https://clinicalconnect.ca>.
- **If ONE ID is your iDP**, then Ontario Health (Digital Services) authorizes ONE ID accounts that your ClinicalConnect LRA(s), submit using AGS. The ONE ID credentials themselves would originally have been created by your organization's ONE ID LRA. Users can access ClinicalConnect from <https://swo.clinicalconnect.ca>.
- Mainly only larger healthcare organizations, like hospitals, would become 'federated' to act as their own iDP, and use their own organization's credentials to access ClinicalConnect. These users can access ClinicalConnect from <https://swo.clinicalconnect.ca>.

Log into ClinicalConnect, in one of three ways:

(If you're unsure of who your Identity Provider is, [click here](#) for a list of Participants that identifies your iDP)





Identity Provider	Login Link	Identity Provider for:
	Log In	Individuals authorized to use credentials provided by HHS/their ClinicalConnect LRA.
	Log In	Individuals authorized to use their own organization's credentials to access ClinicalConnect. These individuals' organizations are Ontario Health (Digital Services) Federated Identity Providers.
	Log In	Individuals authorized to use ONE® ID credentials to access ClinicalConnect.

For more information please visit: <https://info.clinicalconnect.ca/CC/healthcare/quicklinks>

Ways to Access ClinicalConnect

There are different ways ClinicalConnect can be accessed as described below. Your ClinicalConnect LRAs are able to assign various access settings which may be configured for your organization, when creating ClinicalConnect accounts for staff. Most often, which access settings are made available, in AGS, to your LRAs is determined by you, and/or your Privacy Contact and in certain situations, require involvement from the Health Information Technology Services (HITS) technical team to configure within your organization's health information system. The chart below summarizes the different access types.

Understanding the Different Access Types

Full Access (includes Contextual Launch capability only if enabled by the organization)		Restricted Access (only if enabled by the organization)	
Web-based Access	Contextual Launch Access	Contextual Launch Only Access (Partial Restriction)	Restricted Contextual Launch Access (Full Restriction)
 www.clinicalconnect.ca	 <small>*Available in select organizations only</small>	 <small>*Available in select organizations only</small>	 <small>*Available in select organizations only</small>
<ul style="list-style-type: none"> Access via Web outside of own clinical system using external URL LRA must create account in AGS Must have username and password to log into ClinicalConnect (CC) Must use SSPM to create own permanent password 	<ul style="list-style-type: none"> Access also available from organization's clinical system (e.g. Meditech, Cerner) Organization must set up users to authenticate their CC credentials in own system Seamless launch into patient's ClinicalConnect record without a secondary log in User has ability to Search/view other patient records while in CC No additional functions required in AGS 	<ul style="list-style-type: none"> No Web Access CC access only available from organization's clinical system (e.g. Meditech, Cerner) Seamless launch into patient's ClinicalConnect record without a secondary log in User has ability to Search/view other patient records while in CC LRA must create account in AGS as "Contextual Launch Only" Organization must then set up users to authenticate their CC credentials in own system *Available in select organizations only 	<ul style="list-style-type: none"> No Web Access CC access only available from organization's clinical system (e.g. Meditech, Cerner) Seamless launch into patient's ClinicalConnect record without a secondary log in No ability to Search/view other patient records while in CC. Must return to own system and select another patient. LRA must create account in AGS as "Contextual Launch Only" and add "Restricted Contextual Launch" option Organization must then set up users to authenticate their CC credentials in own system

Full Access

When “Full Access” is mentioned in this Guide, this means that users will be able to access ClinicalConnect via the internet at <https://clinicalconnect.ca>, or at <https://swo.clinicalconnect.ca> (if ONE ID or your organization is the Identity (Account) Provider), and as well, if your organization is enabled with Contextual Launch capability, they can access the portal also from your organization’s health information system. Access from your HIS is called Contextual Launch.

Other settings are available to LRAs at select organizations (depending on their iDP and if they are enabled with Contextual Launch functionality) to further restrict how their users can access ClinicalConnect; in an effort to provide greater ability to manage how their authorized users can access their patients’ PHI in ClinicalConnect, additional access settings are available called “**Contextual Launch Only**” (CLO) and “**Restricted Contextual Launch**” (RCL). These additional settings are described below.

Contextual Launch Only and Restricted Contextual Launch options are available at select organizations that have implemented the Contextual Launch function from their health information system.

- The **Contextual Launch-Only** option allows for some users to be further restricted to access ClinicalConnect **only** from your health information system, but then have the ability to search for other patients’ Personal Health Information (PHI) once into ClinicalConnect.
- This **Restricted Contextual Launch** provides a further restriction, whereby users can only access ClinicalConnect from your health information system, but then once in the portal, don’t have the ability to search for records of patients beyond the one they were originally looking at in your HIS.

Who Decides If/How Access Restrictions are Used in Your Organization?

It’s up to Participant Organizations’ **Legal Signing Authority** and/or **Privacy Contact** to decide if and how they want their LRAs to apply the restrictions mentioned above to ClinicalConnect end users. To request information about whether these restrictions could be made available in your organization, please email support@clinicalconnect.ca.

Overview of “Under the Authority Of” (UAO) Selector and AGS

In certain circumstances, you should be aware that ClinicalConnect users in your organization may be ‘cross-authorized’ to access ClinicalConnect under authority of multiple organizations, including your own. This means they can use one set of credentials to access the portal and upon login, will be presented with an Under Authority Of (UAO) Selector screen which they must select which organization they’re accessing PHI under authority of. Once logged in, they can toggle between multiple organizations if needing to view patients registered to their other authorizing organizations. Audit reporting reflects accesses according to which organization the user selected.

Assurance Levels for ClinicalConnect or AGS Users

An Assurance Level refers to the level of confidence that can be placed in an identity claim, in other words, ‘is this person who they claim to be?’ Ontario Health (Digital Services) – or OHDS – has defined Assurance Levels based on its assessment of the applicability and appropriateness of the identity requirements corresponding to different information classifications.



Assurance Levels must be assigned when creating accounts for new users, and when appointing individuals to various roles including as Privacy Contact, Privacy Auditor and Local Registration Authority. Assurance Levels are also verified as part of the semi-annual attestations. To do this, you may need to validate with your Human Resources departments/supervisors that your organization’s onboarding of new staff includes identity validation in line with Ontario Health (Digital Services) requirements. Those requirements, including a list of acceptable documentation and related processes to verify an individual’s identity, are presented on Ontario Health Digital Services’ website.




View the ONE® ID Identity Assurance Level Standards” found on Ontario Health Digital Services’ website: <https://www.ehealthontario.on.ca/en/support-topics/one-id-lra/policy-and-standards>

How are Assurance Levels defined?

Assurance Levels are defined, per Ontario Health (Digital Services), below:

Level of Assurance	Information Classification	Description of Level of Assurance & Applicability to ClinicalConnect
AL1 Unverified Identity	AL1 is appropriate for information that has a sensitivity level of “unclassified”, and is normally used for public information and internal communications, such as internal documents and unclassified communications, normally intended for communication between staff. AL1 is insufficient when Personal Health Information (PHI) or Personal Information (PI) is accessed.	An unverified identity: An individual supplies all identification information, which is taken at face value. No assurance needed as to veracity of identity claim.  For ClinicalConnect or ancillary system access, AL1 is not acceptable.
AL2 Verified Identity	AL2 is appropriate for information that has a high sensitivity level within OHDS and the health sector environment, and that is intended for use by specific and authorized individuals only. If compromised, this information could reasonably be expected to cause serious injury or financial losses to one or more of the parties involved or would require legal action for correction. View the ONE® ID Identity Assurance Level Standards” found on OHDS’ website: https://www.ehealthontario.on.ca/en/support-topics/one-id-lra/policy-and-standards	A verified identity: An individual is uniquely identified through a managed registration process and identity claim is verified with documentary evidence, which may be supplemented by contextual evidence in appropriate circumstances.  For ClinicalConnect or ancillary system access, AL2 is acceptable/required. Also note that all ClinicalConnect Privacy Contacts and Privacy Auditors must have their identity verified as they too must be designated as AL2, since they’ll be granted access to ClinicalConnect’s Security Audit Manager (SAM) online tool.

Level of Assurance	Information Classification	Description of Level of Assurance & Applicability to ClinicalConnect
AL3 Corroborated Identity	<p>AL3 is appropriate for information that is extremely sensitive and of the highest value within OHDS and the health sector environment. This information is intended for use by named and authorized individuals only.</p> <p>Additional information to assign AL3: Identity must be corroborated where an AL3 is required. Identity corroboration may either be by:</p> <ul style="list-style-type: none"> • Direct verification by an Authoritative Party (e.g., Vital Statistics Agency, Revenue Canada); and/or • A trusted third-party professional (e.g., lawyer, doctor, minister). <p>All identity documents for AL3 must contain a photograph of the End User:</p> <ul style="list-style-type: none"> • A copy of the identity document must be taken and retained on record; and <p>End Users must sign their Registration application with a handwritten signature, in accordance with the organization's policies and procedures.</p>	<p>A corroborated identity: An individual is uniquely identified through a managed registration process and identity claim is verified and corroborated with authoritative source(s) (e.g. the issuer of the documentary evidence presented).</p> <p> For ClinicalConnect or ancillary system access, AL3 is acceptable. Note that AL3 does not give the user access to any additional personal health information from that of an AL2.</p>

How are Assurance Levels Assigned?

Like your LRAs when requesting ClinicalConnect accounts for your staff, you'll be prompted to assign an Assurance Level (AL) when appointing individuals to certain roles using AGS. You must be confident that through your organization's onboarding process, the identity of the individual has been verified in line with OHDS' definitions and processes, such that they can assign an AL2 or higher.

Assurance Levels Summary

- Should an Assurance Level need to change from what displays for each user in AGS, this can be updated in AGS under the "Modify User Properties" function.
- If at any point, an AL is changed to a '1', the user's access to ClinicalConnect or the ancillary system, such as the Security Audit Manager, will automatically be disabled since access to ClinicalConnect requires a '2' or higher.

The Access Governance System

The Access Governance System (AGS) is a web portal that is used to centrally manage and automate common account management processes for ClinicalConnect accounts. The portal is hosted by Hamilton Health Sciences and allows LRAs to request, approve, review, attest and fulfill ClinicalConnect accounts in a user friendly, secure and efficient manner.

AGS is compatible with Internet Explorer 9+ or Mozilla Firefox.

Key Features of AGS

- Validates information submitted by users during account request process
- Intelligently route requests and approvals to appropriate recipients
- Offers content-rich ClinicalConnect account management reports

Benefits of AGS

- Improves end user experience when requesting access to ClinicalConnect accounts
- Provides quick turnarounds for account management requests such as additions/modifications/deletions
- Manages inactive accounts efficiently
- Provides the ability for key ClinicalConnect 'roles' to review accounts and key appointments in accordance with the Participation Agreement

Legal Signing Authority's Use of AGS

This guide explains how Legal Signing Authorities (LSAs) typically use AGS to perform the following duties:

- Appointing/Revoking new Privacy Contact (PC), Information Security Contact (ISC) and Local Registration Authorities (LRAs)
- Performing semi-annual attestations of your organization's PC, ISC and LRAs
- Adding or removing sites, if your organization has more than one site accessing ClinicalConnect
- Updating your contact information as the Legal Signing Authority (LSA)
- Replacing yourself as the Legal Signing Authority (LSA)
- Delegating the task of appointing and revoking LRAs to your organization's Privacy Contact

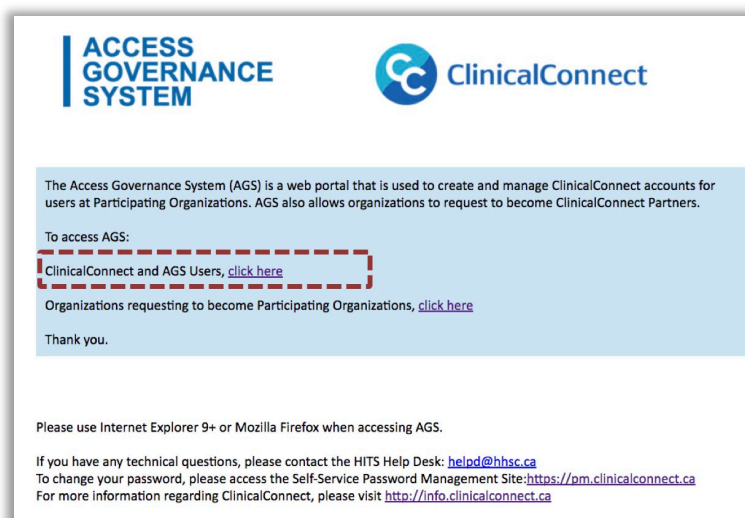
Note that you cannot request to terminate your participation in ClinicalConnect using AGS. You must submit that request in writing to the ClinicalConnect Program Office by emailing agreements@clinicalconnect.ca.

Logging into AGS

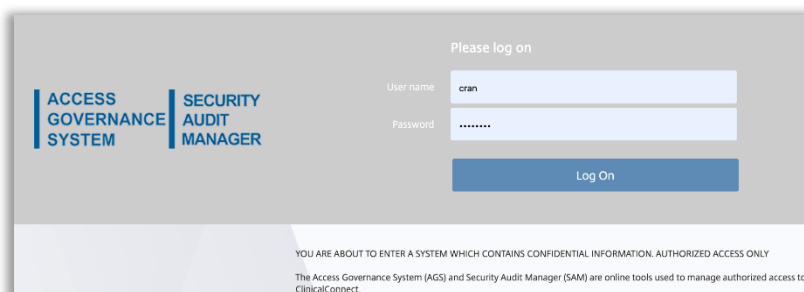
To access AGS, type the following URL: <https://ags.clinicalconnect.ca>

AGS is compatible with Internet Explorer 9+ or Mozilla Firefox.

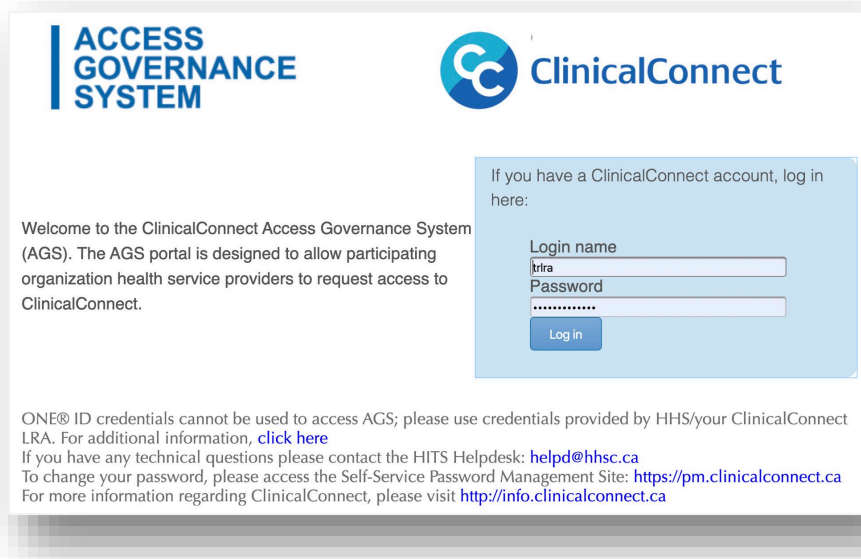
1. Select 'ClinicalConnect and AGS users'



2. You'll be prompted to enter your AGS username and password on the screen below. If you are unsure of your login credentials, please contact the Access Management Team at cc-lra@hhsc.ca or by phone at 905-521-2100 ext. 46727.

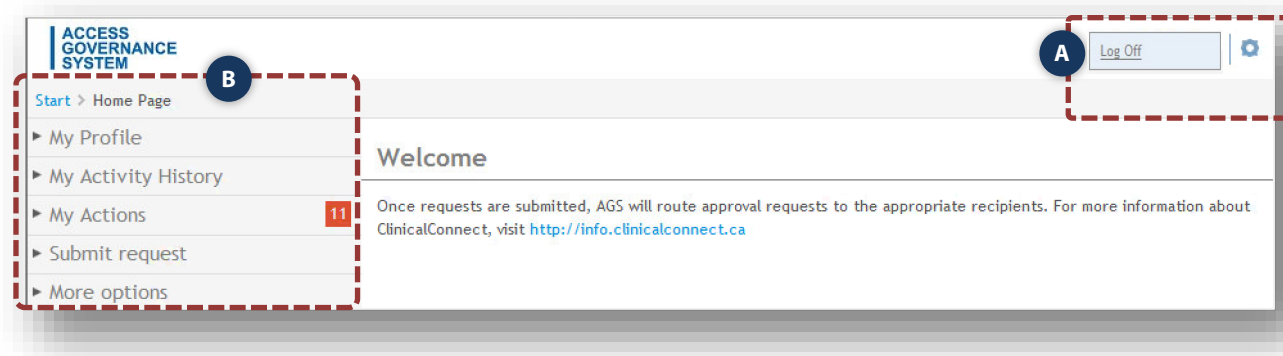


3. Enter your login credentials again into the AGS login screen.



4. The AGS landing page will display your name in the top right corner of the screen **(A)**. The drop down arrow beside your name will display the 'Log Off' function. Ensure you log out of AGS when you're finished your work.

The main AGS menu options are located on the left **(B)** side of the screen. Your menu may contain notification indicators in the section called 'My Actions', as shown in the image below if you have pending action items waiting for you to complete.

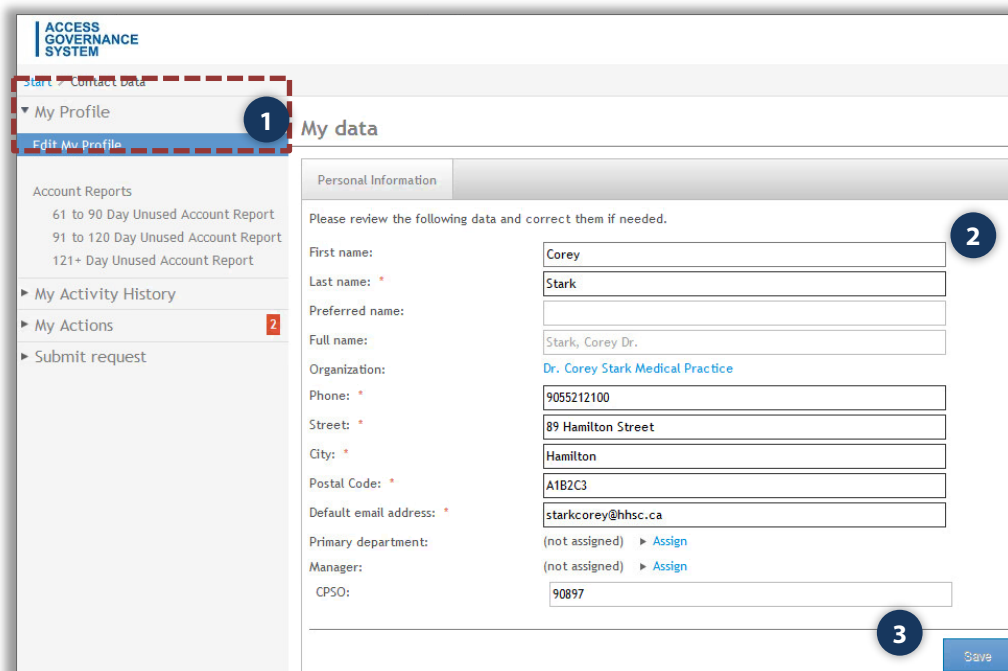


'My Profile' Menu

Edit My Profile

LSAs can update their own profile in AGS if their contact information changes. A name change request will notify ClinicalConnect's Access Management Team to review/approve the request, then the LSA will receive an email confirming that their name and their username have been changed. It is important to keep your profile current.

1. To edit your profile, select **'My Profile'** then select **"Edit My Profile"**.
2. Update the information available on the screen.
3. Click **'Save'** to submit the changes.



ACCESS GOVERNANCE SYSTEM

Start > Contact data

▼ My Profile

Edit My Profile

Account Reports

- 61 to 90 Day Unused Account Report
- 91 to 120 Day Unused Account Report
- 121+ Day Unused Account Report

► My Activity History

► My Actions

► Submit request

My data

Personal Information

Please review the following data and correct them if needed.

First name: Corey

Last name: Stark

Preferred name:

Full name: Stark, Corey Dr.

Organization: Dr. Corey Stark Medical Practice

Phone: 9055212100

Street: 89 Hamilton Street

City: Hamilton

Postal Code: A1B2C3

Default email address: starkcorey@nhsc.ca

Primary department: (not assigned) ▶ Assign

Manager: (not assigned) ▶ Assign

CPSO: 90897

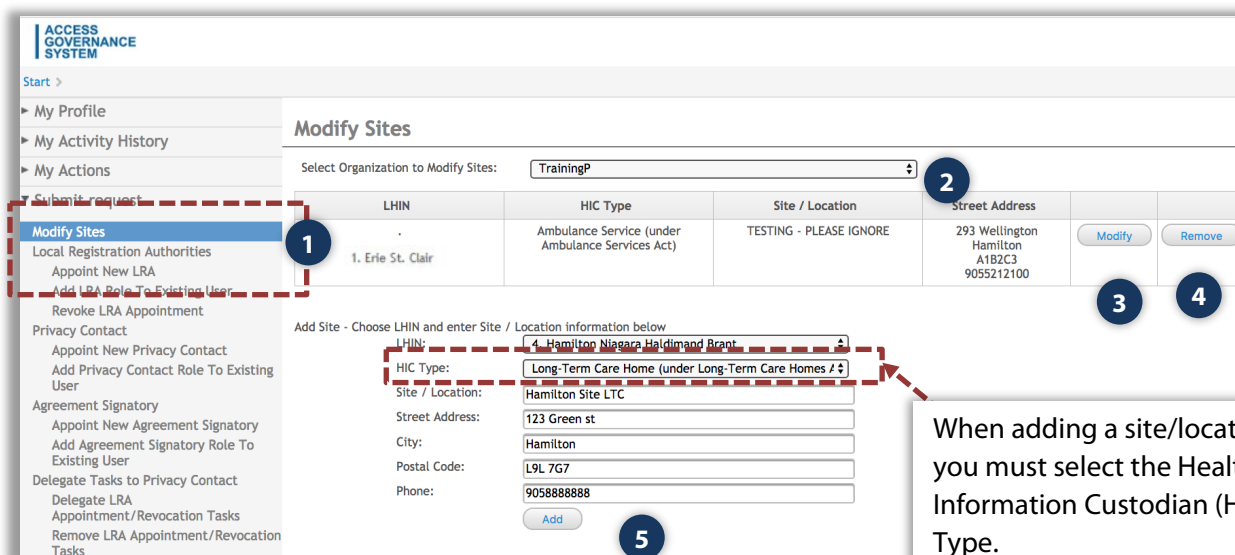
Save

'Submit Request' Menu

Modifying Sites

LSAs must keep their Participation Agreement current by appropriately adding, removing or modifying their organization's sites/locations in a timely manner using AGS. LSAs must always list the sites or locations where users can access ClinicalConnect and must **'Add a Site'** in cases where the organization acquires or builds a new facility and would like users at that new site to have access to ClinicalConnect as appropriate. Similarly, the LSA must **'Remove a Site'** if they no longer operate it or do not want health service providers at that site to access ClinicalConnect, or **'Modify a Site'** to change its name, or contact information. All site additions or modifications will trigger an approval process and the LSA will be notified if their requested change is approved or denied.

1. To modify your site information, select the **"Submit Request"** menu option, then select **"Modify Sites"**.
2. Select the organization to display a list of the approved sites associated with the select organization.
3. Select **"Modify"** to change the site/location and address information.



ACCESS GOVERNANCE SYSTEM

Start >

- My Profile
- My Activity History
- My Actions
- Submit request
 - Modify Sites**
 - Local Registration Authorities
 - Appoint New LRA
 - Add LRA Role To Existing User
 - Revoke LRA Appointment
 - Privacy Contact
 - Appoint New Privacy Contact
 - Add Privacy Contact Role To Existing User
 - Agreement Signatory
 - Appoint New Agreement Signatory
 - Add Agreement Signatory Role To Existing User
 - Delegate Tasks to Privacy Contact
 - Delegate LRA
 - Appointment/Revocation Tasks
 - Remove LRA Appointment/Revocation Tasks

Modify Sites

Select Organization to Modify Sites: TrainingP

LHIN	HIC Type	Site / Location	Street Address		
1. Erie St. Clair	Ambulance Service (under Ambulance Services Act)	TESTING - PLEASE IGNORE	293 Wellington Hamilton A1B2C3 9055212100	Modify	Remove

Add Site - Choose LHIN and enter Site / Location information below

LHIN: 4. Hamilton Niagara Haldimand Brant

HIC Type: Long-Term Care Home (under Long-Term Care Homes /)

Site / Location: Hamilton Site LTC

Street Address: 123 Green st

City: Hamilton

Postal Code: L9L 7G7

Phone: 9058888888

Add

When adding a site/location, you must select the Health Information Custodian (HIC) Type.

4. **Removing a site:** Select the site to remove and confirm your selection.



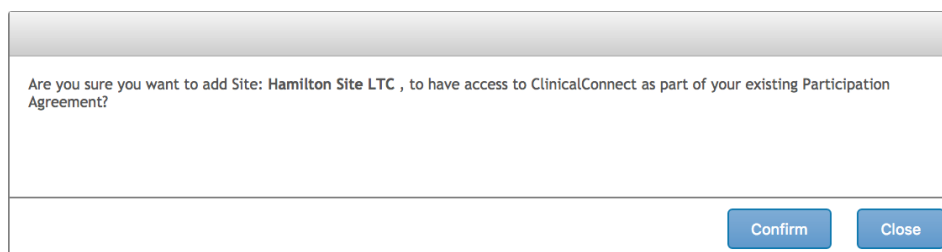
Confirmation

Second new Address A2 has been selected to be removed, are you sure?

Request Cancel

! About Removing Site(s): The LRA(s) for your organization will receive notification that the site has been removed and to verify users in your organization that should still have access to the portal. Also, the LSA cannot remove the last site from their Agreement as this would effectively terminate their participation in ClinicalConnect. A request to take that action must be emailed to agreements@clinicalconnect.ca.

5. Adding a Site: Select the LHIN and enter the site name, location and address information.



Are you sure you want to add Site: Hamilton Site LTC , to have access to ClinicalConnect as part of your existing Participation Agreement?

Confirm Close

Confirm your addition. The new site will appear in the site list, but cannot be modified or removed until it has been formally approved and the LSA has been notified. If denied, the site will be removed from the list.

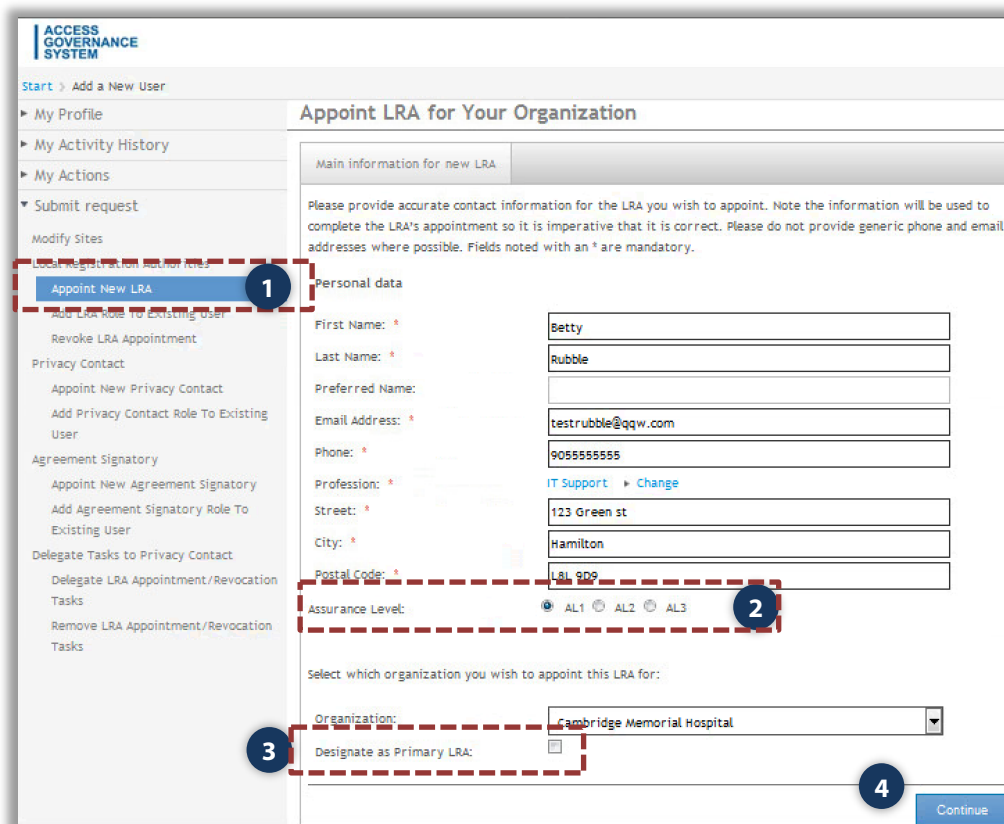
Appointing a New LRA

Once your organization's Participation Agreement is fully approved, the LSA is required to appoint a **Primary** and a **Backup LRA** for their organization. A Participant can have multiple LRAs, but must always have at least one LRA. The LRAs are responsible for creating and managing accounts on an ongoing basis for the organization. As part of the appointment process, the LSA will be required to identify which LRA will be considered their Primary LRA. Being the Primary LRA simply means their name and email address are included on the welcome message to new end users in your organization as accounts are created, as a main point of contact if required.

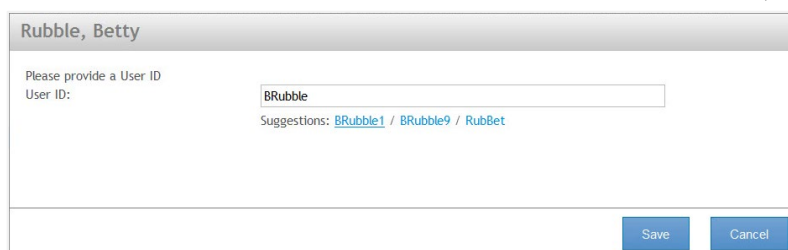
An LSA who has authority over multiple organizations can '**cross-appoint**' an LRA to cover more than one of their organizations. This appointment can be assigned when "**Appointing a New LRA**" or by "**Add LRA Role to Existing User**" shown further in the user guide.

To appoint an LRA for your organization:



1. Select "**Submit Request**", then "**Appoint LRA**" and complete the required fields.
2. **Assurance Levels** must be assigned when creating a new user. Please refer to the [Assurance Level information](#) in this guide to determine the appropriate level to assign.



3. **Primary LRA:** If the appointed LRA will be the Primary LRA, please select the check box. If a Primary LRA already exists, you will be prompted to override this and assign the new LRA as the primary.
4. Complete all the required fields and click **"Continue"**.
5. Select a **username** from the suggestions provided, or enter your own variation (if the username is available), then click **'Save'**. If the username is available, AGS will allow you to save the information. You must provide the LRA with the username, and a temporary password will be emailed to them.



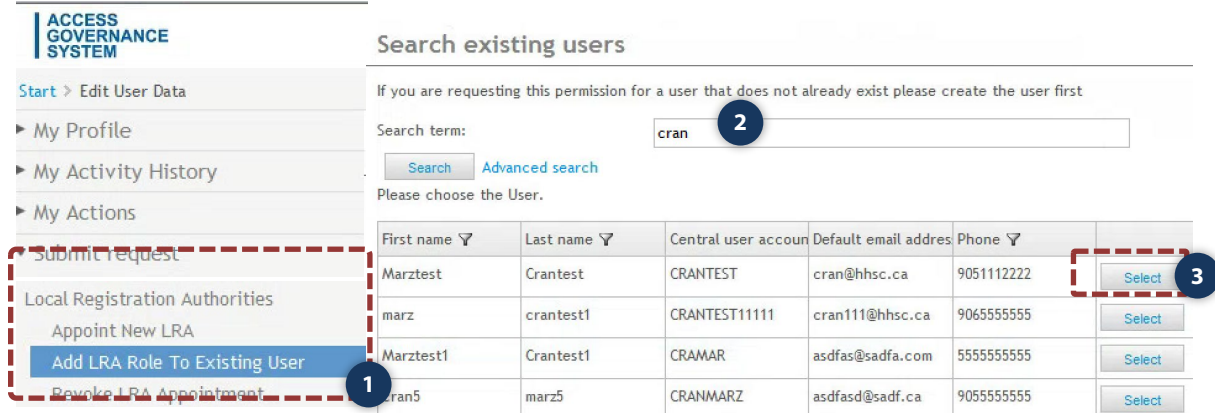
6. Once the information is saved, you will receive a confirmation message indicating that the account has been successfully requested. Once the LRA appointment has been submitted, the LRA will receive notification of their new appointed role and instructions regarding the LRA orientation pathway.

 Your request to appoint a new LRA for your organization has been received and the LRA will be contacted 

Adding the LRA Role to an Existing User

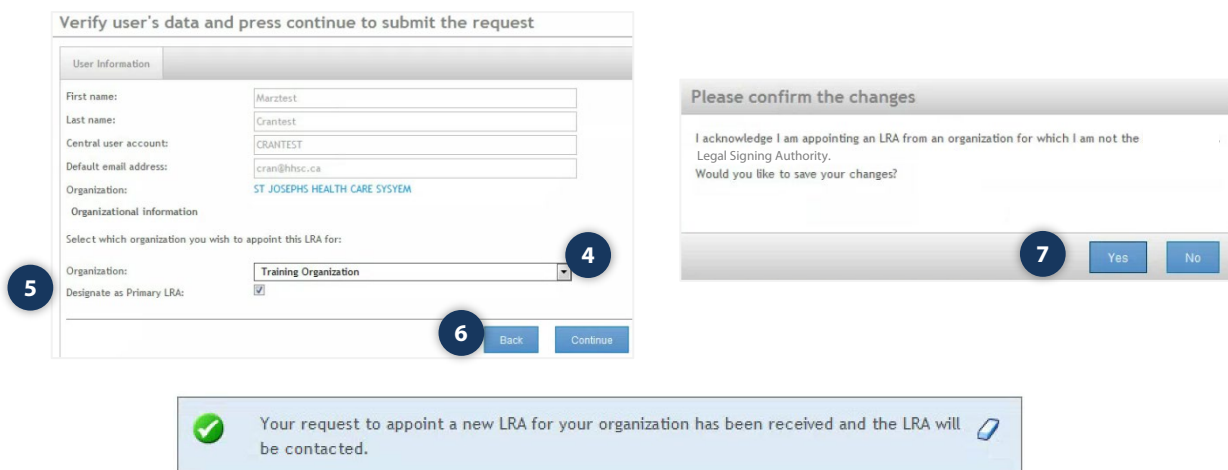
The LSA can add the LRA role to an existing user in their organization, or from another organization. This may be useful if adding a backup or replacement LRA, and in situations where organizations may be sharing an LRA. The new LRA will be notified by email of their appointment and will be required to complete the LRA Orientation before they can create and manage accounts using AGS.

1. Select **"Add LRA Role to Existing User"** from the menu.
2. Use the Search field to search for the user.
Search format: Last name, First name or a combination Last name, (comma, space) First name e.g. Smith, Jane. You may use the Advanced Search function to narrow your search results.
3. Select the user you wish to appoint as an LRA. Validate that you have selected the correct user.



First name ▼	Last name ▼	Central user account	Default email address	Phone ▼	
Marztest	Crantest	CRANTEST	cran@hhsc.ca	9051112222	Select
marz	crantest1	CRANTEST11111	cran111@hhsc.ca	9065555555	Select
Marztest1	Crantest1	CRAMAR	asdfas@sadfa.com	5555555555	Select
cran5	marz5	CRANMARZ	asdfasd@sadf.ca	9055555555	Select

4. **Organization:** Use the drop down to select the organization that this LRA will be appointed to support.
5. **Primary LRA:** If the appointed LRA will be the Primary LRA, select the check box. If a Primary LRA already exists, you will be prompted to override this and assign the new LRA as the primary (see below).
6. Click **"Continue"**.
7. In cases where the LSA is appointing an LRA from an organization for which he/she is not the LSA, the following confirmation prompt will display.



Verify user's data and press continue to submit the request

User Information

First name: Marztest

Last name: Crantest

Central user account: CRANTEST

Default email address: cran@hhsc.ca

Organization: ST JOSEPHS HEALTH CARE SYSTEM

Organizational information

Select which organization you wish to appoint this LRA for:

Organization: Training Organization

Designate as Primary LRA: ☒

Back Continue

Please confirm the changes

I acknowledge I am appointing an LRA from an organization for which I am not the Legal Signing Authority.

Would you like to save your changes?

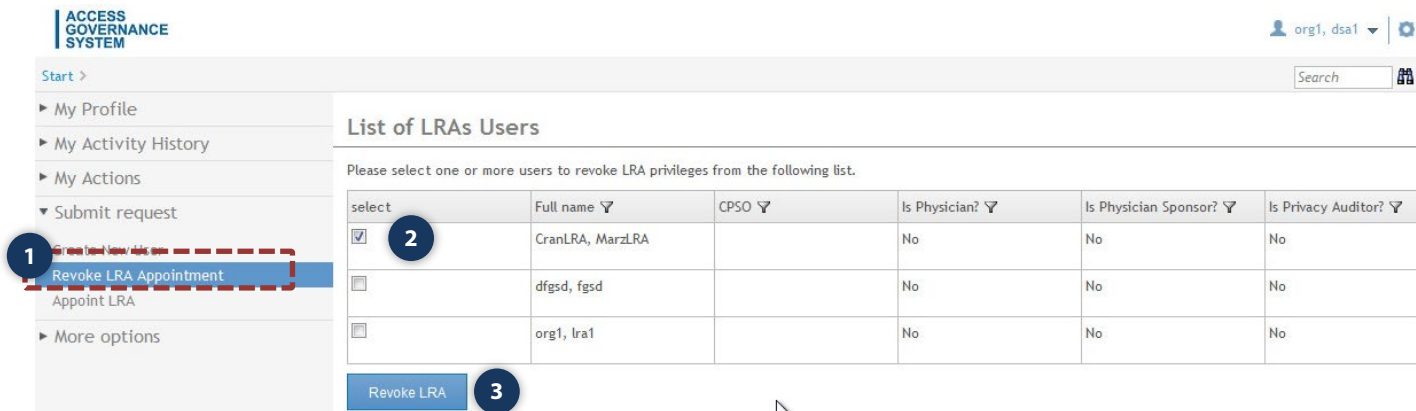
Yes No

✓ Your request to appoint a new LRA for your organization has been received and the LRA will be contacted.

Revoking an LRA Appointment

The LSA must also revoke an LRA appointment if the LRA is no longer in the role, or has left the organization.

1. Select **'Revoke LRA Appointment'** from the menu. A list of appointed LRAs for your organization will display.
2. Select the LRA you wish to revoke privileges for. Click **"Revoke LRA"**.



The screenshot shows the ACCESS GOVERNANCE SYSTEM interface. On the left, a sidebar menu has 'Revoke LRA Appointment' highlighted with a red dashed box and a blue circle labeled '1'. The main area is titled 'List of LRAs Users' and contains a table with columns: 'select', 'Full name', 'CPSO', 'Is Physician?', 'Is Physician Sponsor?', and 'Is Privacy Auditor?'. The first row is selected, indicated by a checked checkbox and a blue circle labeled '2'. At the bottom of the table, there is a blue button labeled 'Revoke LRA' with a blue circle labeled '3' next to it.

select	Full name	CPSO	Is Physician?	Is Physician Sponsor?	Is Privacy Auditor?
<input checked="" type="checkbox"/>	CranLRA, MarzLRA		No	No	No
<input type="checkbox"/>	dfgsd, fgsd		No	No	No
<input type="checkbox"/>	org1, lra1		No	No	No

Once the LRA appointment has been revoked, the LRA will receive notification of the revocation and their access to AGS as an LRA, as well as to the LRA SharePoint site, will be removed.

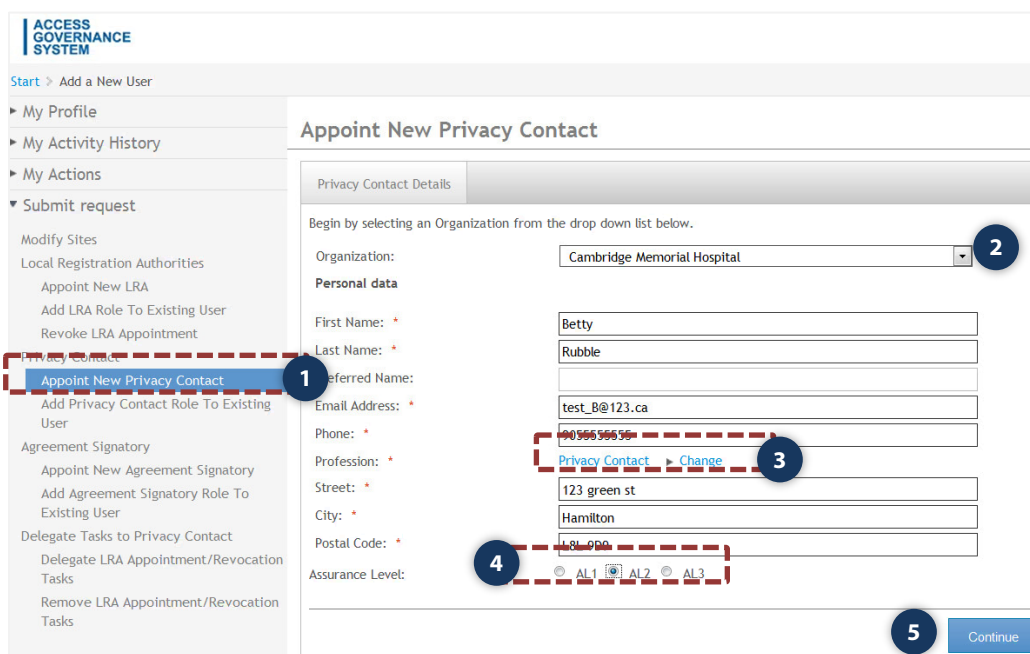
Appointing a New Privacy Contact

The LSA may appoint a new Privacy Contact (PC) if the existing PC needs to be replaced. An organization must have one PC appointed at all times. The new PC will receive an email notification from ClinicalConnect Access Governance System of their appointment.

! When appointing a new PC, the LSA will be prompted to confirm they want to revoke the previous PC and appoint someone new. Also note that all new Privacy Contacts are required to complete an orientation to their role, offered as an eLearning module. They receive instructions to complete this module once appointed by you.

To appoint a new Privacy Contact:

1. From the **'Submit Request'** menu, select **'Appoint New Privacy Contact.'**
2. Select the organization from the drop down and complete the required fields
3. Select 'Privacy Contact' in the profession field.
4. **Assurance Levels** must be assigned when creating a new user. Please refer to the Assurance Level information to determine the appropriate level to assign.
5. Select **'Continue'**.



6. If a Privacy Contact already exists, the following message will display. Select 'Yes' to continue. Select 'No' to end the process and return to the previous screen.

Privacy Contact Replacement

Warning! Assigning a new Privacy Contact for CAMBRIDGE MEMORIAL HOSPITAL will revoke the existing Privacy Contact: Mitchell Abrams. Continue with the Privacy Contact Replacement?

6
Yes
No

7. Select a username option from the provided suggestions or enter your own variation then select **"SAVE."** If the username is available, AGS will allow you to save the information and present a confirmation message.


Rubble, Betty

Please provide a User ID
User ID:


BRubble

Suggestions: [BRubble1](#) / [BRubble9](#) / [RubBet](#)

7
Save
Cancel



The new person Rubble, Betty was successfully added and is appointed as Privacy Contact for CAMBRIDGE MEMORIAL HOSPITAL.



The new PC will receive an email from the ClinicalConnect Access Governance System, notifying them of their appointment and instructions to complete their orientation to the role of Privacy Contact.

Adding a Privacy Contact Role to an Existing User

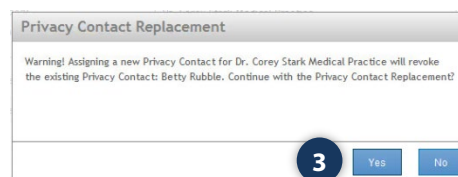
Another way to appoint a new Privacy Contact is to Similar to add the role of PC to someone who already has access to ClinicalConnect, using the option 'Add Privacy Contact Role to an Existing User'.

1. Under **"Submit Request"**, select **"Add Privacy Contact Role to an Existing User"**. Your Organization name will display in the first field.
2. Leave the search field blank and click **'Search'** to display a list of users. From this list, select who you'd like to appoint as the new PC.

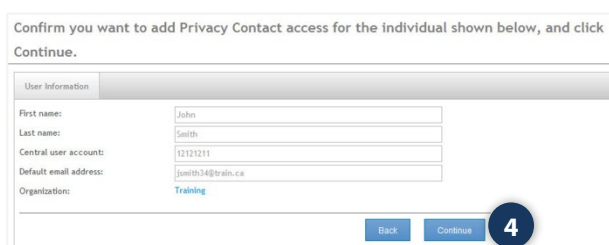


First name	Last name	Central user account	Organization	Default email address	Phone	
John	Smith	12121211	Training	jsmith34@train.ca	1112221234	Select
as333333	33waerae	A33WAERAE	CAS Healthcare	asdfas@asdfadsf.com	9055212100	Select
Adam	Ant	AANT	Training	adam@anthill.com	555222323	Select
asdfas	asdf	AASDF	Training	ksadmfkj@test.com	9059990000	Select
testFirst	testLast	ACCOUNT\TEST.USERNA	SOUTHWEST CCAC - P	test@swactest.ca	9055212100	Select

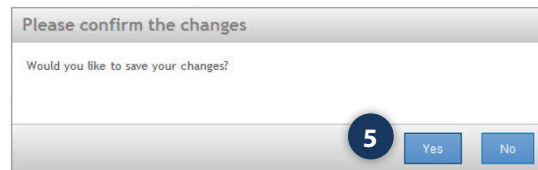
3. The following message will display. Select **"Yes"** to continue with the PC appointment or select **"No"** to end the process and return to the previous screen.



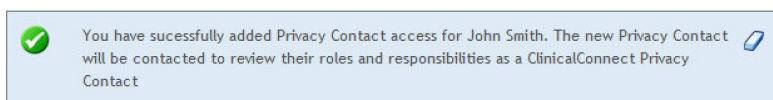
4. Confirm that the user you've selected should be appointed as the new PC and click **"Continue"**.



5. Confirm the changes.



The new PC will receive an email from the ClinicalConnect Access Governance System, notifying them of their appointment and instructions to complete their orientation to the role of Privacy Contact (if they aren't already the Privacy Contact of another ClinicalConnect Participant Organization).

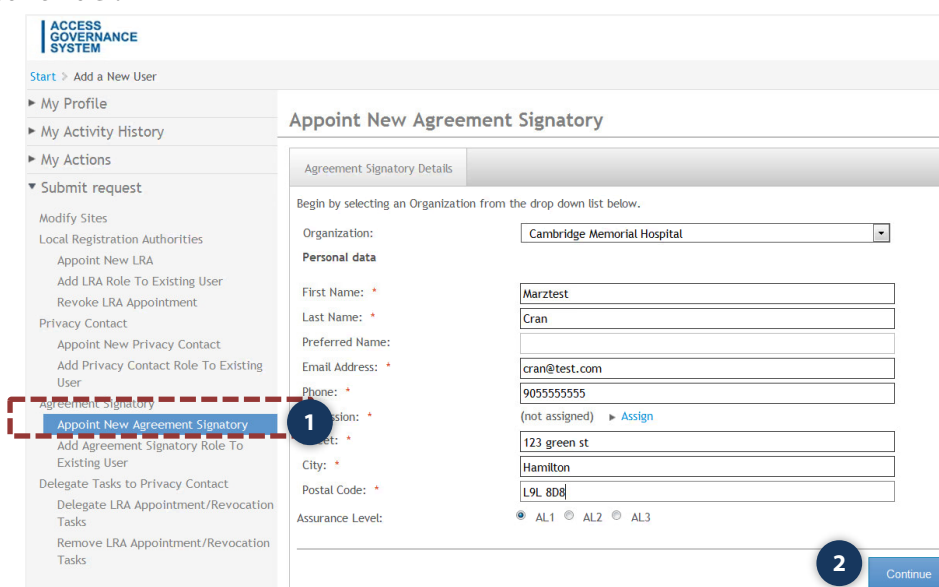


Appointing a New Legal Signing Authority

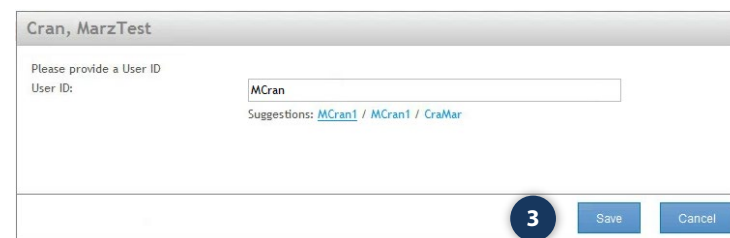
In some cases where an organization's LSA may need to be changed, the current LSA can appoint someone new to fill that role using AGS. This process is used if the new LSA does not already have access to AGS. If the user already has access to AGS, please refer to the next process "**Add Agreement Signatory Role to Existing User**".



Note: In situations where an LSA leaves the organization and a replacement LSA has not been appointed using AGS, the replacement LSA must email agreements@clinicalconnect.ca indicating they now hold that role, include their contact information, and then they will be contacted with their AGS credentials in order to resume the duties of the previous signatory.

1. Select '**Appoint New Agreement Signatory**' and complete the required fields.
2. Click '**Continue**'.



3. Select a username option from the provided suggestions or enter your own variation then select "**SAVE.**" If the username is available, AGS will allow you to save the information.



 The new person Cran, MarzTest was successfully added and approval workflow will be launched to appoint this user as DSA Signatory for Training. 

The new LSA will receive an email notification from ClinicalConnect Access Governance System of their appointment.

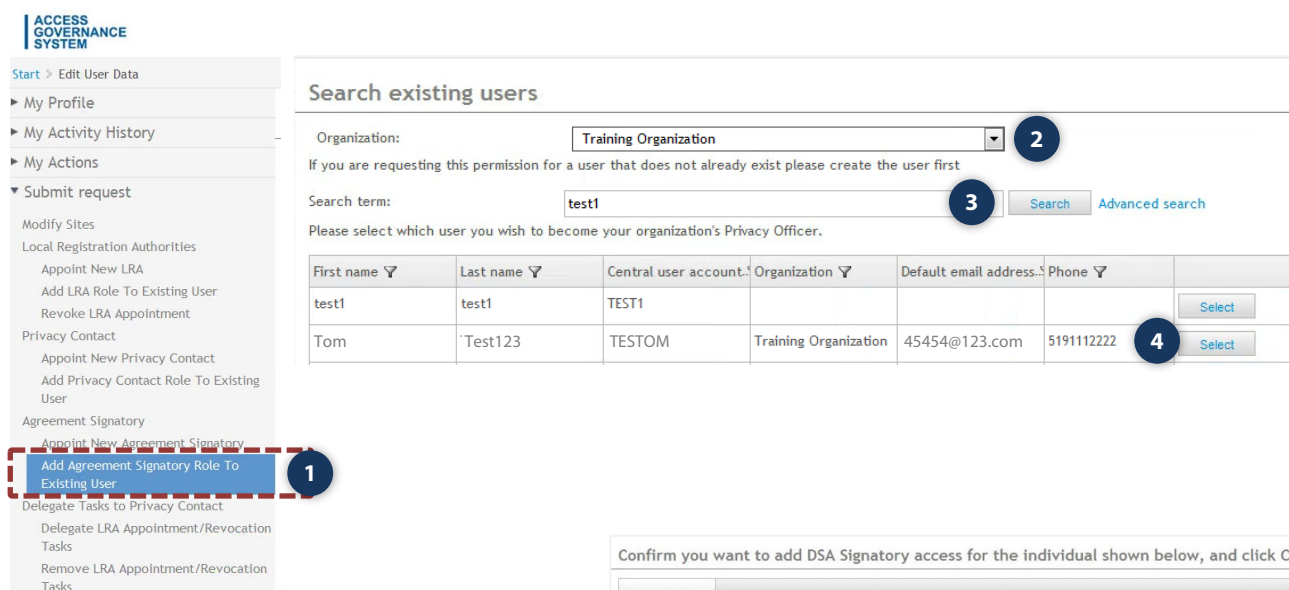
Adding Agreement Signatory Role to Existing User

In some cases where an organization's LSA may need appoint someone who already holds the a ClinicalConnect-related role for another organization, so is an **existing user** of ClinicalConnect and/or AGS.

1. Select 'Add Agreement Signatory Role to Existing User'.
2. Select the organization from the drop down.
3. Use the Search field to search for the user.

Search format: Last name, First name or a combination Last name, (comma, space) First name e.g. Smith, Jane. You may use the Advanced Search function to narrow your search results.

4. Select the user.



ACCESS GOVERNANCE SYSTEM

Start > Edit User Data

- My Profile
- My Activity History
- My Actions
- Submit request
 - Modify Sites
 - Local Registration Authorities
 - Appoint New LRA
 - Add LRA Role To Existing User
 - Revoke LRA Appointment
 - Privacy Contact
 - Appoint New Privacy Contact
 - Add Privacy Contact Role To Existing User
 - Agreement Signatory
 - Appoint New Agreement Signatory
 - Add Agreement Signatory Role To Existing User** (1)
 - Delegate Tasks to Privacy Contact
 - Delegate LRA Appointment/Revocation Tasks
 - Remove LRA Appointment/Revocation Tasks

Search existing users

Organization: Training Organization (2)

If you are requesting this permission for a user that does not already exist please create the user first

Search term: test1 (3) Search Advanced search

Please select which user you wish to become your organization's Privacy Officer.

First name ▼	Last name ▼	Central user account ▼	Organization ▼	Default email address ▼	Phone ▼	
test1	test1	TEST1				Select
Tom	Test123	TESTOM	Training Organization	45454@123.com	5191112222	Select (4)

5. Confirm the user's information and select "Continue".



Confirm you want to add DSA Signatory access for the individual shown below, and click Continue.

User Information

First name: Tom

Last name: Test123

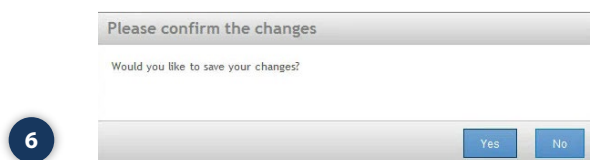
Central user account: TESTOM

Default email address: 45454@123.com

Organization: Training Organization

Back Continue (5)

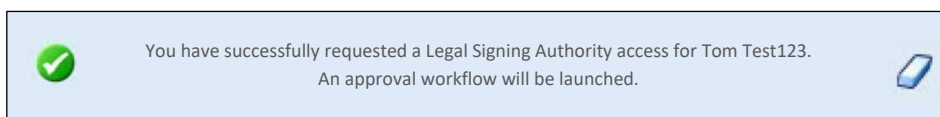
6. Confirm the selection. The new LSA will receive an email notification from ClinicalConnect Access Governance System of their appointment.





Please confirm the changes

Would you like to save your changes?

Yes No (6)



 You have successfully requested a Legal Signing Authority access for Tom Test123. An approval workflow will be launched. 

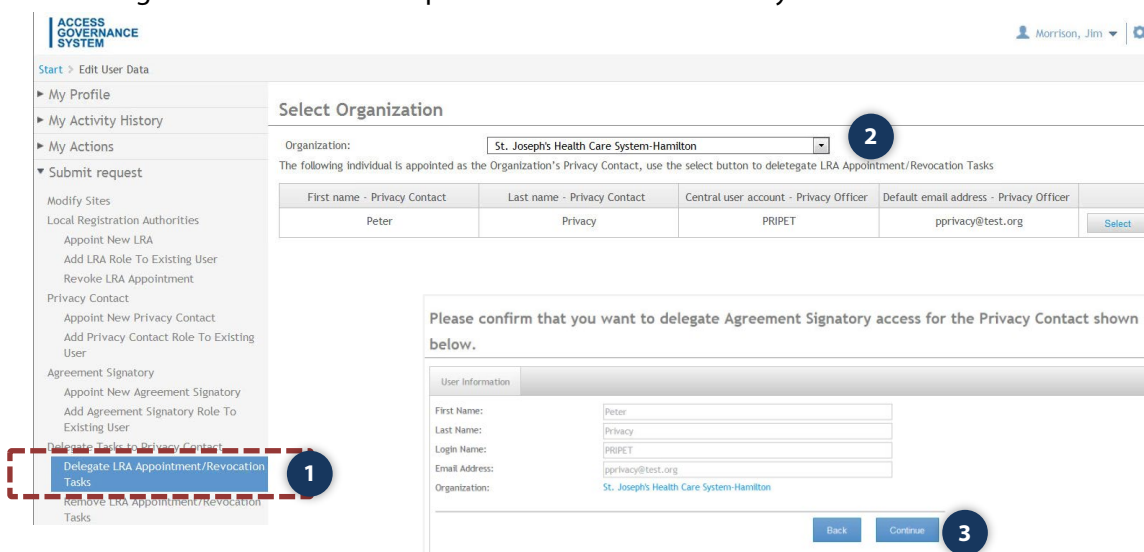
Delegating Tasks to Your Privacy Contact

Please note this section does not apply to physicians who are approved as Sole Practitioner Participants in ClinicalConnect.

In some cases, an LSA of an organization may wish to delegate their responsibilities with respect to appointing and revoking LRAs to their organization's Privacy Contact. These are the only tasks that may be delegated by the LSA to the Privacy Contact.

Note: The task of *attesting* the LRAs each cycle (May 1 and November 1) continues to be the responsibility of the LSA.

1. Select **"Delegate LRA Appointment/Revocation Tasks"**
2. Select the organization from the drop down and select the Privacy Contact.



ACCESS GOVERNANCE SYSTEM

Start > Edit User Data

My Profile

My Activity History

My Actions

Submit request

Modify Sites

Local Registration Authorities

Appoint New LRA

Add LRA Role To Existing User

Revoke LRA Appointment

Privacy Contact

Appoint New Privacy Contact

Add Privacy Contact Role To Existing User

Agreement Signatory

Appoint New Agreement Signatory

Add Agreement Signatory Role To Existing User

Delegate tasks to Privacy Contact

Delegate LRA Appointment/Revocation Tasks

Remove LRA Appointment/Revocation Tasks

Morrison, Jim

Select Organization

Organization: St. Joseph's Health Care System-Hamilton

The following individual is appointed as the Organization's Privacy Contact, use the select button to delegate LRA Appointment/Revocation Tasks

First name - Privacy Contact	Last name - Privacy Contact	Central user account - Privacy Officer	Default email address - Privacy Officer	
Peter	Privacy	PRIPET	pprivacy@test.org	Select

Please confirm that you want to delegate Agreement Signatory access for the Privacy Contact shown below.

User Information

First Name: Peter

Last Name: Privacy

Login Name: PRIPET

Email Address: pprivacy@test.org

Organization: St. Joseph's Health Care System-Hamilton

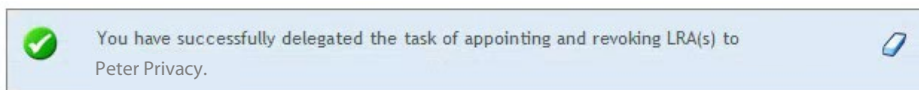
Back Continue

3. Confirm your selection and click **"Continue"**.

Please confirm the changes

Would you like to save your changes?

Yes No



The Privacy Contract, to whom the task of appointing/revoking LRAs has been delegated, will be notified that they now have the option to perform these tasks in AGS. The LSA also maintains their ability to appoint/revoke LRAs, even if these tasks are delegated.

Appointing a New Information Security Contact

LSAs are also responsible for managing the appointment of your organization's **Information Security Contact (ISC)**. The role of Information Security Contact (ISC) is required by all ClinicalConnect Participant Organizations.

A summary of the ISC role is provided below:

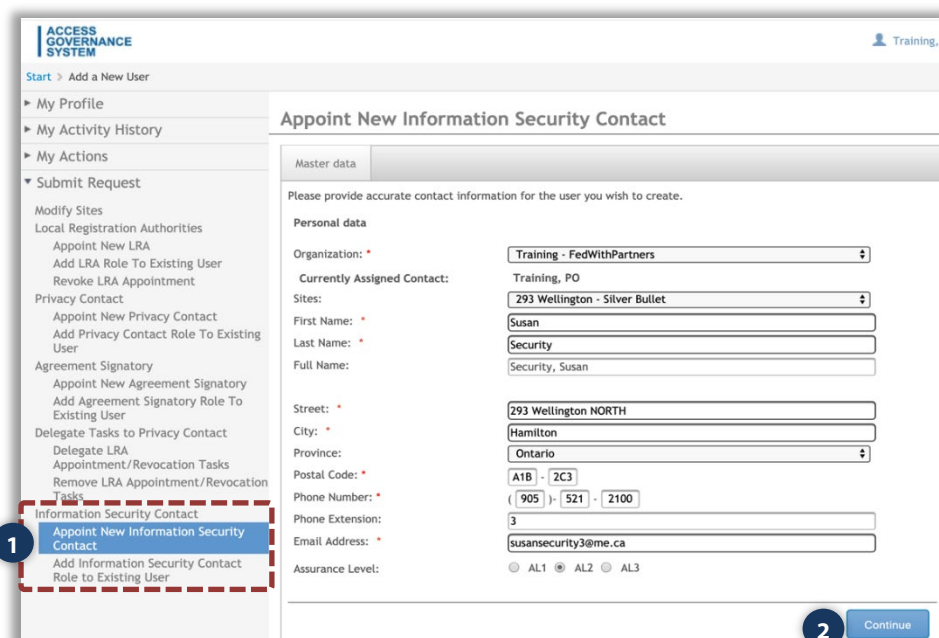
- Managing information security matters related to the use of ClinicalConnect at the organization.
- Ensuring reporting of applicable information security incidents in compliance with the ClinicalConnect Information Security Incident Management policy.

To update your ISC appointment:

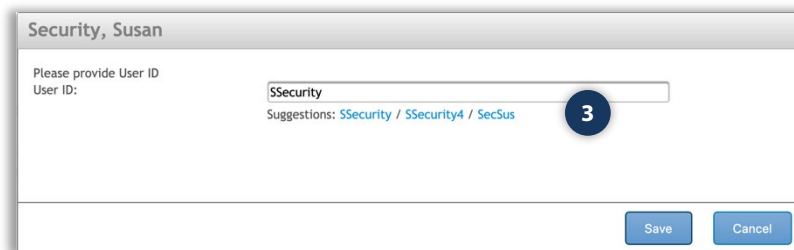
1. Select '**Appointment New Information Security Contact**'

NOTE: If you want to appoint a person to the role of an ISC and they already have AGS access (e.g. they are your Privacy Contact or an LRA) then you can use the option '**Add Information Security Contact Role to Existing User**' instead. If your organization has multiple sites, your appointed ISC will oversee all of the sites associated with your organization. You do not need to appoint an ISC for each site

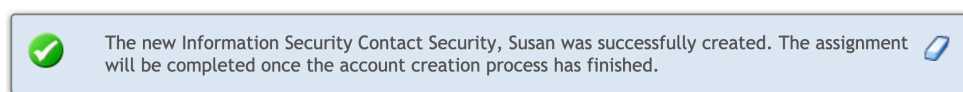
2. Complete the required fields then click '**Continue**'.



3. Select a username from the suggestions provided, or enter your own variation (if the username is available), then click **'Save'**. If the username is available, AGS will allow you to save the information. You must provide the users with the username, and a temporary password will be emailed to them.



Once the information is saved, you will receive a confirmation message indicating that the account has been successfully requested.



The new ISC will receive an email notification from ClinicalConnect Access Governance System of their appointment and their login credentials that provides them with access to the ISC SharePoint site where they will find the ClinicalConnect Security Policies.

'My Actions' Menu

Completing Pending Attestations

What are Attestations?

"Attestation" refers to the practice of periodically checking and certifying that only the individuals who need certain access privileges to ClinicalConnect and/or AGS have those access privileges. As the LSA for your organization, you're responsible to attest that your Privacy Contact, Information, Security Contact and your Local Registration Authorities (LRAs) still holds those roles.

Attestation Notification Schedule

LSAs will receive email notifications with instructions to perform their attestations every **May 1** and **November 1**. Attestations must be completed in a timely basis to avoid having the individuals' access disabled.

- LSA will receive a reminder email if the attestations are **not complete within 2 weeks** of receiving the initial notification.
- If attestations are **not complete within 4 weeks** of receiving the initial notification, an escalation email is sent to the organization's Privacy Contact.
- If attestations are **not complete within 6 weeks**, LSAs will receive final warning to complete attestations within the next two weeks and failure to do so will result in automatic revocation of PC and LRA appointments and corresponding access to AGS.

An example of the email notification regarding semi-annual attestations is presented below:

Subject: Action Required: You Must Perform Semi-Annual ClinicalConnect Attestations
Dear Sue Legal Signing Authority

Please be advised you must log into the ClinicalConnect [Access Governance System](#) (AGS) to perform attestations. You will find your attestation requests under "My Actions", then "Pending Attestations".

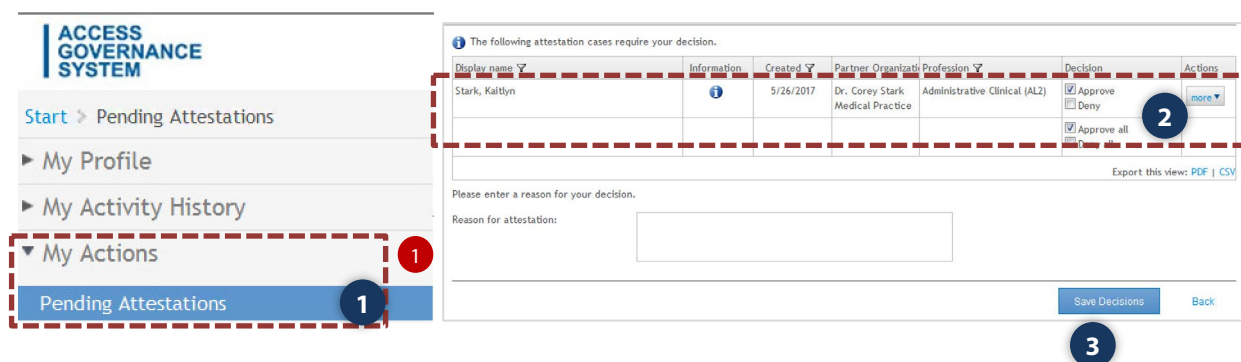
The attestation process is invoked starting every May 1 and November 1 in accordance with the ClinicalConnect Participation Agreement and you are required to complete these attestations for AGS and/or ClinicalConnect users in your organization to verify they are still authorized to use one or more of the systems.

Please complete these attestations as soon as possible.

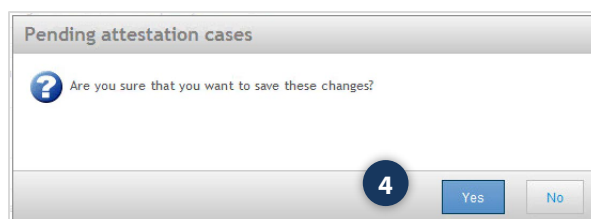
Regards,
ClinicalConnect Administration Team at Hamilton Health Sciences

To complete your attestations when prompted:

1. Select **"My Actions"** from the menu, then **"Pending Attestations."** Your outstanding attestations will be flagged with the red indicator, showing the number of attestations that need to be completed.
2. The unattested accounts will be listed. Select **'Approve'** if the user's information is correct and if the individual still holds the role as stated for your organization. Denying an attestation is the same as removing the appointment for the PC or LRA role. The attestation process will also include the user's Assurance Level that was selected by the requestor when their account was created. If the Assurance Level displayed beside the profession needs to be changed, the LSA must first approve the attestation, then using the "Modify User Properties" function, change the Assurance Level.
3. Save your attestation decision(s).



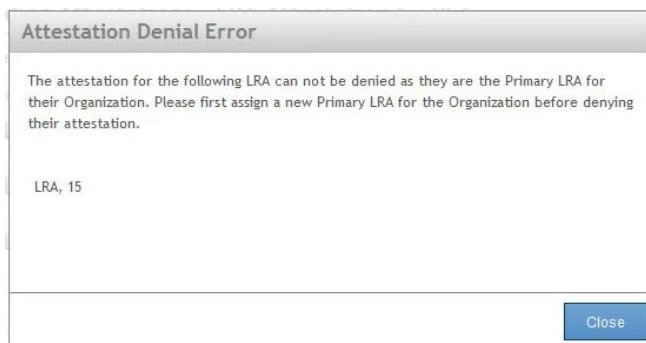
4. Confirm your decision(s). The completed attestation will drop off your attestation list and the red indicator, showing the number of attestations, will update accordingly.



Refer to the "Completing Pending Attestations in AGS eLearning video" available at <https://info.clinicalconnect.ca/CC/healthcare/access-governance-system-ags>

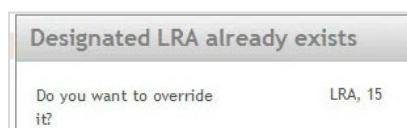
Other Attestation Tips


- If the LSA denies the attestation of their Privacy Contact or Information Security Contact, an on-screen message will appear stating that all Participants must have a Privacy Contact and Information Security Contact. The LSA can then appoint themselves as the organization's PC and ISC, or appoint someone new. A new Privacy Contact and Information Security Contact must be appointed before the denial of the attestation can be completed.
- If an LSA denies a Primary LRA's attestation, an on-screen message will appear stating this person is the Primary LRA, and a new Primary LRA must be appointed before the denial of the attestation can be completed as shown in this example.



At this point, the LSA can select **“Submit Request”** and complete one of two options:

1. Select **“Appoint a New LRA”**: if this is a new LRA who will be the **“Primary LRA”** be sure to select **“Designate as Primary LRA”** when completing the user information. If a Primary LRA already exists, you will be automatically prompted to override the existing Primary LRA, then continue completing the submission for the newly-appointed LRA.



 If a new LRA is appointed who is not yet trained, the LRA will receive a welcome email with details to begin their LRA orientation. The same applies when a new Privacy Contact is appointed who has not yet completed the training for their role.

2. Select **“Add LRA Role to Existing User”** if you’d like to designate an existing ClinicalConnect user or existing LRA as your organization’s Primary LRA and be sure to select **“Designate as Primary LRA”**, then select **“Continue”**.

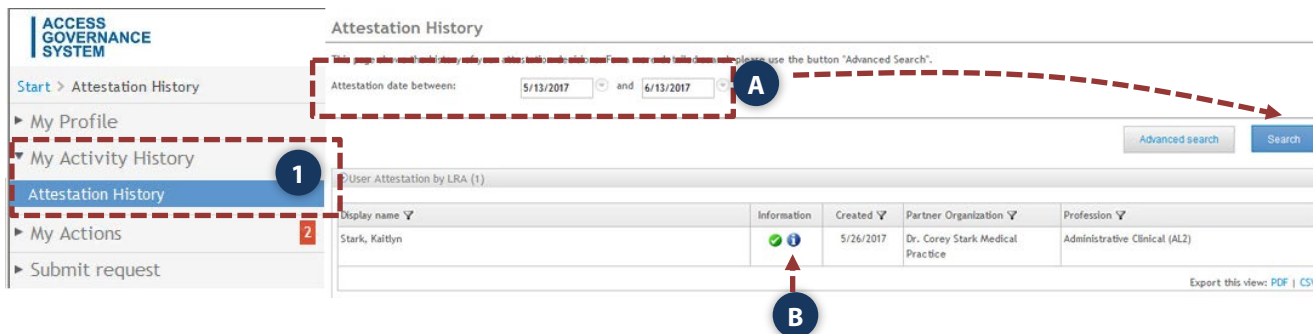
'My Activity History' Menu

Attestation History

After each attestation cycle, your completed attestations will be captured in the Attestation History menu option. These attestations will list attested PC and LRAs within the defined date range **(A)**. Select the **(B)** information icon to view additional user details.

1. Log into AGS, select **"My Activity History"** from the menu, then select **"Attestation History"**.

Attestation Date Range: You may change the date range, then "Search" to re-fresh the list and display your attestation history



ACCESS GOVERNANCE SYSTEM

Start > Attestation History

My Profile

My Activity History

Attestation History

My Actions



Submit request

Attestation History

Attestation date between: 5/13/2017 and 6/13/2017

Advanced search Search

User Attestation by LRA (1)

Display name	Information	Created	Partner Organization	Profession
Stark, Kaitlyn	 	5/26/2017	Dr. Corey Stark Medical Practice	Administrative Clinical (AL2)

Export this view: PDF | CSV