SECURITY ACCESS MODEL - 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 development and on-going management and administration of the Security Access Models used to define and control access to the C&P system.

1.1 Purpose

The purpose of this policy is to ensure that both the BC MQIO and the participating health organizations are aware of their obligations to control and effectively administer access to the C&P system.

1.2 Scope

The C&P system Security Access Models (SAMs) are used to control user access to information that is appropriate, and necessary to a user's role. For each C&P system application (e.g. Application Manager, and symplr Provider) and/or CACTi modules, SAMs are developed based on input from each of the HOs specific to their users' access requirements.

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.

2 POLICY

2.1 Policy Statement #1

All user access to the C&P system must be controlled through the applicable C&P Security Access Model and supporting user assignment matrices, and through approved User Access Request Forms.

2.2 Policy Statement #2

The C&P Security Access Models must be reviewed and approved by each of the participating health organizations and the BC MQIO prior to implementation. Any updates to existing Security Access Models roles (and/or privileges assigned to those roles), must be reviewed and approved by a director level position (or equivalent) at each participating HOs.

2.3 Policy Statement #3

The C&P system's Security Access Models must be managed over time through version control. A copy of approved SAMs (and any subsequent addendums and/or amendments) must be stored by both the approving HOs and by the BC MQIO. Previous versions of SAMs must be archived.

2.4 Policy Statement #4

Quarterly, a HO's matrix of users assigned to approved C&P roles must be reviewed by that HO to validate appropriate user privileges. The HOs will send BC MQIO a request for any changes to the HO's user matrix as soon as the requirement for a change is discovered.

BC MQI must also review a matrix of users assigned to approved BC MQIO roles to validate appropriate user privileges, and if required, update user privileges.

Changes to BC MQIO and HO user matrices will be processed within three (3) days of receipt.

2.5 Policy Statement #5

BC MQIO and the HOs must adhere to the following privacy principles when determining the user role assignments:

- **Need to know**: users should only have access to information that is necessary to fulfill their roles and responsibilities of the SAM group they have been assigned to.
- **Least privilege**: users should only be provided with the **minimum** level of privileges required to fulfill their roles and responsibilities of the group they have been assigned to.

2.6 Policy Statement #6

As defined in the executed Provincial Practitioner Credentialing & Privileging Program, Participation Agreement:

*Each Participating Organization will safeguard the security of the Database as set out in the **Security Access Model** and the ISA.*

*Should it be determined that a Breach (as defined in the ISA) has occurred where Practitioner Personal Information has been inappropriately accessed, used or disclosed by any Authorized User or where the Database has been used by any Authorized User in contravention of the **Security***

***Access Model**, BC MQIO has the right to suspend or terminate such Authorized User's access to the Database.*

3 KEY RESPONSIBILITIES

3.1 BC MQIO

- to ensure that role-based access controls are in place in compliance with the PHSA, VCH, PHC Role-Bases Access Control policy;
- to update and maintain the Security Access Models in accordance with approved requests from HO's impacted by those requests;
- to update and maintain the HOs user access matrices in accordance with approved requests from the HO responsible for the user; and
- to develop and implement an archiving policy for SAMs, and other C&P related policies, protocols, standard operating procedures and other operational documents.

3.2 Health Organizations

- to provide input to the development and maintenance of C&P SAMs and approve or reject completed SAMs and subsequent addendums and/or amendments;
- to advise BC MQIO when changes to a user's work responsibilities should impact their existing access privileges to the C&P system;
- to validate user C&P role assignments and permissions at least quarterly;
- to ensure that user assignments to SAM roles are consistent with the privacy principles of "Need to Know" and "Least Privilege"; and
- to request BC MQIO to make updates to one of more SAMs as may be required from time to time.

4 RELATED BC MQI DOCUMENTS

- BC MQIO Security Access Model Management Procedure
- BC MQIO - UAM - Monitoring Policy
- BC MQIO - UAM - Monitoring Procedure
- BC MQIO - User Access Management Policy
- BC MQIO - User Access Management Procedure
- Provincial Practitioner Credentialing & Privileging Program, Participation Agreement (2015)

5 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 (including VPP):
   PHSA SHOP (healthcarebc.ca)

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

6 VERSION CONTROL

VERSION CONTROL		
Date	**Version**	**Version Notes**
Nov. 15, 2017	V1.0	Approved by BC MQI and released.
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. *No feedback was received from the health authorities related to this policy.*

7 APPENDICES

7.1 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	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.
CACTUS	Former name of the vendor providing the C&P system. Current vendor is "symplr".
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. Application Manager and symplr Provider) and Cactus software modules (e.g. Committee Manager, Provider Directory, etc.).
Data	Data, including Personal Information or Confidential Information that is either directly or indirectly deposited in, stored in, or accessed from the C&P system.
FIPPA	BC Freedom of Information and Protection of Privacy Act

TERM	DEFINITION
	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)
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.
symplr	symplr (formerly Cactus) is the software vendor providing the web-based C&P system software. symplr: Healthcare Governance, Risk & Compliance Solutions
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 from a HO facility, a home office, and a remote location or via a mobile device.
User Assignment Matrix	Typically, a spreadsheet that represents what job titles (and related users) are assigned to specific roles and groups as defined in the Security Access Model(s).

END