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, BC MQIO will develop, comply with, and make available to the participating health organizations, policies, protocols, standard operating procedures and other operational documents as necessary for the smooth and effective functioning of the BC MQIO 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 BC MQIO policy is specific to the provisioning and de-provisioning of user access to the C&P system applications and modules.

1.1   Purpose

The purpose of this policy is to:

- ensure that access to the C&P software and related information is controlled and effectively administered;
- ensure that only valid, authorized and authenticated users are permitted to access the C&P software and information; and
- ensure that user access to the C&P software and information is in compliance with the participating health organizations' policies.

1.2   Scope

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

1.3   Exceptions

None

Released:	15/MAR/2018	Next Review:	15/MAR/2021	Page 1 of 7

2   POLICY

2.1   Policy Statement #1
Documented access management must be in place that outlines procedures and oversight mechanisms to govern and administer access to the C&P systems and information. This documentation is to include:

- how-to validate identity of users before providing access to the C&P systems and information;
- how-to ensure that all access to the C&P system is approved by an authorized director, manager, supervisor or delegate appointed for such purposes;
- how-to provision and to de-provision users, and maintain up-to-date access privileges of users; and
- how-to provide access to third-parties (external users/non-HO affiliated users) or for extracting data from the C&P System.

See Related Documents (Related Documents) and References (References) sections of this document for additional information.

2.2   Policy Statement #2
An authorized C&P user must only have access to information restricted to their authorized User Group based on an approved User Access Request form and one or more approved C&P Security Access Models (SAMs).

2.3   Policy Statement #3
All C&P system users must comply with:

- the provisions of the BC *Freedom of Information and Protection of Privacy Act*, and
- the organization policies and procedures specific to the protection and safeguarding of information from unauthorized disclosure in place at their HO.

2.4   Policy Statement #4
User access to the C&P system must only be approved based on the user's role in accordance with the following principles:

- **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 privileges necessary to fulfill their roles and responsibilities. *(Note: this is **no**t related to clinical privileges, but to system user privileges, i.e. read, update, delete, etc.).*

2.5   Policy Statement #5
Inactive C&P user IDs, or dormant user accounts, must be disabled promptly. To preserve the integrity of audit logs, User-IDs or accounts are not to be deleted.

2.6   Policy Statement #6
Audit logs should contain sufficient detail to ensure that users can be held accountable for their actions, and that events and processes can be reconstructed, and security violations detected to serve as evidence in disciplinary or legal proceedings.

2.7 Policy Statement #7

Existing user accounts and access rights must be reviewed at **least semi-annually** to detect dormant accounts and accounts with excessive privileges. Examples of dormant accounts and accounts with excessive privileges include:

- an active account assigned to external contractors, vendors or employees that no longer work for BC MQIO or an HO;
- an active account with access rights for which the user's role and responsibilities do not 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   RESPONSIBILITIES AND COMPLIANCE

3.1 Responsibilities

3.1.1 BC MQIO System Administrator
- enabling and disabling accounts, and monitoring and auditing access to the C&P databases;
- validating that user access is necessary to meet a BC MQIO and/or participating HO's business or operational objective or initiative;
- periodically performing reviews of user privileges to ensure access privileges are current and up-to-date;
- implementing, and monitoring, appropriate security and privacy measures to protect personal information that can be accessed by authorized users,
- generating and releasing a User List Report for review and approval by each HO's user access delegate, and
- reviewing and maintaining audit logs.

3.1.2 BC Clinical and Support Services (BCCSS)
- BCCSS is responsible for ensuring that processes are in place to provide access support, including password resets.

3.1.3 Participating Health Organizations
- requesting BC MQIO to activate, modify and/or deactivate a user's access;
- managing C&P users' Active Directory Accounts;
- reviewing and validating their HO's C&P users' access privileges (at least semi-annually) using a formal process; and
- implementing and monitoring appropriate security and privacy measures to protect personal information that can be accessed by authorized users.

3.2 Compliance

Failure to comply with this Policy may result in disciplinary action.

Released:	15/MAR/2018	Next Review:	15/MAR/2021	Page 3 of 7

4 RELATED DOCUMENTS
- Third-Party Remote Access Policy
- User Access Management Procedure

5 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(s).
Authorized User(s)	Any employee or independent contractor of a participating Health Organization that is authorized by his or her employer (or principal) to access any, or all, of the C&P system, subject to the Security Access Model and to controls implemented by the BC MQIO.
BC MQI	The BC Medical Quality Initiative program under which the C&P databases and 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 Participation Agreement and 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.
BCCSS	BC Clinical and Support Services that provide non-clinical support services to BC health authorities, including the organizations participating in the PPCPP.
C&P	Provincial Practitioner Credentialing & Privileging System (C&P) that includes Privileging Dictionaries, Cactus (and/or symplr) software databases as defined in the Information Sharing Agreement (e.g. AppCentral and Visual Cactus) and Cactus software modules (e.g. iCommittee, iDirectory, etc.).
Deprovisioning	User deprovisioning (aka off-boarding) is the process of removing access of an

TERM	DEFINITION
	individual user to an organization's resources.
FIPPA	*BC Freedom of Information and Protection of Privacy Act* http://www.bclaws.ca/Recon/document/ID/freeside/96165_00
HOs	Health organizations comprised of BC health authorities and their affiliates participating in the Provincial Practitioner Credentialing & Privileging Program (C&P). Including: • 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)
HO's User Access Delegate	Person(s) at each health organization with the delegated authority to approve additions and/or changes to the C&P system Security Access Models.
IMITS	PHSA Information Management/Information Technology Services
Participating Organizations	Health organizations comprised of BC health authorities and their affiliates participating in the Provincial Practitioner Credentialing & Privileging Program (C&P).
PHSA	Provincial Health Services Authority
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.
Provisioning	User access provisioning (aka on-boarding) is the creation management and maintenance of an end-user's access and privileges to access the C&P system.
Security Access Model (SAM)	The C&P Security Access Models (SAMs) are user role-based access control (RBAC) methods used to regulate access to the C&P system databases and modules. Depending on their role, an individual user can be given privileges to perform one or more types of specific tasks, such as read (view), create, update, or delete data. The C&P SAMs are approved by the participating health organizations.

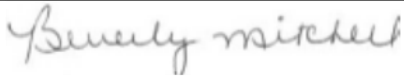| TERM	DEFINITION
Support Services	Those support services to be provided by the BC MQIO to the participating health organizations, as defined in the BC MQIO Support Services Manual.
User	All persons authorized to access the C&P resources and data. This includes employees and non-employees including, but not limited to, physicians, researchers, volunteers, students, and contractors, partnership organization staff, or any other person accessing the C&P from a HO facility, a home office, and a remote location or via a mobile device.
User Access Request Form	Form initiated and approved by a health organization to request user access, reactivate user access, modify user access or deactivate user access as related to the C&P system.

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:
   http://2pod.phsa.ca/workplace-resources/policies-procedures
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   APPENDICES

None

VERSION CONTROL

FIRST ISSUED:	15-NOV-2017 (Version 1.0)		
APPROVING BODY:	BC MQIO		
FINAL SIGN OFF:	**Name**	**Title**	**Signature & Date Signed**
	Beverly Mitchell	Provincial Director, Provincial Practitioner Credentialing & Privileging Program	February 19, 2108
DEVELOPED BY:	**Name**	**Dept.**	**HO**
	Moira E. Connor	BC MQIO	PHSA
	Joan Poon	BC MQIO	PHSA
	Michael Ng	BC MQIO	PHSA
OWNER(S):	Beverly Mitchell, Provincial Director, Provincial Practitioner Credentialing & Privileging Program		
POSTED DATE:	**15 MARCH 2018**		
VERSION:	**V 2.0**		
REVISION:	**Name of Reviser**	**Description**	**Date**
	Moira E. Connor & Michael Ng	Updated to reflect review feedback and additional content.	February 2018