

Privacy & Security Attestation Submission Guide



This guide reviews how Privacy Contacts use the Access Governance System (AGS) to complete the ClinicalConnect Privacy & Security Attestation.

October 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

Table of Contents

ClinicalConnect’s Application Process 4

Support Contacts & Resources 4

Changing Your Supplied Temporary Password & Enrolling in Self-Service Password Manager (SSPM) 5

Logging into AGS to Complete Your Privacy & Security Attestation 5

Completing and Submitting the Privacy & Security Attestation..... 7

Viewing Your Submitted Privacy & Security Attestation 11

Reviewing the Status of Your Submitted Privacy & Security Attestation..... 12

ClinicalConnect's Application Process

As part of the ClinicalConnect Participation Agreement submission, the Legal Signing Authority appointed you as the Privacy Contact for your organization. This guide explains how to use the Access Governance System (AGS) to complete your organization's Privacy & Security Attestation (PSA). The PSA is released via email to you, and you'll be contacted with credentials to log into AGS to complete this PSA. The PSA is completely only after your organization's Privacy Pre-Assessment has been approved by the ClinicalConnect Program Office.

Completing the PSA is mandatory to ensure your organization's compliance with the requirements stipulated in the ClinicalConnect Terms & Conditions. If you have any questions about the content of the PSA, please contact the ClinicalConnect Program Office by emailing privacy@clinicalconnect.ca.

In addition, please note that as explained to Privacy Contacts required to complete the Attestation, you are also required to complete a ~70-minute Privacy Contact Orientation, offered in the form of eLearning modules. It's recommended that you complete this Orientation prior to completing the Attestation, but either way, your organization will not be fully approved until you have completed both requirements.

If you're attempting to complete your PSA but have not yet been contacted with credentials to log into AGS, please email cc-LRA@hhsc.ca.

Support Contacts & Resources

Access Management Team

If you have trouble accessing the Access Governance System, contact the ClinicalConnect Program Office's Access Management Team.
Email: cc-LRA@hhsc.ca

Changing Your Supplied Temporary Password & Enrolling in Self-Service Password Manager (SSPM)

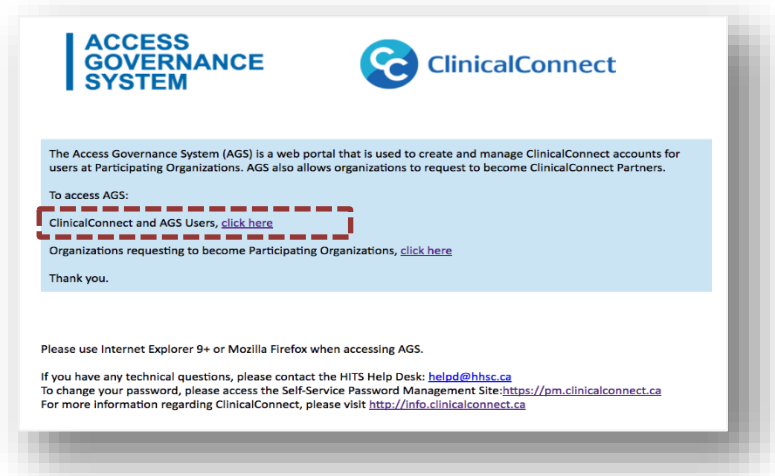
If you don't already have credentials for the Access Governance System, Privacy Contacts will be emailed a temporary password, including instructions to change it to one of your choice. You'll also be contacted by phone to provide your username that you'll need to change the temporary password to one of your choice. Follow the instructions provided, and then this username, and new password, become your credentials to log into AGS to complete the PSA.

Self-Service Password Manager is accessed at <https://pm.clinicalconnect.ca>.

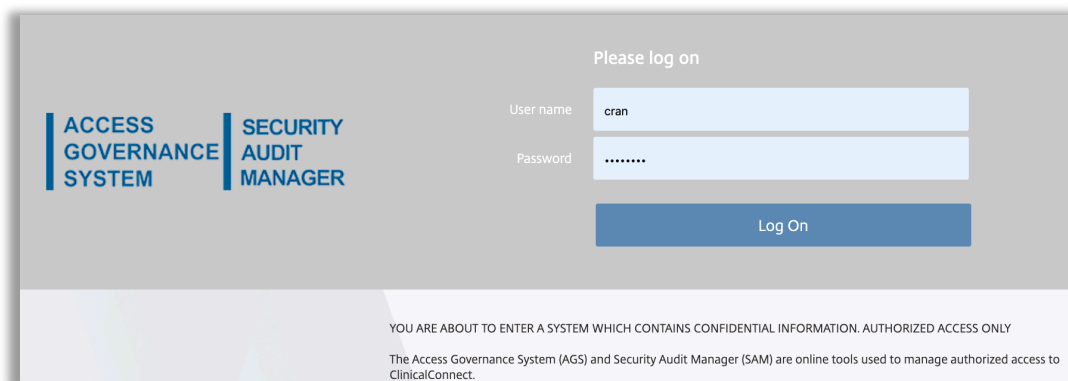
Logging into AGS to Complete Your Privacy & Security Attestation

Note: please use Internet Explorer 9+ or Mozilla Firefox when accessing AGS.

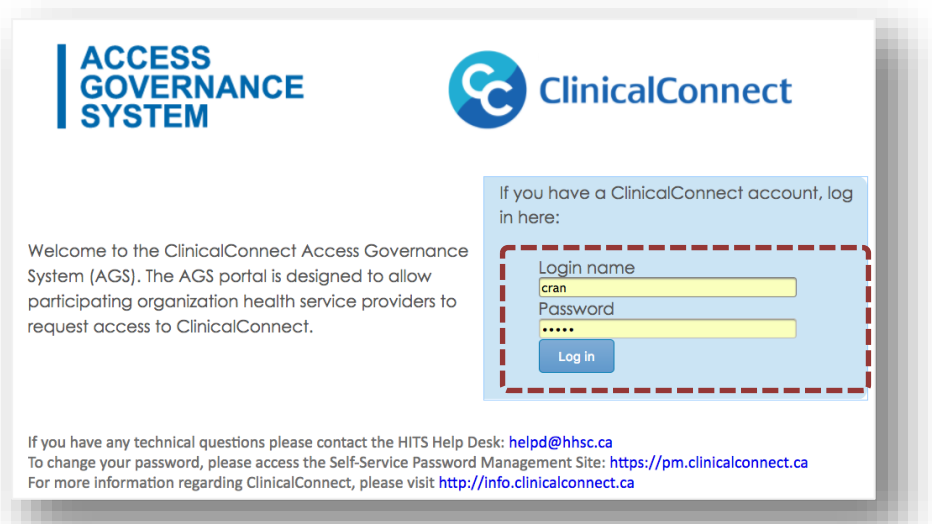
1. Visit <https://ags.clinicalconnect.ca> to login into AGS.
2. Select 'ClinicalConnect and AGS users'



3. You may be prompted to log into the following screen; please do so using what will be your AGS username and password as described above.

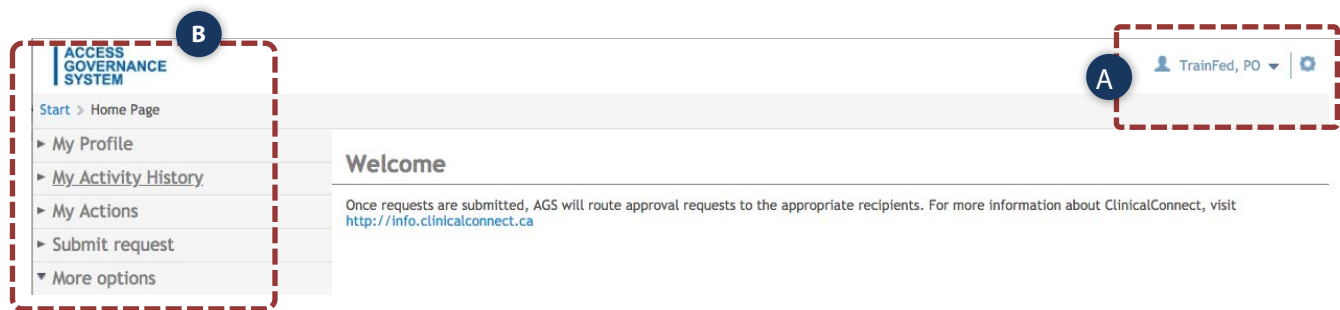


4. Enter your AGS credentials again on the AGS homepage.

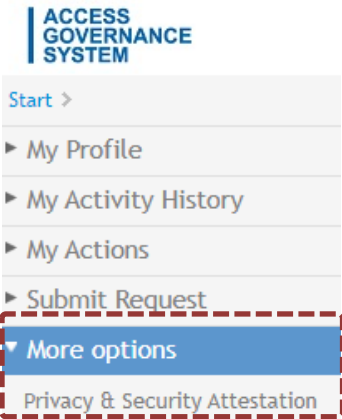


At this point, you have logged into AGS and will be presented with options on the left hand side. You'll also see your name in the top right corner of the screen **(A)**. Clicking the arrow beside your name will provide the option to **'Log Out'** of AGS. Ensure you log out of AGS when you're finished, even if you haven't completed finished your PSA, as it can be saved and returned to later to complete.

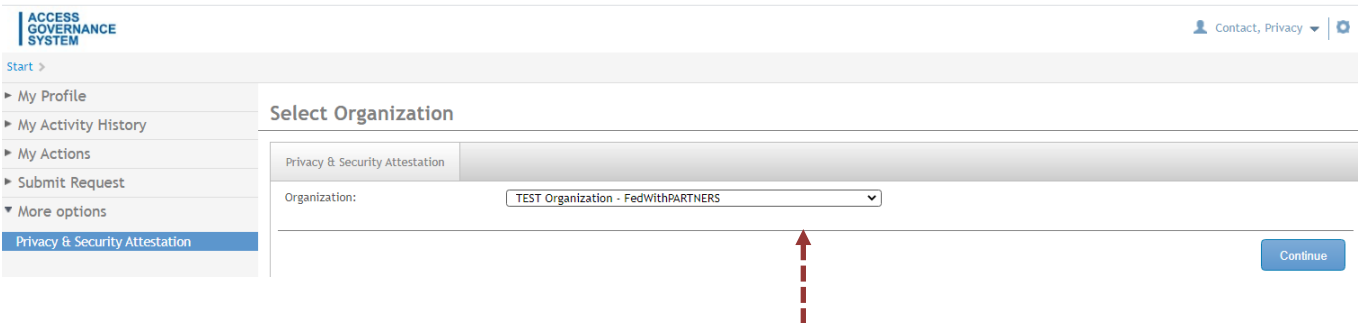
Your navigation menu appears on the left **(B)** side of the screen.



Completing and Submitting the Privacy & Security Attestation



Select **"More Options"**, then **"Privacy & Security Attestation"**.



Your organization will display in the field, then click 'Continue'.

If you are the Privacy Contact for multiple ClinicalConnect Participant Organizations, select the organization that you wish to complete/view the Privacy & Security Attestation, then click Continue.

The Privacy & Security Attestation will display as shown below.

ACCESS
GOVERNANCE
SYSTEM

Start > > Contact Data

My Profile

My Activity History

My Actions

Submit Request

More options

Privacy & Security Attestation

Contact, Privacy

Please complete the Privacy & Security Self-Assessment.

Privacy & Security Attestation

ClinicalConnect Privacy & Security Attestation

To improve the quality and timeliness of health care decision-making, and to enhance access to remote medical consultations, ClinicalConnect makes a broad set of personal health information (PHI) available to Participants. ClinicalConnect is an effective and efficient means of providing shared access to patients' PHI within their circle of care and is used by health care organizations across South West Ontario.

In Ontario, the *Personal Health Information Protection Act, 2004 (PHIPA)* governs the protection of PHI. It includes rules regarding the collection, use, and disclosure of PHI by health information custodians (HICs). It is a requirement that every ClinicalConnect Participant be a HIC; as such, every Participant is legally required to have the correct measures in place to ensure compliance with *PHIPA* while using the portal in the delivery of health care to patients.

The ClinicalConnect Program Office requires that all Participant organizations (excluding Sole Practitioner HIC type who complete an equivalent attestation) complete the Privacy & Security Attestation, a key piece of the application process to access ClinicalConnect. Working through the Privacy & Security Attestation will assist Participants to meet *PHIPA* requirements and also the requirements to participate in ClinicalConnect.

Please complete the ClinicalConnect Privacy & Security Attestation as per the instructions below:

The ClinicalConnect Privacy & Security Attestation must be completed and submitted using the ClinicalConnect Access Governance System (AGS), as part of a Health Information Custodian's application to become a Participant in ClinicalConnect. You may use this working copy of the Privacy & Security Attestation to familiarize yourself with the requirements before logging into AGS to submit your organization's Privacy & Security Attestation when requested to do so by the ClinicalConnect Program Office. The organization's Privacy Contact must check off the appropriate check box for each of the attestation statements listed.

After the Privacy & Security Attestation has been submitted through AGS, the ClinicalConnect Program Office will review the organization's responses and follow up with its Privacy Contact as required within 4 weeks. An organization will not be provided with access to ClinicalConnect until it has satisfied all the requirements.

Once you have finished answering the questions, please complete the information fields located at the bottom of the Attestation and Submit to continue. You will receive an email confirming receipt of the Attestation.

ClinicalConnect Privacy & Security Attestation:

In accordance with the requirements of Ontario's Personal Health Information Protection Act, 2004 (PHIPA) and the ClinicalConnect Policies, I attest the following statements on behalf of my organization:

Attestation Statements	Compliant?	Policy Reference/Comment (Optional)
1. The organization has established policies and practices (information practices) to ensure the appropriate collection, use, disclosure, modification, retention, destruction and ongoing protection of personal health information (PHI) in accordance with <i>PHIPA</i> and applicable legislation.	<input type="radio"/> Yes <input type="radio"/> No	

Read and scroll down to complete the ClinicalConnect Privacy & Security Attestation. **All questions are mandatory.**

Attestation Statements

Compliant?

Policy Reference/Comment (Optional)

1. The organization has established policies and practices (information practices) to ensure the appropriate collection, use, disclosure, modification, retention, destruction and ongoing protection of personal health information (PHI) in accordance with PHIPA and other applicable legislation and to ensure its staff (and other Agents) comply with those policies and practices.

☐ Yes ☐ No

2. The organization has appointed a privacy contact person in accordance with section 15 of PHIPA.

☐ Yes ☐ No

3. The organization has posted or made available to the public a written statement of its information practices (e.g. a Privacy Notice or Privacy Statement) that complies with section 16 of PHIPA and states who individuals can contact with privacy inquiries or complaints and how they can obtain access to or request correction of a record of PHI.

☐ Yes ☐ No

4. The organization has established policies and/or practices for managing complaints or challenges to the organization's compliance with PHIPA, its own policies or privacy best practices.

☐ Yes ☐ No

5. The organization has established policies and practices regarding the type of consent required to collect, use and disclose PHI for different purposes (e.g. that (assumed) implied consent

☐ Yes ☐ No

6. The organization has established policies and/or practices regarding the role that a substitute decision-maker (SDM) plays when a patient is not capable with respect to making their own decisions regarding the collection,

☐ Yes ☐ No

You may use the optional text fields to provide additional comments or to reference a policy if needed.

ClinicalConnect Privacy and Security Attestation Validation:

All fields below must be completed.

I (print name) on behalf of the (Organization Legal Name)

Role:

Organization Address:

Signature (type name):

Date (YYYY-MM-DD):

Save Draft

Submit

You have the option to **"Save"** the PSA then return to it at a later time to complete and submit it in full.

If your Attestation is complete, click **"Submit"**.

Please confirm the changes


Please confirm you're ready to submit your Privacy & Security Attestation


Click "Yes" to submit.

Yes

No

The following confirmation message will display.



Your organization's Privacy & Security Attestation has been submitted for review. Should you wish to review your submission status, you may do so under the "My Activity History" menu 

If you are saving a partially-completed Attestation, the following screen will display when you click "Save" at the end of the Attestation form as shown above. Click 'Yes' to save the information.


Please confirm the changes


Would you like to save your changes?

Yes

No

You will receive the following message:



Your ClinicalConnect Privacy & Security Attestation has been saved until you return to complete and submit the final version. 

Viewing Your Submitted Privacy & Security Attestation

Once you have submitted the Privacy & Security Attestation, it will be saved in the “More Options” section in AGS. To review your submission, select “**Privacy & Security Attestation**” and your information will be displayed as indicated in the header.

Here is a summary of your Privacy & Security Attestation submission.

Privacy & Security Attestation								
<h3>ClinicalConnect Privacy & Security Attestation</h3> <p>To improve the quality and timeliness of health care decision-making, and to enhance access to remote medical consultations, ClinicalConnect makes a broad set of personal health information (PHI) available to Participants. ClinicalConnect is an effective and efficient means of providing shared access to patients' PHI within their circle of care and is used by health care organizations across South West Ontario.</p> <p>In Ontario, the <i>Personal Health Information Protection Act, 2004 (PHIPA)</i> governs the protection of PHI. It includes rules regarding the collection, use, and disclosure of PHI by health information custodians (HICs). It is a requirement that every ClinicalConnect Participant be a HIC; as such, every Participant is legally required to have the correct measures in place to ensure compliance with <i>PHIPA</i> while using the portal in the delivery of health care to patients.</p> <p>The ClinicalConnect Program Office requires that all Participant organizations (excluding Sole Practitioner HIC type who complete an equivalent attestation) complete the Privacy & Security Attestation, a key piece of the application process to access ClinicalConnect. Working through the Privacy & Security Attestation will assist Participants to meet <i>PHIPA</i> requirements and also the requirements to participate in ClinicalConnect.</p> <p>Please complete the ClinicalConnect Privacy & Security Attestation as per the instructions below:</p> <p>The ClinicalConnect Privacy & Security Attestation must be completed and submitted using the ClinicalConnect Access Governance System (AGS), as part of a Health Information Custodian's application to become a Participant in ClinicalConnect. You may use this working copy of the Privacy & Security Attestation to familiarize yourself with the requirements before logging into AGS to submit your organization's Privacy & Security Attestation when requested to do so by the ClinicalConnect Program Office. The organization's Privacy Contact must check off the appropriate check box for each of the attestation statements listed.</p> <p>After the Privacy & Security Attestation has been submitted through AGS, the ClinicalConnect Program Office will review the organization's responses and follow up with its Privacy Contact as required within 4 weeks. An organization will not be provided with access to ClinicalConnect until it has satisfied all the requirements.</p> <p>Once you have finished answering the questions, please complete the information fields located at the bottom of the Attestation and Submit to continue. You will receive an email confirming receipt of the Attestation.</p> <p>ClinicalConnect Privacy & Security Attestation:</p> <p>In accordance with the requirements of Ontario's Personal Health Information Protection Act, 2004 (PHIPA) and the ClinicalConnect Policies, I attest the following statements on behalf of my organization:</p> <table><thead><tr><th>Attestation Statements</th><th>Compliant?</th><th>Policy Reference/Comment (Optional)</th></tr></thead><tbody><tr><td>1. The organization has established policies and practices (information practices) to ensure the appropriate</td><td>Yes</td><td></td></tr></tbody></table> <p>ClinicalConnect Privacy and Security Attestation Validation:</p> <p>All fields below must be completed.</p> <p>I (print name) Test Privacy Contact on behalf of the (organization name) Test Organization</p> <p>Role: Test PC</p> <p>Organization Address: 123 Anytown Street, Anytown, Province, A1A 1A1</p> <p>Signature (type name): Test Privacy Contact Date: 10/1/2020 12:00:00 AM</p> <p>Export this view: PDF CSV</p>			Attestation Statements	Compliant?	Policy Reference/Comment (Optional)	1. The organization has established policies and practices (information practices) to ensure the appropriate	Yes	
Attestation Statements	Compliant?	Policy Reference/Comment (Optional)						
1. The organization has established policies and practices (information practices) to ensure the appropriate	Yes							

You may export your Privacy & Security Attestation as a PDF if needed.

Reviewing the Status of Your Submitted Privacy & Security Attestation

ACCESS GOVERNANCE SYSTEM

Start > My Activity History

My Profile

My Activity History

Request History

Approval History

Attestation History

My Actions

Submit Request

More options

My Activity History

This section provides an overview of your earlier requests, approvals, attestation cases as well as violations.

What would you like to see?

Overview of your submitted requests

There is one request.

Violations

one employee.

Attestation cases

ases.

To review the status of your submitted Privacy & Security Attestation, select **"My Activity History"**.

Your Privacy & Security Attestation will be listed in the **"Status Messages"** section or the **"Request History"** section.

Click the information icon to view details about the status of your submission.

Status messages

My most recent requests

Privacy & Security Attestation
10/1/2020 - State: Request

i

Request information

Information

History

Next decisions

Product:

Privacy & Security Attestation

Recipient:

Contact, Privacy

Requester:

Contact, Privacy

Request date:

10/1/2020 11:25:15 AM

Reason:

Close

Withdraw request

The Request information tabs include: Information, History and Next Decisions.

The **Information** tab shows the date and time you submitted your Privacy & Security Attestation.

Request information

Information History **Next decisions**

Request

At: 4/22/2015 3:21:10 PM

Reason: No reason entered

By: Privacy, Paul

Grant ClinicalConnect Privacy

At: 2/6/2015 10:15:58 AM

Reason: No reason entered

By: ClinicalConnect Privacy

Approval procedure: CP - Calculated group of approvers

Grant ClinicalConnect Agreements

At: 2/6/2015 10:19:07 AM

Reason: No reason entered

By: ClinicalConnect Agreements

Approval procedure: CP - Calculated group of approvers

The **History** tab explains where your Attestation submission is in the approval process with date and time stamps for each step.

Request information

Information History **Next decisions**

The following users are currently entitled to approve this request.

User	Primary department	Phone
ClinicalConnect, Privacy		9055212100

The following users are presumably entitled to approve this request after the current workflow step.

User	Primary department	Phone
ClinicalConnect, Agreements		9055212100

To return to the previous screen, click **"Close"**.

Close Withdraw request

The **Next Decisions** tab shows the users that are entitled to approve your Privacy & Security Attestation