

USER ACCESS MANAGEMENT POLICY

1 INTRODUCTION

The BC Medical Quality Initiative (BC MQI) program makes the provincial Credentialing and Privileging (C&P) databases, privileging dictionaries, and CACTI modules (known as the C&P system) available for use to participating health organizations (HOs).

The BC Medical Quality Initiative Office (BC MQIO) is responsible for the administration of the BC Medical Quality Initiative, including the C&P system, and for providing related support services as defined in the Participation and Information Sharing Agreements.

As part of their duties, the BC MQIO will develop, comply with, and make available to the participating health organizations, the policies, protocols, standard operating procedures and other operational documents as necessary for the smooth and effective functioning of the BCMQIO and the performance of its duties and services.

A BC MQIO developed policy or procedure will not be binding on a participating health organization if it would cause that HO to be non-compliant with its own legal, privacy, or security requirements. Each HO has the option to have their legal counsel review the BC MQI policies and procedures that impact them to ensure alignment with their HO's internal policies and procedures

This BCMQIO policy is specific to the provisioning and de-provisioning of user access to the C&P system applications and modules.

1.1 Purpose

The objectives of this policy are to:

- comply with PHSA's Access Management policy, and best practices;
- ensure that all access actions are traceable to an identifiable individual or process;
- ensure that access to the C&P software and related information is controlled and effectively administered; and
- ensure that only valid, authorized and authenticated users are permitted to access the C&P software and information.

1.2 Scope

This policy applies to all BC MQIO and health organization staff who authorize, administer and/or monitor access to the C&P system.

1.3 Exceptions

None

1.4 Compliance

Failure to comply with this policy could result in disciplinary action resulting from undetected, and/or unauthorized access, use or disclosure of C&P system data.

| | | | | |
|--|--------------|--------------|--------------|--------------|
| Released: | 01/SEPT/2021 | Next Review: | 01/SEPT/2024 | Page 1 of 10 |
| This document has been prepared solely for use by the BC MQIO and health organizations participating in the provincial Credentialing & Privileging (C&P) system. A printed copy of this document may not reflect the current electronic version stored on the BC MQIO SharePoint site. | | | | |

2 POLICY

2.1 Policy Statement #1 – Access Management Procedures

BC MQIO must have formal user access management procedures in place that include:

- instruction on how-to validate the identity of users before providing access to the C&P systems and information;
- instructions on how-to ensure that all access to the C&P system is approved (using the prescribed User Access Request Form), by an authorized director, manager, supervisor or delegate appointed for such purposes;
- instructions on how-to provision and to de-provision users, and maintain up-to-date access privileges of users;
- a formal User Access Request form and associated user acknowledgement of the C&P system Terms of Use; and
- instructions on how-to provide access to third-parties (external users/non-HO affiliated users), or providing data extracts from the C&P System.

BC MQIO must provide each HO with scheduled reports to support the review of that HO's C&P system user access (e.g. User Activity Monitoring reports and each HO's-Cactus Prod User List report).

2.2 Policy Statement #2 - Access Authorization

Using the prescribed User Access Request form, a health organization's director of medical affairs, or delegate, is responsible for authorizing BC MQIO's system administrator when access actions are required for that HO's C&P users (e.g. user activation, changes in user permissions, user deactivation), and as required, to create, update or deactivate the user's Active Directory account for the C&P System.

Using the prescribed User Access Request form, the provincial director of the BC Medical Quality Initiative, is responsible for authorizing BC MQIO's system administrator when C&P access actions specific to BC MQIO staff are required (e.g. user activation, changes in user permissions, user deactivation), and as required, to create, update or deactivate the user's Active Directory account for the C&P System.

2.3 Policy Statement #3 – User Change Notification

A health organization's director of medical affairs (or delegate), must notify BC MQIO's system administrator when an employee's status changes as the result of a promotion, demotion, removal from a user group, re-assignment, transfer or other change that may affect a HO's employee's access privileges to access C&P data. This notification can be completed using the prescribed User Access Request form, or by sending BC MQIO an email containing the pertinent information.

Using the prescribed User Access Request form (or an email), the provincial director of the BC Medical Quality Initiative, must notify BCMQIO's system administrator when a BC MQIO employee's status changes as the result of a promotion, demotion, removal from a user group, re-assignment, transfer or other change that may affect a BC MQIO employee's access privileges to C&P data.

| | | | | |
|--|--------------|--------------|--------------|--------------|
| Released: | 01/SEPT/2021 | Next Review: | 01/SEPT/2024 | Page 2 of 10 |
| This document has been prepared solely for use by the BC MQIO and health organizations participating in the provincial Credentialing & Privileging (C&P) system. A printed copy of this document may not reflect the current electronic version stored on the BC MQIO SharePoint site. | | | | |

BC MQIO system administrator must review the affected employee's C&P privileges based on their status change, and update as applicable. BC MQIO must retain the processed User Access Request form (or email), as part of the Cactus user access audit documentation.

2.4 Policy Statement #4 – De-Provisioning User Accounts

The HOs are responsible for maintaining Active Directory accounts for their employees. In addition, within **5 working days** of when it becomes known that a C&P system user is leaving (or has left), a HO, that HO's director of medical affairs, or delegate, must instruct the BC MQIO to remove the user's C&P system access privileges on a specific date. Ideally, the last day of the user's work (related to C&P use) will be concurrent with their last day of C&P access.

The BC MQIO is responsible for maintaining Active Directory accounts for their staff. In addition, within **5 working days** of when it becomes known that a BC MQIO C&P system user is leaving (or has left) the BC MQIO, the provincial director of the BC Medical Quality Initiative must instruct the BC MQIO system administrator to remove the user's C&P system access privileges. Ideally, the last day of the user's work (related to BC MQIO C&P use) will be concurrent with their last day of C&P access.

BC MQIO must comply with de-provisioning requests **immediately** upon receipt.

2.5 Policy Statement #5 – User Access Roles

An authorized C&P user must only have access to information based on their authorized User Group (as defined in an approved C&P Security Access Model), and their approved User Access Request form.

A health organization's director of medical affairs, or delegate, will ensure that their HO's C&P user access requests are consistent with that person's job responsibilities (e.g. access to health organization only, or to provincial information), and are based on the privacy principles of "need-to-know" and "least privilege".

The provincial director of the BC Medical Quality Initiative, will ensure that their BCMQIO user access requests are consistent with that person's job responsibilities, and are based on the privacy principles of "need-to-know" and "least privilege".

Privacy principles of Need-to-know and least privilege are described below:

- **Need-to-know** - users will be granted access to the C&P system only where that access is required to fulfill their roles and responsibilities.
- **Least privilege** - users will be given the minimum system privileges necessary to fulfill their roles and responsibilities. *Note: this is **not related to clinical privileges**, but to system user privileges such as access to information (e.g. forms), and allowed user functions (e.g. read, update, delete).*

2.6 Policy Statement #6 – Privacy Obligations

All persons requesting access to the C&P system must complete the prescribed C&P User Access Request form, and acknowledge that they will comply with the defined C&P Terms of Use.

| | | | | |
|--|--------------|--------------|--------------|--------------|
| Released: | 01/SEPT/2021 | Next Review: | 01/SEPT/2024 | Page 3 of 10 |
| This document has been prepared solely for use by the BC MQIO and health organizations participating in the provincial Credentialing & Privileging (C&P) system. A printed copy of this document may not reflect the current electronic version stored on the BC MQIO SharePoint site. | | | | |

Non-compliance with the Terms of Use could result in immediate termination of a user’s access privileges and further disciplinary action.

2.7 Policy Statement #7 – Segregation of Duties

Roles and functions responsible for authorizing requests for provisioning, de-provisioning or other changes to a user’s access to the C&P system, and the roles and functions responsible for carrying out those requests, must be segregated.

Segregation of C&P duties applies to both the health organizations staff and to BC MQIO staff.

2.8 Policy Statement #8 – Verification of User Accounts & Roles

To detect dormant accounts and accounts with excessive access privileges, a health organization’s director of medical affairs, and the provincial director of the BC Medical Quality Initiative (or their delegates), must complete a monthly review of their users’ accounts and access rights. Examples of dormant accounts, or accounts with excessive privileges include:

- an active account assigned to external contractor, vendor or employee that no longer works for an HO or the BC MQIO;
- an active account with access rights for which the user’s role and responsibilities no longer require access.;
- system administrative rights or permissions (including permissions to change the security settings or performance settings of a system) granted to a user who is not an administrator; and
- unknown active accounts.

3 KEY RESPONSIBILITIES

| Organization | User Access Management Responsibilities | Related Policy Statement |
|--------------|---|--|
| BC MQIO | <ul style="list-style-type: none"> • to ensure that formal C&P system user access management procedures are in place; | <ul style="list-style-type: none"> • Policy Statement #1 |
| | <ul style="list-style-type: none"> • to ensure that an approved User Access Request form is in place and available for HOs and/or BC MQIO use; | <ul style="list-style-type: none"> • Policy Statement #1 |
| | <ul style="list-style-type: none"> • monthly, to generate, and release to the HOs, a HO-Cactus Prod User List report (specific to each HO) that defines that HO’s C&P user accounts and privileges; | <ul style="list-style-type: none"> • Policy Statement #1 |
| | <ul style="list-style-type: none"> • in accordance with the prescribed schedule, to provide User Activity Monitoring reports to the HOs for their review; | <ul style="list-style-type: none"> • Policy Statement #1 |
| | <ul style="list-style-type: none"> • to complete, and approve a User Access Request forms for new, or changes to existing, BC MQIO C&P user accounts; | <ul style="list-style-type: none"> • Policy Statement #2 • Policy Statement #3 |
| | <ul style="list-style-type: none"> • to manage the BC MQIO employees’ Active Directory accounts; | <ul style="list-style-type: none"> • Policy Statement #4 |

USER ACCESS MANAGEMENT POLICY

| Organization | User Access Management Responsibilities | Related Policy Statement |
|---|--|---|
| | <ul style="list-style-type: none"> to provision and de-provision user accounts in response to a complete, and approved, User Access Request form; | <ul style="list-style-type: none"> Policy Statement #2 Policy Statement #4 |
| | <ul style="list-style-type: none"> to update user access system privileges per approved User Access Request forms (or email); | <ul style="list-style-type: none"> Policy Statement #3 |
| | <ul style="list-style-type: none"> monthly, to review the BC MQIO's HO-Cactus Prod User List report to ensure that BC MQIO user access and privileges are valid, and up-to-date; | <ul style="list-style-type: none"> Policy Statement #5 Policy Statement #8 |
| | <ul style="list-style-type: none"> in accordance with the prescribed schedule, to review the BC MQIO User Activity Monitoring (UAM) reports to determine unauthorized BC MQIO user activities; | <ul style="list-style-type: none"> Policy Statement #5 <p><i>Note: Also reference the User Activity Monitoring Policy and Procedure documents.</i></p> |
| | <ul style="list-style-type: none"> to ensure that all BCMQIO staff requesting access to the C&P system have acknowledged the C&P system Terms of Use prior to provisioning their user account; and | <ul style="list-style-type: none"> Policy Statement #6 |
| | <ul style="list-style-type: none"> to ensure that BCMQIO roles for authorizing BC MQIO staff user access to the C&P system are segregated from the roles responsible for actioning the request. | <ul style="list-style-type: none"> Policy Statement #7 |
| Participating Health Organizations | <ul style="list-style-type: none"> to ensure that the prescribed User Access Request forms are complete, and approved, prior to releasing to BC MQIO; | <ul style="list-style-type: none"> Policy Statement #2 Policy Statement #3 |
| | <ul style="list-style-type: none"> to manage the HO's C&P user's Active Directory Account; | <ul style="list-style-type: none"> Policy Statement #4 |
| | <ul style="list-style-type: none"> to notify the BC MQIO of pending, or recent C&P user terminations, or other changes to a C&P user's work status (using the User Access Request form or email); | <ul style="list-style-type: none"> Policy Statement #2 Policy Statement #4 |
| | <ul style="list-style-type: none"> in accordance with the prescribed schedule, to review the User Activity Monitoring reports to determine unauthorized user activities; | <ul style="list-style-type: none"> Policy Statement #5 <p><i>Note: Also reference the User Activity Monitoring Policy and Procedure documents.</i></p> |
| | <ul style="list-style-type: none"> monthly, to review the HO's -Cactus Prod User List report to ensure that user access and privileges are valid, and up-to-date. | <ul style="list-style-type: none"> Policy Statement #5 Policy Statement #8 |

Released:

01/SEPT/2021

Next Review:

01/SEPT/2024

Page 5 of 10

This document has been prepared solely for use by the BC MQIO and health organizations participating in the provincial Credentialing & Privileging (C&P) system. A printed copy of this document may not reflect the current electronic version stored on the BC MQIO SharePoint site.

| Organization | User Access Management Responsibilities | Related Policy Statement |
|--------------|--|---|
| | <ul style="list-style-type: none"> to ensure that HO staff requesting access to the C&P system have acknowledged the C&P system Terms of Use portion of the User Access Request form; and | <ul style="list-style-type: none"> Policy Statement #6 |
| | <ul style="list-style-type: none"> to ensure a segregation of duties of roles and responsibilities. | <ul style="list-style-type: none"> Policy Statement #7 |

4 RELATED BC MQI DOCUMENTS

- BC MQIO - User Access Management Procedure
- BC MQIO - User Access Request Form
- BC MQIO - UAM - Monitoring Policy
- BC MQIO - UAM - Monitoring Procedure
- BC MQIO - Security Access Model (SAM) Management Policy
- BC MQIO - Security Access Model (SAM) Management Procedure
- BC MQIO - Breach Management Policy
- BC MQIO - Breach Management Procedure & Checklist

5 RELATED DOCUMENTS

- PHSA IAP-020 - Privacy and Confidentiality Policy
- PHSA, VCH, PHC - Information Security Policy
- PHSA, VCH, PHC - Access Management Policy

6 LINKS TO KEY REFERENCES

- 1) PHSA Information Access & Privacy:
<http://2pod.phsa.ca/quality-safety/privacy/Pages/default.aspx>
- 2) PHSA Information Management/Information Technology Services (IMITS):
<http://2pod.phsa.ca/our-phsa/browse-by-department/Pages/Information-Management-Information-Technology-Services-IMITS.aspx>
- 3) PHSA Policies & Procedures:
[PHSA SHOP \(healthcarebc.ca\)](http://www.healthcarebc.ca/PHSA_SHOP)
- 4) PHSA Legal Services:
<http://2pod.phsa.ca/our-phsa/browse-by-department/Pages/Legal-Services.aspx>
- 5) BC MQI Teamsite:
<http://our.healthbc.org/sites/CPSolutions/SitePages/Home.aspx>
- 6) BC *Freedom of Information and Protection of Privacy Act*:
http://www.bclaws.ca/Recon/document/ID/freeside/96165_00

7 VERSION CONTROL

| VERSION CONTROL | | |
|-----------------|---------|---|
| Date | Version | Version Notes |
| March 15, 2018 | V1.0 | Approved and released by BC MQI. |
| July 10, 2021 | V2.0 | Draft released for review. |
| August 27, 2021 | V3.0 | Draft updated to reflect release date of September 1, 2021 and next review date of September 1, 2024. <i>No feedback was received from the health authorities related to this policy.</i> |
| | | |
| | | |

8 APPENDICES

8.1 Appendix A: Definitions

| Term | Definition |
|--------------------|--|
| Access | A privilege to use computer information in some manner. A user might be granted read access to a file, meaning that the user can read the file but cannot modify or delete it. The C&P system (Cactus software) has several different types of access privileges that can be granted or denied to specific users or groups of users as defined in the Security Access Model. |
| Authorized User(s) | Any employee or independent contractor of a participating health organization, or the BC MQIO, that is authorized by his or her employer or principal to access the C&P databases subject to the Security Access Model, and to controls implemented by BC MQIO. |
| BC MQI | The BC Medical Quality Initiative Program under which the C&P databases and provincial privileging dictionaries are made available for use to the participating health organizations, and administered by the BC MQIO, in accordance with the terms of the PPCPP Participation Agreement under the direction of PMSEC. |
| BC MQIO | The BC Medical Quality Initiative Office is tasked to administer the BC MQI including the C&P databases and privileging dictionaries and to provide certain support services (as defined in the Participation Agreement) to the participating health organizations regarding their use of the C&P system. The BC MQIO is within, and administered by, the Quality, Safety & Outcome Improvement department of PHSA. PMSEC is responsible for the governance and strategic direction of both the BC MQIO and the BC MQI. |
| BC MQIO Staff | Any employee of PHSA, or another participating organization, where that employee is working under the direction of PHSA, or any independent contractor of PHSA, who perform the duties of the BC MQIO. |
| CACTUS | Former name of the vendor providing the C&P system. Current vendor is "symplr". <i>Note: the term "Cactus" is generally used to refer to the C&P system.</i> |
| C&P | Provincial Practitioner Credentialing & Privileging System (C&P) that includes Privileging Dictionaries, symplr (formerly Cactus) software |

| Term | Definition |
|-----------------------------|--|
| | databases as defined in the Information Sharing Agreement (e.g. Application Manager and symplr Provider), and Cactus software modules (e.g. Committee Manager, Provider Directory, etc.). |
| Employee | As defined in the BC <i>Freedom of Information and Protection of Privacy Act</i> : "employee", in relation to a public body, includes <ul style="list-style-type: none"> (a) a volunteer, and (b) a service provider |
| FIPPA | <i>BC Freedom of Information and Protection of Privacy Act</i> |
| HO's | Health organizations comprised of BC health authorities and their affiliates participating in the Provincial Practitioner Credentialing & Privileging Program (C&P). Including: <ul style="list-style-type: none"> • Fraser Health Authority (FHA) • Interior Health Authority (IHA) • Northern Health Authority (NHA) • Providence Health Care Society (PHC) • Provincial Health Services Authority (PHSA) • Vancouver Coastal Health Authority (VCH) • Vancouver Island Health Authority (VIHA) |
| Participating Organizations | Health organizations (and their affiliates) that are participating in the Provincial Practitioner Credentialing & Privileging System. |
| PMSEC | The Provincial Medical Services Executive Council (previously known as the Physician Services Strategic Advisory Committee or PSSAC), which is comprised of the Vice Presidents of Medicine or equivalents from each of the Participating Organizations and a representative from the British Columbia Ministry of Health, and any successor to such Council that may be constituted from time to time. |
| PPCPP | Provincial Practitioner Credentialing & Privileging Program |
| symplr | symplr (formerly Cactus) is the name of the software vendor providing the web-based C&P system software. symplr: Healthcare Governance, Risk & Compliance Solutions |
| UAM | User Activity Monitoring – module provided by symplr. |
| User | All persons authorized, or not, to access the C&P resources and data. This includes employees and non-employees including but not limited to physicians, researchers, volunteers, students, and contractors, partnership organization staff, or any other person accessing the C&P |

BC MQIO
USER ACCESS MANAGEMENT POLICY

| Term | Definition |
|------|--|
| | from a HO facility, a home office, and a remote location or via a mobile device. |

END