ClinicalConnect® Program

Support Services Reference Guide

Updated: August 2023

Table of Contents

Document Revisions

Version/Date	Author	Description
June 2015	HITS eHealth Office	Summary of ClinicalConnect Services & Service Levels
March 2017	HITS eHealth Office	Update to the Summary of ClinicalConnect Services & Service Levels
February 2018	HITS eHealth Office	Update to incorporate escalation processes when iDP is fed org or ONE ID
April 2018	HITS eHealth Office	Update to revise escalation for access issues when iDP is fed org or ONE ID

December 2018	HITS eHealth Office	Various changes to ensure content of this Guide reflects current ClinicalConnect Program Office operations
April 2020	HITS eHealth Office	Various changes to ensure content of this Guide reflects current ClinicalConnect Program Office operations
October 2020	HITS eHealth Office	Update information about Privacy Contact orientation format
September 2021	HITS eHealth Office	Various changes to ensure content of this Guide reflects current ClinicalConnect Program Office operations
January 2023	HITS eHealth Office	Various changes to ensure content of this Guide reflects current ClinicalConnect Program Office operations
August 2023	HITS eHealth Office	Added cross-reference to the ConnectMyHealth Support Services Reference Guide

Introduction to ClinicalConnect Support Services

This Support Services Reference Guide sets out the understanding between the ClinicalConnect Technology Service Delivery Partner, Hamilton Health Sciences' (HHS) Health Information Technology Services (HITS) division and Participant Organizations, with respect to support services associated with operating, and using, ClinicalConnect.

Readers are encouraged to become familiar with the following documentation pertaining to participating in ClinicalConnect. Please refer to the ClinicalConnect Information Website (https://info.clinicalconnect.ca) for the most up-to-date information about the portal.

The HITS eHealth Office at Hamilton Health Sciences is also known as the ClinicalConnect Program Office (CCPO), referred to throughout this document.

This summary discusses the day-to-day operations and requirements associated with the obligations outlined in the ClinicalConnect Participation Agreement and its associated Terms & Conditions. Generally, it is assumed all Participant Organizations will:

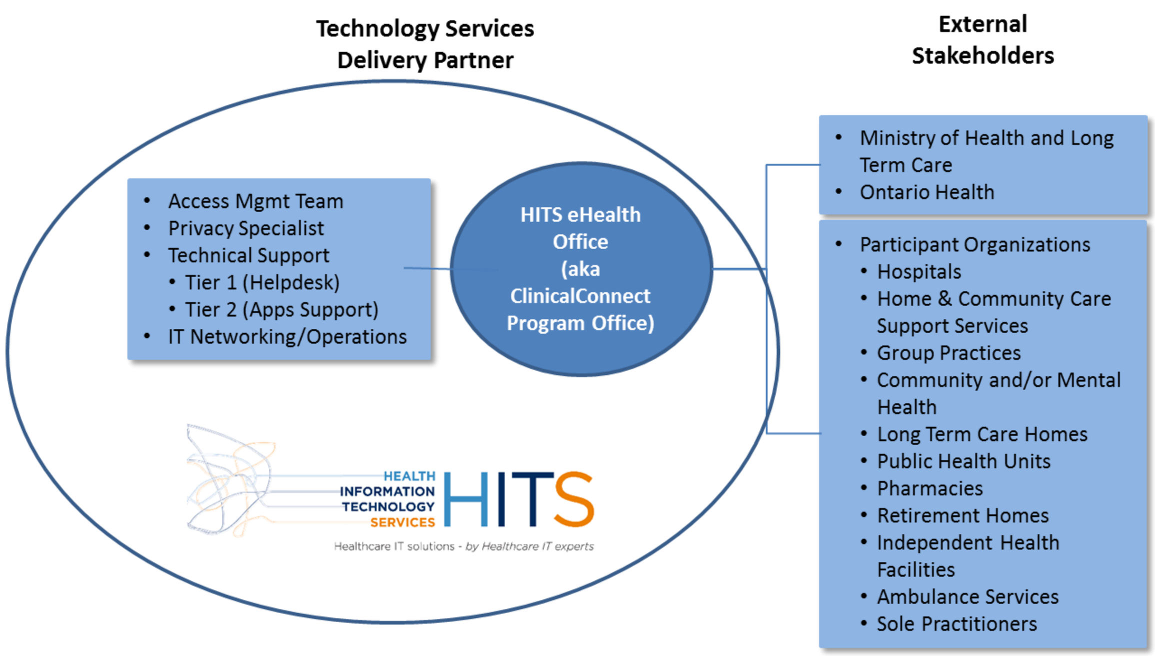
- Follow the established support model for placing support calls/logging issues according to the processes outlined in this document, noting there may be different escalation paths depending on the Identity (Account) Provider (iDP) for the organization that has authorized the user's access to ClinicalConnect.
- Be responsible for creating and executing appropriate contingency plans in the event ClinicalConnect is, or becomes, unavailable.
- Maintain devices (computers and associated applications (i.e. internet browsers) and printers) to the level of compatibility as defined by the applications discussed in this document to ensure proper function, and that if authorized by the sponsoring Participant to access and/or store PHI obtained through ClinicalConnect using a mobile device (i.e. laptops, smartphones, memory sticks, tablets), mobile devices used will be strongly encrypted.
- Ensure that details provided about the organization and its sites approved to use ClinicalConnect remain current at all times, using the Access Governance System (AGS) to make updates as/when required. Examples of details that must always be current in AGS include, but are not limited to: if a site no longer

provides direct healthcare to patients, or if a physician, approved as a Sole Practitioner Participant Organization, no longer provides direct healthcare in south west Ontario (also known as Ontario Health West Region).

This document is not intended to be a legal document, but rather a method by which the parties may understand the current levels of service and the responsibilities of each party involved in operating or using ClinicalConnect.

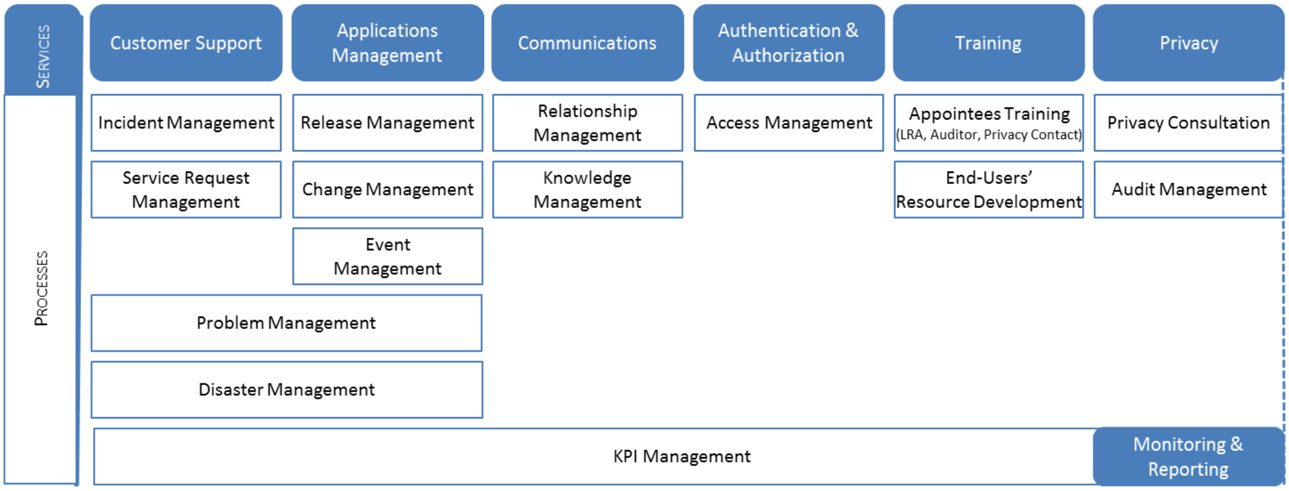
Regional Model

This diagram shows the relationships between internal stakeholders who contribute to the operation of ClinicalConnect, and external stakeholders, some of whom are users of ClinicalConnect. The HITS eHealth Office is the hub connecting internal and external stakeholders.



Summary of ClinicalConnect Program Office's Support Services

The following processes are managed by the ClinicalConnect Program Office and support the efficient delivery of the ClinicalConnect service.



- Customer Support: focuses on incident and service request management
- Applications Management: focuses on activities related to release cycles, including but not limited to testing, events monitoring, problem/change management and disaster recovery (per ITIL v3 framework)
- Communications: focuses on using communications to manage stakeholder relationships, service delivery and knowledge transfer, internally and externally
- Authorization & Authentication: focuses on ensuring proper control of user identification and entitlement
- Training: focuses on developing end user training resources to be leveraged by Participant Organizations, plus educating ClinicalConnect Local Registration Authorities, Privacy Contacts and Auditors, and providing orientation to physicians who become Sole Practitioner HIC Participants unto themselves
- Privacy: focuses on Participants' privacy compliance with respect to ClinicalConnect, as well as managing the overall audit program run by the ClinicalConnect Program Office
- Monitoring & Reporting: focuses on measurement and metrics reporting, which in turn supports all aspects of Applications, Customer Support, Communications services

ClinicalConnect Program Office's Privacy Service

The ClinicalConnect Program Office provides privacy oversight of, and to, its Participants. Team members support privacy-related services including:

- Monitoring ClinicalConnect usage and liaising with Participant Privacy Contacts as appropriate
- Handling day-to-day inquiries from Participants with respect to privacy matters
- Responding to patient inquiries, in cooperation with Participants as required
- Implementing consent directives in ClinicalConnect based on patients' requests, or re-directing such requests if the patient requests a consent directive based at the source system level versus only in ClinicalConnect
- Generating access audits for Sole Practitioners
- Operating the ClinicalConnect Privacy Advisory Committee (CCPAC). CCPAC serves as the privacy committee supporting the ClinicalConnect Program Office and is chaired by the ClinicalConnect Program Office Privacy Specialist. Membership includes representation from HIC types and geographical locations across Ontario Health West Region from ClinicalConnect Participant Organizations and the Committee meets bi-monthly. Membership is reviewed annually.
- Hosting webinars, as required, to provide privacy-related updates to ClinicalConnect Privacy Contacts

The tasks outlined above are performed in accordance with the ClinicalConnect Privacy Policies. A brief description of each policy is provided below, and additional information is available to ClinicalConnect Privacy Contacts on the Privacy Contact SharePoint site, and to Sole Practitioners (physicians) on the Sole Practitioner SharePoint site.

Harmonized Access and Correction Policy – This policy and its associated procedures apply to Requests for Access and Requests for Correction in respect of records of Personal Health Information (PHI) viewable through ClinicalConnect. This policy and its associated procedures do not apply to Requests for Access and Requests for Correction in respect of records of PHI that have not been contributed to ClinicalConnect.

Harmonized Assurance Policy – This policy and its associated procedures apply to the conduct of ClinicalConnect Program Office, HICs who create and contribute or who collect, use or disclose PHI in ClinicalConnect, and agents and Electronic Service Providers (ESPs) of the HICs or ClinicalConnect Program Office.

Harmonized Auditing and Logging Policy – This policy and its associated procedures apply to logging, auditing and monitoring viewable through ClinicalConnect for the purpose of facilitating the identification and investigation of actual or suspected Privacy Breaches or Security Breaches related to PHI in ClinicalConnect.

Harmonized Consent Management Policy – This policy and its associated procedures apply to obtaining consent, implementing Consent Directives and overriding Consent Directives in respect of the individual's PHI viewable in ClinicalConnect for the purpose of providing or assisting in the provision of healthcare to the individual, and not to obtaining consent, implementing Consent Directives or overriding Consent Directives in respect of any other PHI or for any other purpose.

Harmonized Inquiries and Complaints Policy – This policy and its associated procedures apply to Inquiries and Complaints in respect of ClinicalConnect. This policy and its associated procedures do not apply to Inquiries or Complaints in respect of any system other than ClinicalConnect or in respect of any information other than PHI viewable in ClinicalConnect.

Harmonized Privacy and Security Training Policy – This policy and its associated procedures apply to the provision of information by HICs and the ClinicalConnect Program Office to their agents and ESPs to appropriately inform them of their duties under PHIPA, the ClinicalConnect Participation Agreement and the policies, procedures and practices in respect of privacy and security implemented in relation to ClinicalConnect. This policy and its associated procedures do not apply to privacy and security training:

- In respect of any system other than ClinicalConnect;
- In respect of any information other than PHI in ClinicalConnect;
- To agents of HICs who do not collect, use or disclose PHI in ClinicalConnect;
- To ESPs of HICs who do not view, handle or otherwise deal with PHI in ClinicalConnect; or
- To agents or ESPs of the ClinicalConnect Program Office who do not view, handle or otherwise deal with PHI in ClinicalConnect.

Harmonized Privacy Breach Management Policy – This policy and its associated procedures apply to Privacy Breaches in respect of ClinicalConnect and not in respect of any system other than ClinicalConnect or in respect of any information other than PHI in ClinicalConnect.

Harmonized Retention Policy - This policy and its associated procedures apply to retention of the following records in respect of ClinicalConnect:

- Personal Health Information (PHI);
- Personal Information (PI) collected to support Provider Registry;
- Audit logs and audit reports that contain PHI/PI;
- Information collected about an individual to respond to:
  - Requests for Access or Requests for Correction under the *Personal Health Information Protection Act, 2004* (PHIPA);
  - Requests to make, modify, or withdraw a Consent Directive under PHIPA; and
  - Inquiries or Complaints under PHIPA.
- Information created about an individual as part of an investigation of Privacy Breaches and/or Security Incidents;
- System-level logs, tracking logs, reports and related documents for privacy and security tasks that do not contain PHI/PI;
- Corporate documents collected or created by the ClinicalConnect Program Office, including:
  - Templates or resources developed by the ClinicalConnect Program Office in respect of ClinicalConnect;
  - Assurance-related documents; and
  - ClinicalConnect Program Office business documents.

This policy and its associated procedures do not apply to copies of records of PHI/PI that have been made from ClinicalConnect and retained by the HIC, or by the agents or ESPs of the HIC, other than the ClinicalConnect Program Office and its agents or ESPs.

Summary of Ancillary Online Tools

For the purposes of this document, ClinicalConnect is considered the 'service' but access to the 'service' is supported by various online tools that are mentioned in the pages that follow:

1. **Access Governance System (AGS)** (https://ags.clinicalconnect.ca) is used to request, review, approve, fulfill and attest ClinicalConnect accounts.

AGS is used by a number of key roles at ClinicalConnect Participant Organizations, excluding HHS, and including Legal Signing Authorities, Privacy Contacts and Local Registration Authorities. Note that if ONE® ID is the Identity Provider for the Participant Organization, or the Organization itself is a federated Identity Provider, ONE ID/organization's credentials cannot be used to access AGS as it is not a federated service of Ontario Health at this time, however HHS will supply credentials for the role holders listed above to access AGS and perform required duties.

2. **Self-Service Password Manager (SSPM)** (https://pm.clinicalconnect.ca) is used by end users who need access to both ClinicalConnect and/or these ancillary online systems, to change temporary passwords for the first time to a permanent one, or manage passwords on an ongoing basis.

Please note that SSPM cannot be used to change passwords associated with ONE ID or federated organizations' credentials; these credentials, including passwords, are managed by Ontario Health for ONE ID, and by the Participant Organization itself, if a federated Ontario Health Identity Provider. SSPM cannot be used to change/reset passwords by ClinicalConnect users from HHS; HHS' ClinicalConnect users should contact the hospital's Computer Access Management team by emailing passadmin@hhsc.ca or by dialing extension 44201 at HHS.

3. **HITS Digital Health Learning Management System (LMS)** (https://mylearning.hhsc.ca/HDH) is used by Privacy Contacts, Privacy Auditors, Local Registration Authorities and Sole Practitioners (physicians) to complete their mandatory orientation to their role, offered in the form of eLearning modules.

4. **Haystack iS Auditing & Surveillance Tool** (https://audit.clinicalconnect.ca) is an online tool used by Privacy Contacts and Privacy Auditors, and provides near real-time surveillance and monitoring of Participant Organizations' users' accesses to ClinicalConnect.

HITS maintains a seasoned staff of Information & Communication Technology experts with in-depth knowledge that is leveraged to support the needs of Participant Organizations and their efficient use of ClinicalConnect, AGS, SSPM, the LMS and Haystack iS.

About Your Participation in ClinicalConnect

Roles & Responsibilities When Participating in ClinicalConnect

The following provides a high-level summary of the responsibilities of each key role that must be filled by all Participant Organizations at all times.

Legal Signing Authority

- Ensuring organization upholds the ClinicalConnect Terms & Conditions
- Revoking and appointing new Privacy Contact, Information Security Contact and LRA(s) if required
- Performing semi-annual attestations of Privacy Contact, Information Security 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 operates a private practice in Ontario Health West Region, or is no longer an active member of the College of Physicians & Surgeons of Ontario (CPSO).

Privacy Contact (PC)

- Completing a ~70-minute orientation, in the form of eLearning modules, related to their role as Privacy Contact; the orientation must be complete in order for the organization to be considered for final approval as a Participant. In addition, all replacement Privacy Contacts of existing, approved Participant Organizations must also complete this orientation, and do so within 30 days of being appointed to the role.
- Handling all privacy-related matters as outlined in the ClinicalConnect Terms & Conditions
- Handling all audit-related matters, and being proficient in using Haystack iS
- Completing/signing off on all privacy-related documentation
- Performing semi-annual attestations of Privacy Auditors
- Performing Annual Compliance Attestation on behalf of their organization

Privacy Auditor (PA)

- Completing orientation to the role, offered as a one-hour eLearning module. This eLearning module must be completed within 60 days of being appointed to the role of Privacy Auditor, or the appointment will be automatically revoked, and the individual will need to be re-appointed by the Privacy Contact and begin their orientation pathway again.

- Running audits on ClinicalConnect usage for users at their organization according to the ClinicalConnect Privacy Policies using Haystack iS, and verifying/investigating audit findings as directed by their organization's Privacy Contact.

Note that generation of access audits for Sole Practitioner (Physician) HIC Participant Organizations is fulfilled by the ClinicalConnect Program Office, but the responsibility of verifying/investigating audit findings is the responsibility of the Sole Practitioner HIC's designated Privacy Contact.

Information Security Contact (ISC)

- 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

Local Registration Authority (LRA)

- Completing orientation to the role, offered as a one-hour eLearning course consisting of two parts. Part 1 provides an overview of the LRA and fundamental information about the organization's access to ClinicalConnect, and Part 2 consists of a series of interactive, self-paced modules that teach the LRA how to use the Access Governance System. The entire eLearning course must be complete within 60 calendar days of the LRA being appointed to the role.
- Using AGS to create, manage and revoke ClinicalConnect accounts for users in the organization, or if using ONE ID as the Identity Provider, using AGS to request authorization of users' ONE ID credentials so they can be used to access ClinicalConnect
- Resetting passwords for AGS and ClinicalConnect if HHS is the Identity Provider, or just for ClinicalConnect's ancillary systems, if ONE ID is the Identity Provider
- Attesting ClinicalConnect access for users on a semi-annual basis, regardless of Identity Provider
- Assisting users with their initial login to ClinicalConnect
- Ensuring users understand the User Agreement that they'll be prompted to review and accept the terms of from within the portal itself
- Making arrangements to ensure that ClinicalConnect users are fully aware of their privacy & security responsibilities when using the portal, coordinating with organization's Privacy Contact if needed
- Ensuring that users are aware of who to contact if they have trouble accessing ClinicalConnect, or once in ClinicalConnect have technical issues, who to report that to
- Providing support related to troubleshooting user account issues, if needed
- Ensuring that adequate training about how to use ClinicalConnect is available to staff, leveraging the wide range of training resources, in PDF and video format, available in ClinicalConnect's Resource Centre: http://info.clinicalconnect.ca/CC/healthcare/resource-centre.

Depending on the size or the scope of the expected use of ClinicalConnect, an organization may have multiple LRAs. An organization must have at least one primary LRA, and it is recommended that there is a backup LRA appointed.

If the organization's Identity Provider is ONE ID, it will also have a ONE ID LRA; it is possible one person can be both the ClinicalConnect LRA and the ONE ID LRA, or these roles may be held by different people.

Central Point of Contact (CPC)

Each ClinicalConnect Participant Organization must have at least one CPC assigned to liaise with the ClinicalConnect Program Office, but note that the role of the CPC varies for organizations that contribute data to the portal versus those that do not. In general, the CPC acts as conduit of portal-specific information between ClinicalConnect Service Provider and their organization. For viewer-only Participant Organizations, the designated Primary LRA is also the CPC unless otherwise specified. The primary responsibility for all CPCs, data-contributor or not, is to manage requests for enhancements for ClinicalConnect and/or AGS using the established enhancement request process. At data-contributing organizations, the role of the CPC is more involved. These CPCs are the point of contact between their organization and the Health Information Technology Services (HITS) team – HITS is the IT division at Hamilton Health Sciences. The CPC acts as HITS' contact with respect to the data being fed from their organization's health information system (HIS) into ClinicalConnect. They may also be involved in projects where their organization's data, aggregated in the portal, is then fed to other third-party systems, such as Health Report Manager and/or certain provincial repositories, or used to generate electronic notifications of a patient's encounter to their organization, all with a view to ensure those in a patient's circle of care are kept informed as their healthcare journey evolves. The CPC is often relied on to assist in troubleshooting data availability issues if they occur, as well as notifying HHS of updates/upgrades to their HIS that may impact ClinicalConnect end users as described below. Finally, CPCs of data-contributing Participant Organizations are responsible to fulfill any requirements associated with testing the presentation of their organization's data in ClinicalConnect and will be contacted as required by HITS.

Authorization & Authentication of Access to ClinicalConnect

In support of Ontario Health's Single Sign On standard, Participant Organizations must designate who their Identity Provider (iDP) is; the entity is then responsible for authenticating their users' access to digital health tools, including ClinicalConnect. Where ONE ID or a Participant Organization, if 'federated', is the iDP, the user's ClinicalConnect login credentials can often be associated with/used to access other digital health or related access ('single sign on').

Currently three approved Identity Providers can issue credentials and authenticate users' access ClinicalConnect. Confirm who your Participant Organization's Identity Provider is by clicking here to review the respective Participant Organization list.

Identity Provider	Identity Provider for…	Link to Log Into ClinicalConnect
Hamilton Health Sciences	Individuals authorized to use credentials provided by HHS/their ClinicalConnect LRA.	https://clinicalconnect.ca
ONE ID	Individuals who use ONE® ID credentials to access ClinicalConnect.	https://swo.clinicalconnect.ca
Our organization, an Ontario Health federated iDP Ontario Health	Individuals who use their own organization's credentials to access ClinicalConnect.	https://swo.clinicalconnect.ca

If using ONE ID or your own (federated organization) as your iDP, the link to log into ClinicalConnect is slightly different than if using HHS-provided credentials. **The access point is https://swo.clinicalconnect.ca, and these users will see the screen below where they must select their organization, or if using ONE ID credentials, they'll select ONE ID, from a drop down menu – a menu maintained by Ontario Health.** An example of this experience is provided below:

Notes:

- As previously mentioned, neither ONE ID nor federated organizations' credentials can be used to access AGS, SSPM, the LMS or Haystack iS. HHS-provided credentials must be maintained for individuals requiring access to these systems to perform duties associated with their role(s), as outlined above.
- When using ONE ID credentials to log into ClinicalConnect, there is a 'second logout' requirement that users will experience to ensure both ClinicalConnect and their ONE ID session is logged out.
- When HHS is the Participant Organization's Identity Provider, LRAs use AGS to create ClinicalConnect accounts; LRAs pick a username for the individual, and AGS creates, and sends by email, a temporary password to be changed by the user. This username, and new password, become the user's credentials to access ClinicalConnect from https://clinicalconnect.ca.
- When ONE ID is the Participant Organization's Identity Provider, or the organization itself becomes a federated Identity Provider, LRAs still use AGS to submit requests that their end users' ONE ID credentials, if ONE ID is their iDP/their organization's credentials, be authorized by Ontario Health to 'add the ClinicalConnect service' and then access the portal from https://swo.clinicalconnect.ca.

Launching ClinicalConnect Directly From Other Health Information Systems

ClinicalConnect can be configured to launch directly out of a variety of information systems used at Participant Organizations. For example, at hospitals in Ontario Health West Region, ClinicalConnect can be launched from Meditech, Epic and Cerner. At some Long-Term Care Homes, ClinicalConnect can be launched from PointClickCare, a widely-used information system at LTCs in Ontario. Some Group Practice Electronic Medical Records (EMRs) have the ability to launch ClinicalConnect directly. The benefit of this functionality, known as "Contextual Launch" is that with one click from the user's local health information system, while maintaining patient context, they can obtain data from otherwise disparate sources by launching ClinicalConnect.

Enabling Contextual Launch from an organization's health information system requires configuration by HITS. In addition, if an organization equipped with Contextual Launch experiences issues launching ClinicalConnect, the troubleshooting/escalation path is to contact the organization's ClinicalConnect Local Registration Authority first to ensure the issue isn't being caused by the account set-up. Note the ClinicalConnect LRA may need to consult with their counterpart at your organization – the ONE ID LRA – if Contextual Launch at your organization leverages ONE ID credentials, because ONE ID is your organization's Identity Provider. If the LRA is not able to resolve the issue preventing the launch of ClinicalConnect, the escalation pathway is to contact the vendor of the organization's information system from which Contextual Launch has been enabled. The HITS Helpdesk can only provide technical support if 'clinicalconnect' displays in the URL once the portal has been launched from the information system. In other words, trouble accessing ClinicalConnect may not necessarily be something the HITS Helpdesk can resolve – the vendor of the solution or LRA that provisioned the access originally may be able to. If the internal technical support teams determine that the issue is on the ClinicalConnect technical side, a ticket should be logged with the HITS Helpdesk. From there, the HITS Helpdesk will determine the extent of the communications that are required based on impact as described in the Incident Management Framework that follows.

Ways to Limit How Users Can Access ClinicalConnect

ClinicalConnect users can be set up to access ClinicalConnect in one of three ways. How users' access is configured is determined by their Participant Organization and is set/changed as required by their ClinicalConnect Local Registration Authorities using AGS.

1. **Full Access**: access ClinicalConnect directly via the internet at:
    a. https://clinicalconnect.ca; or
    b. https://swo.clinicalconnect.ca (if using ONE ID credentials, or one's organizational credentials).

As described in the preceding section, users working at organizations, like hospitals, select Long-Term Care Homes and select Primary Care offices, can be set up to launch ClinicalConnect from within their work's health information system. This functionality is referred to as "Contextual Launch".

There are two further restrictions to Contextual Launch that can be applied at the discretion of the organization that limit a user's ability to search for additional patients, and their health data, within ClinicalConnect. These can be applied on a user-by-user basis.

2. **Contextual Launch 'Only' (CL-Only):** limits access to ClinicalConnect only from the organization's health information system (i.e. not also from the web-based instance mentioned above).
3. **'Restricted' Contextual Launch (RCL):** a further restriction that prevents a user from being able to search for other patients' data beyond the one they're currently looking at in the organization's health information system (i.e. once ClinicalConnect is launched from the information system, there is no ability to enter a second patient's name in the Search bar, as there is no Search function nor Census List availability for RCL-designated users. In this case, accessing other patients' records in ClinicalConnect is only possible if the user returns to their own clinical system, selects another patient, and then launches back into ClinicalConnect for that patient).

LRAs wishing to implement option 2 or 3 above should contact the CCPO through their normal support channels.

Support Model

To best explain the support model associated with being a Participant in ClinicalConnect, content is broken down as follows:

1. Initial Orientation & Ongoing Training Support – to ensure ClinicalConnect end users' training needs are met, as well as the individuals designated to use the ancillary online tools.
2. Access Support – to assist with troubleshooting and resolving issues preventing individuals from logging into ClinicalConnect and/or its ancillary online tools.
3. Technical Support – issues using ClinicalConnect, or the ancillary online tools discussed in this document.

Initial Orientation & Ongoing Training Support

ClinicalConnect's Privacy Contacts, Privacy Auditors, Local Registration Authorities and Sole Practitioners (physicians) all complete an orientation to their role via eLearning module(s), prior to gaining access to the ancillary online tools they'll use in their role.

There are various ways to obtain support for using ClinicalConnect or its ancillary systems:

1. Visit https://info.clinicalconnect.ca/CC/healthcare/resource-centre. The ClinicalConnect Resource Centre contains helpful training materials in video and PDF format.

LRAs looking for suggestions of how to incorporate ClinicalConnect resources into their organization's regular training for staff should visit this website for further information:
https://info.clinicalconnect.ca/CC/healthcare/training

In addition, resources are posted to various SharePoint sites for various roles as follows:

- Sole Practitioners: https://eshare.hhsc.ca/sites/teams/cc_sole_practitioners
- Privacy Contacts: https://eshare.hhsc.ca/sites/teams/ccprivacy
- Privacy Auditors: https://eshare.hhsc.ca/sites/teams/ccauditors
- Local Registration Authorities: https://eshare.hhsc.ca/sites/teams/cclra
- Information Security Contacts: https://eshare.hhsc.ca/sites/teams/ccsecurity

Access Support

End users must always first contact their organization's LRA if unable to access ClinicalConnect or its ancillary online systems, as their LRA is the first point of contact for troubleshooting access issues.

If the LRA is unable to resolve the end user's access issue, LRAs' escalation path for assistance, depending on the online tool affected, is shown below.

LRAs' Escalation Path If Unable to Resolve Access Issues for ClinicalConnect or Ancillary Online System(s)		
Identity Provider	**ClinicalConnect**	**Ancillary Systems (AGS, SSPM, LMS or Haystack)**
ONE ID Our organization, an Ontario Health federated iDP Ontario Health	LRA should contact their organization's IT Support/Service Desk. If organization is unable to resolve access issue, an appropriate representative from organization should contact the HITS Helpdesk at HHS, who will involve Ontario Health's Service Desk if/as needed to resolve the access issue.	ClinicalConnect Access Management Team Phone: 905-521-2100 ext. 46727 Email: cc-lra@hhsc.ca

Hamilton Health Sciences	**During Business Hours:** ClinicalConnect Access Management Team Phone: 905-521-2100 ext. 46727 Email: cc-LRA@hhsc.ca **After Hours:** HITS Helpdesk Phone: 905-521-2100 ext. 43000 Email: helpd@hhsc.ca

Technical Support

The process to obtain technical support for issues experienced ***once logged into ClinicalConnect*** is the same regardless of who the Identity Provider is. All technical support inquiries must be directed to the HITS Helpdesk at Hamilton Health Sciences who will triage and resolve accordingly.

Examples of technical issues include:

- "I can't see data for patients I'd expect to see"
- Results or pages aren't loading properly
- ClinicalConnect seems unusually slow in general
- AGS, SSPM, the LMS or Haystack iS are unavailable to log into or not functioning as expected

From within ClinicalConnect itself, users can fill out the *Report Technical Issue* form to enter details of their ClinicalConnect issue. Alternatively, users can also contact the HITS Helpdesk to report their issue by:

1. Phone 905-521-2100 ext. 43000 (Note: always call for urgent issues).
2. Email helpd@hhsc.ca, noting that response time for email-reported incidents may be up to one business day.

The HITS Helpdesk provides Automated Call Distribution and queue management services to ensure timely responses to callers. Requests will be recorded, triaged, tracked and managed using HITS' Incident Response Management System. Incidents are escalated to appropriate vendor(s) if required for specific application failures that occur for HHS-supported applications.

Dedicated Support for ClinicalConnect LRAs

The ClinicalConnect Program Office's Access Management team is dedicated to supporting ClinicalConnect's LRAs from all Participant Organizations once the LRAs' initial orientation/training is complete. The Access Management Team's normal business hours are Monday-Friday, 0800 – 1600 hours, and the team can be contacted by emailing cc-LRA@hhsc.ca, or by phoning 905-521-2100 ext. 46727.

Dedicated Support for Sole Practitioner Participant Organizations

Sole Practitioners (physicians) are able to request assistance directly from the ClinicalConnect Program Office by emailing access@clinicalconnect.ca, or by phoning 905-577-8269 ext. 7.

Incident Management Framework for ClinicalConnect & Ancillary Systems

Summary of Incident Management Process

The following chart defines the type of incident that would be considered Critical (Severity 1), High (Severity 2), Medium (Severity 3) and Low (Severity 4). As such, the level of available support depends on the severity of the reported incidents:

- Severity 1 shall be handled on a 24/7 basis
- Severity 2 shall be handled during regular work hours, with best effort after hours
- Severity 3 and 4 shall generally be handled during regular work hours

HITS' Hours are:
Tier 1 (HITS' Helpdesk):
- 24 hours a day, 7 days a week

Tier 2 (Application Support/Operations Team, required for issues requiring more advanced technical support):
- Monday – Friday: 0800 – 1700 hrs
- Evenings, Weekends & Statutory Holidays: On-call support available as required

Incident Management Framework & Supporting Communication Approaches

Severity Level	Definition	Immediate Response	Target Resolution	Email Communication to User Community		
				No Later than 1 Hour After Issue Confirmed	Follow up Communication	Upon Resolution
Critical Sev 1	• Production Access Unavailable (clinicalconnect.ca) • Federated Access Environment Unavailable (swo.clinicalconnect.ca) • ONE ID/Federated org credentials can't be used to access swo.clinicalconnect.ca* • No workaround available. • Significant impact on user community.	CCPO updates Info Site's System Notices page	60 minutes	Helpdesk emails appropriate distribution list. Essence of message: Environment down; working to restore; ETA to restore or next update	Email appropriate distribution list after 4 hrs from first notification of the issue; if issue hasn't yet been resolved. Essence of message: Environment down; work continues to restore; ETA to restore or next update	Helpdesk emails appropriate distribution list. Essence of message: Environment now available
High Sev 2	• Production environment noticeably unstable or slow (Service Degradation) • Entire source system/repository's data unavailable • Provincial Client Registry (PCR) unavailable. • Mission-critical functionality unavailable (e.g., EID, New Results flags, Reporting). • Contextual Launch is unavailable from one or more HISs**	CCPO updates Info Site's System Notices page	4 hours	Helpdesk emails appropriate distribution list. Essence of message: Component down; working to restore; ETA to restore or next update	Email appropriate distribution list after 48 hrs from first notification of the issue; if issue hasn't yet been resolved. Essence of message: Component down; work continues to restore; ETA to restore or next update	Helpdesk emails appropriate distribution list. Essence of message: Source system or critical functionality restored
Medium Sev 3	• Part of a source system/repository's data unavailable, but Production environment remains stable. • Non-mission critical functionality unavailable, but workaround is available.	CCPO updates Info Site's System Notices page	3 business days	N/A – no mass email communication	N/A – no mass email communication	N/A – no mass email communication
Low Sev 4	• Unique/individual incidents being reported with no indication of widespread effect. • Low impact on user community. • Workaround available.	N/A – notice not posted to Info System Notices page for Sev 4 issues	5 business days	N/A – Email directly with customer as required through to resolution.	N/A – Email directly with customer as required through to resolution.	N/A – Email directly with customer through to resolution.

* Many users now use either ONE ID credentials, or their organization's credentials, to access ClinicalConnect from https://swo.clinicalconnect.ca. When Ontario Health is having a technical issue affecting these credentials, it can result in users not being able to access ClinicalConnect at all. Or, the federated login environment (aka https://swo.clinicalconnect.ca) can become unavailable because of issues being experienced by OH. Both scenarios can result in these users not being able to log into the Federated Environment which represents a Critical/SEV 1 issue, and an unplanned downtime communication is normally issued to affected ClinicalConnect users by the HITS Helpdesk.
** Issues related to launching ClinicalConnect from third-party information systems will be reviewed on a case-by-case basis and an appropriate communication may be issued directly by the ClinicalConnect Program Office (not the HITS Helpdesk) to the ClinicalConnect Local Registration Authorities appointed for the affected organization(s), with instruction to ensure their user community is aware.

Availability of ClinicalConnect and Ancillary Online Systems

Planned Downtimes

- A planned downtime may relate to data from a specific source system (data outage) or the portal itself (full portal downtime).
- HITS schedules regular maintenance/update downtimes for ClinicalConnect, which are generally monthly, and normally during the day on Saturdays, or on Wednesday evenings.
- The HITS Helpdesk makes every effort to inform Participant Organizations and end users of scheduled downtimes via email, as follows:
    - If downtime is expected to last 8 or more hours: two weeks' notice is provided
    - If downtime is expected to last less than 8 hours: one week notice is provided
    - A reminder of the downtime may also be issued up to two days in advance of the scheduled downtime date.
    - If the downtime needs to be extended from the previously-published end time, a notice will be issued to create awareness amongst ClinicalConnect end users
- Following the completion of scheduled maintenance that impacts the ClinicalConnect end user experience, the HITS Helpdesk will issue a notice via email that summarizes any new features and functionality.
- HITS reserves the right to schedule downtimes for ClinicalConnect as required, and every attempt is made to schedule downtimes such that the impact on the ClinicalConnect user community is minimized.

Unplanned Downtimes

- An unplanned downtime may relate to data from a specific source system (data outage) or the portal itself becomes unexpectedly unavailable.
- In the event an urgent/emergency downtime is required, it will be scheduled with as much advance notice as possible and Participant Organizations end users will be notified by email from the HITS Helpdesk.
- In either scenario, the ClinicalConnect user community will be notified as explained in the Incident Management Framework shown above.

Downtime Notifications

Notifications regarding ClinicalConnect's availability or outages affecting an entire source system within the portal will be communicated via email from the HITS Helpdesk, and posted to the System Notices page of the ClinicalConnect information website (https://info.clinicalconnect.ca/CC/healthcare/system-notices). In the event of a partial source system outage impacting ClinicalConnect users, a notification will be posted to the System Notices page per above. In the event of the HITS' email system being unavailable, Participant Organizations can call the HITS Helpdesk (905) 521-2100 x43000, and a recorded message will indicate the current status of ClinicalConnect or check the System Notices webpage identified above.

Obligations of Data-Contributing Organizations

Data-contributing organizations' Central Point of Contact, or their delegate, must notify HITS regarding changes to their information systems that may impact the ClinicalConnect service. The HITS Application Support team, in conjunction with the ClinicalConnect Program Office, will review all change notifications received from data contributors to ensure that changes will not adversely impact the technology or operational environment of ClinicalConnect and may contact the CPC to coordinate testing if appropriate/required; any change, including source system downtimes, that impacts the ClinicalConnect user experience will be communicated by the HITS

Helpdesk to ClinicalConnect users so they're aware of the timing associated with work being performed on source systems.

In general, data-contributing organizations must:

- Identify and provide contact information for the organization's ClinicalConnect CPC – the individual(s) responsible for their data integration with ClinicalConnect, as well as their organization's Helpdesk (if applicable), using the Contact Information Form provided by the ClinicalConnect Program Office. If the designated CPC changes, Participant Organizations must provide contact information for a replacement by emailing ccimpactreview@hhsc.ca.
- Provide access to applicable staff to solicit information and expertise with respect to the contribution of data from the organization's information system.
- Provide testing resources and conduct upgrade or regression testing as required/appropriate/identified to maintain the integrity of the application integration with partner/Participant Organization systems.
- **Include the 'ClinicalConnect service' in their change management processes, which means providing:**
    - **Immediate notice** of any unplanned outages involving the organization's health information system, that impact the ClinicalConnect user community
    - **At least three months' notice** of any major upgrade planned for the organization's health information system (that will result in a source system downtime, may require modifications to the ClinicalConnect integration and/or may require testing to ensure the change is not adversely impacting ClinicalConnect)
    - **At least two weeks' notice** of any other kind of planned update or maintenance to the organization's health information system, including new or updated report types (that may impact a user's access to or view of data from the source system).

These notifications from the organization must be emailed to ccimpactreview@hhsc.ca. Unplanned outage notifications should also be made by phone to the HITS Helpdesk at 905-521-2100 ext. 43000. Ensuring HITS is well aware of planned or unplanned outages will enable its Helpdesk to create sufficient awareness amongst the ClinicalConnect user community.

Organizations that contribute data to the ConnectMyHealth Patient Portal should also review the ConnectMyHealth Support Services Reference Guide available here:
https://info.clinicalconnect.ca/CC/healthcare/connectmyhealth-documents

Conversely, HITS will provide notice to all Participant Organizations' end users of any changes that are expected to impact the ClinicalConnect service in a manner consistent with the Service Provider's change management standards and processes. The HITS Change Advisory Board (CAB) assesses and approves all HITS-driven changes to software, hardware, and systems.

Enhancement Requests for ClinicalConnect & Ancillary Online Systems

- All net new project, service or enhancement requests should be submitted by completing the appropriate Enhancement Request Form available from https://info.clinicalconnect.ca/CC/healthcare/enhancements. CPCs must follow the submission instructions as included in the form and explained on the Enhancement Request page of the ClinicalConnect information website.
- Only Enhancement Request forms completed and submitted by the Participant Organization's Central Points of Contact (CPC) will be accepted.
- It's important to note that enhancement requests are submitted at an 'organization' level, meaning requests should be submitted that will benefit the organization, as opposed to only a small group of users within the organization. Identifying enhancements with this in mind will help ensure widespread benefit to

users at similar Participant Organizations who have access to the portal from across the continuum of care. This approach will assist the ClinicalConnect Program Office's Enhancement Request Committee to prioritize the request and determine its feasibility for the ClinicalConnect user community as a whole.
- The Enhancement Request Committee reviews requests, validates and prioritizes enhancements that require a change to the portal's current design/operation. This includes consideration of potential costs to make the requested change. The Enhancement Request Committee Lead provides regular updates to the CPC about the status of their enhancement request, and may require additional information about the request.
- If the enhancement request is approved, it will be scheduled for implementation accordingly, taking into account the enhancement's complexity and the ClinicalConnect release cycle roadmap/schedule.
- Communications to the ClinicalConnect user community will be issued as appropriate in the form of notices from the HITS Helpdesk to create awareness of the change.

Contact Information

Questions about the ClinicalConnect Program Office's support services should be emailed to support@clinicalconnect.ca.