CPCSSN RCSSSP

CPCSSN Security Policy

Version 3.0

This document was prepared by:

Authors: Donald White and Lorne Kinsella

Contributors: Michael Cummings, Andy Gibb, Brian Forst, Rachael Morkem, Chad Herman, and Ken Martin

Version History

Date	Document Version	Document Revision History	Document Author/Reviser
2012/2015	1.0/2.0	Original documents	Ken Martin
11-24-2021	3.0	Initial draft	Don White/Lorne Kinsella
12-14-2021	3.0	Draft revision	Rachael Morkem/Chad Herman
01-19-2022	3.0	Final draft	Don White

Approvals

Date	Document Version	Approver Name and Title	Approver Signature
	3.0	Steering Committee Members	

CPCSSN RCSSSP

Table of Contents

Introduction

This document defines the *Information and Systems Security Policy* for the Canadian Primary Care Sentinel Surveillance Network **(CPCSSN)**. It:

- Establishes policy for the protection of the confidentiality, integrity, and availability of CPCSSN information assets (i.e., the combination of hardware, software, information, data, and operational environments that support CPCSSN in its provision of services)
- Establishes the responsibilities for information security within CPCSSN
- Establishes policy for the protection of CPCSSN hardware, software, information, data, and operational environments

Objective

The objective of this Information and Systems Security Policy is to provide CPCSSN management and staff direction and support for information security in each phase of CPCSSN project implementation and ongoing operations.

Need for an Information and Systems Security Policy

The information entrusted to CPCSSN represents a valuable and confidential asset, the management of which is a serious responsibility. By developing an *Information and Systems Security Policy* and procedures to manage and enforce it, those responsible for CPCSSN are better able to:

- Protect the security and integrity of health information entrusted to CPCSSN
- Protect CPCSSN's computer systems from misuse
- Minimize the impact of service interruptions by ensuring the continuous availability of critical systems
- Comply with applicable federal and provincial privacy regimes governing the collection and handling of personal information and personal health information.

Key Principles

- Confidentiality - data access shall be confined to those with specified authority to view the data
- Data Integrity - all information shall be properly maintained throughout the operational lifetime of the data
- System Availability - information shall be delivered promptly to authorized CPCSSN staff, researchers, stakeholders and contractors when needed

- Accountability - CPCSSN authorized staff, researchers, stakeholders and contractors shall remain aware of their roles and responsibilities with respect to security, and shall be accountable for them
- Compliance - Comprehensive and reliable procedures to detect and resolve security breaches shall be in place

Definitions

- CPCSSN Project – is an initiative sponsored by the Public Health Agency of Canada and with the approval of local research ethics boards to create a pan-Canadian database on chronic diseases from anonymized health information extracted from the EMRs of participating primary care providers (Sentinels) for public health surveillance and research.
- EMR – electronic medical record
- PHI – Personal Health Information
- ITM – Information Technology Manager for CPCSSN and the position responsible for security of CPCSSN data on the regional and National CPCSSN databases.
- CAC – the Queen's University Centre for Advanced Computing
- SRE – the CPCSSN Secure Research Environment

Scope

CPCSSN's policies and procedures around the management of EMR data are inclusive of privacy, encryption, and security considerations, as they ultimately serve to build and maintain relationships with patients and their family practitioners.

CPCSSN federates data from regional networks across Canada. The federated data, as well as regional network data are stored at the Centre for Advanced Computing (CAC) at Queen's University, which is PHIPA, HIPPA and ISO 27002 compliant, thereby making it the preferred site for the storage of health information.

This Information and Systems Security Policy applies to:

- National CPCSSN Core Server at Queen's Computing Centre
- Regional servers at Queen's Computing Centre
- Test server at Queen's Computing Centre (for approved secure researcher access)
- CPCSSN Secure Research Environment (SRE) Servers
- Firewall at Queen's Computing Centre
- Virtual private network (VPN) at Queen's Computing Centre
- Notebook and desktop computers in academic/health care settings that store any de-identified CPCSSN data
- Central repository database on central server at Queen's Computing Centre.

Roles and Responsibilities

CPCSSN Committee, management and staff recognize the importance of ensuring compliance with this Policy, as well as best practices and established procedures for data security and integrity.

Information Technology Manager (ITM)

The ITM is responsible for the implementation and enforcement of this Policy and shall have organizational security management responsibilities for:

- Management of IT infrastructure and data management functions in compliance with Information and Systems Security Policy
- Coordinating and working with regional data managers responsible for CPCSSN Data on regional databases to ensure the compliance with this Information Security Policy, as well as other CPCSSN Security Documents.
- Oversee the operations of the National CPCSSN Database at the CAC to ensure the ongoing security and integrity of CPCSSN data on the central and regional servers.

Queen’s Centre for Advanced Computing

The Queen’s Centre for Advanced Computing (CAC) is responsible for installation, configuration and maintenance of the physical servers, network, and security infrastructure.

CPCSSN Data Manager Responsibilities

The CPSSSN Data Managers are responsible for:

- administration and management of the CPCSSN regional servers which host the regional network EMR data.
- The CPCSSN Secure Research Environment (SRE) is managed and administered by the CPCSSN SRE Administrator, a part time role filled by a Data Manager.

CPCSSN Staff Responsibilities

Each CPCSSN staff member has the following privacy and security related duties:

- Adhering to CPCSSN’s Privacy Policy, terms of their signed Pledge of Confidentiality & Privacy for CPCSSN and other CPCSSN or regional network policies related to acceptable use of CPCSSN or regional network hardware, software, and network

- Safeguarding hardware, software, and personal information in their care from damage or corruption of data
- Ensuring that no breaches of computer security result from their actions
- Preventing the introduction of malicious software on CPCSSN computers by ensuring that such computers are never used for purposes other than the running of CPCSSN
- Reporting any suspected or actual breaches in security to the ITM

Availability

The following CPCSSN computer applications shall have at least two (2) individuals with the expertise to manage or administer them:

- Central and regional server IT assets, processes, and communications, including but not limited to the CPCSSN's ITM.
- Regional server IT assets, processes, and communications, including but not limited to the regional Data Manager.
- CPCSSN Secure Research Environment (SRE)

Physical and Environmental Security

Secure Areas

The data centre for the National CPCSSN database at a secure facility at Queen's University (CAC) is under 24-hour surveillance, with a security guard that monitors the premises, security cameras around the perimeter, and intrusion alert security system that is monitored by a 24-hour security company.

- Entrance to the CAC is restricted by physical access controls.
- Visitors to the CAC are signed in and always escorted on the premises
- The CAC is protected against external and environmental threats, including fire, floods, power failures, and other environmental failures
- No member of the public is permitted access to CPCSSN's regional and central data repositories at the CAC

Equipment Security

Workstations used by CPCSSN staff shall be situated and protected in accordance with CPCSSN Security Best Practices Checklist.

Equipment Maintenance

All information technology (IT) equipment hosting CPCSSN data at the CAC, including file servers, shall be covered by the Service Agreement with CAC.

All CPCSSN personal computer/terminal maintenance shall be covered by CPCSSN's in-house IT department. Where it is necessary to contract with a third party to provide such maintenance, the third party will be required to sign a CPCSSN Pledge of Confidentiality & Privacy.

Security of Equipment Off-Premises

CPCSSN file servers, data storage units, and the workstations contain confidential data. Decommissioning of such equipment at the regional networks shall be performed on premises except where extenuating circumstances prohibit this and then only with the approval of the regional data manager. At the central data repository housed by the Queen's Computing Centre, removal of any equipment housing CPCSSN data shall be supervised by CPCSSN's ITM.

Secure Disposal or Reuse of Equipment

Data storage devices must be purged of all data before disposal.

Computer System Security

- Access to all computers (i.e., desktop. , laptops, regional & central servers) used for CPCSSN purposes must be password protected including inactivity timer-based screen lockout
- All computers used for CPCSSN purposes must have an enabled firewall and anti-virus software
- All confidential information (i.e., practice/CPCSSN health care provider or patient data) must be stored in disk files that are protected by a strong password and 256-bit encryption (e.g. VHDX, WinZip, 7-Zip)
- All encrypted disk volumes are dismounted when not in use, including inactivity timer-based automatic dismount
- All confidential data stored on external media (e.g. CD, DVD, USB drive) disk files are protected by a strong password and 256-bit encryption
- All computer disk files containing confidential information are electronically erased/shredded before decommissioning
- Any data leaks/exposures or security incidents must be immediately reported to the Network Director and the ITM

Network Security

The CAC utilizes virtual private networks (VPNs), a system of data encryption and digital signatures, to create a secure portal to ensure data transferred over the Internet is protected in transit.

Connecting to a CPCSSN Core or Regional Server is only permitted through a secure Virtual Private Network (VPN) connection provided by the CAC.

VPN User Responsibilities

Each CPCSSN authorized staff, researcher, stakeholder and contractor shall be responsible for following CPCSSN's Security Best Practices Checklist, including but not limited to:

- Must not share Certificate Key or password with other persons
- Must not access CPCSSN with another person's Certificate Key and password
- Must choose passwords in accordance with provisions in the CPCSSN Security Best Practices Checklist

With the increase in CPCSSN Data Managers and users working remotely implementation of additional measure such as Two Factor Authentication (2FA) should be considered.

Mobile Computing and Teleworking

- Prior to accessing CPCSSN resources at the CAC, staff shall first complete CPCSSN's Security Best Practices Checklist and obtain approval from the ITM
- Remote access to CPCSSN is permitted for CPCSSN authorized staff, researchers, stakeholders, and contractors working outside of CPCSSN premises, provided that CPCSSN's Security Best Practices Checklist is complied with
- Access to CPCSSN from a public Internet connection is only permitted via the CAC VPN Network.

External / 3rd Party Access

Where trusted third-party partners are provided access to CPCSSN Regional Servers the following additional precautions must be taken.

- Prior to granting access to CPCSSN to authorized third parties, such as researchers or contractors, the Data Manager and CPCSSN Data Stewards will assess the potential risks to CPCSSN security

- Security will be addressed in writing in all third-party agreements involving access to, maintenance of, or service provision to, CPCSSN. Except where otherwise authorized by the Data Manager, third parties will be required to execute CPCSSN's Pledge of Confidentiality & Privacy for CPCSSN, prior to authorization to access CPCSSN resources.
- Third party user login account must have non-admin level account privileges
- Users must establish a secure connection via the Queens CAC OpenVPN network
- A Secure file transfer (SFTP) Server running on a separate virtual server shall be used for file transfers

Shared Network Storage

Shared network file-space is provided on the CPCSSN Core servers for the purpose of sharing and collaborating on datasets between regional networks.

- The Data Managers create and administer shared network folders as needed and are responsible to manage shared folder access, permissions, file maintenance and data retention policies.
- Files stored on shared network folders should be removed when they are no longer needed.
- Users must not attempt to access shared folders that are not specifically shared with them.

Exchange of Sensitive Information

Users must not transfer or otherwise send data containing PHI on physical media unless it is via encrypted mobile storage device and protected with strong encryption and password.

- PHI must never be transmitted by email or electronic messaging.
- With the exception of SFTP service provided for third party access, CPCSSN data transmitted via a VPN requires a two-stage security clearance process to ensure access is restricted to only those authorized CPCSSN personnel, contractors, or researchers.
- All CPCSSN data shall be encrypted during transmission to ensure message integrity.

Cryptographic Controls

All data shall be strongly encrypted during transmission to protect its confidentiality, integrity, and authenticity.

- Where used, private keys shall be always protected.
- Symmetric key lengths shall be at least 128 bits.

- Data used during system testing shall be treated as confidential data and shall be protected from unauthorized access and corruption of data integrity.

User Access Management

Access Control Policy

Access to CPCSSN applications shall be restricted to those who have a “need-to-use” access granted by the ITM or in the case of regional access, by the regional Network Director.

User Access Management

- Registration - All authorized staff, researchers, stakeholders and contractors must sign the CPCSSN Confidentiality agreement before access is granted to CPCSSN.
- Authentication - Users shall be authenticated at every login to CPCSSN through the VPN portal by entering their authorized Certificate Key and password that is unique to the user.
- Authorization - All users shall have the system and data access privileges permitted by their assigned role(s) and only those system and data access privileges permitted by their assigned role(s). The only users who shall have data access privileges to PHI on participating EMRs are the regional Data Managers or staff authorized by the regional Network Director.

Provisioning / De-provisioning

When staff join or leave CPCSSN:

- New CPCSSN staff and contracted personnel sign CPCSSN’s Pledge of Confidentiality & Privacy for CPCSSN prior to the enabling of user accounts and logins.
- The manager responsible for the employee shall inform the ITM when a new employee is onboarded.
- The ITM will manage creating user accounts on the CPCSSN Regional and Core Servers as needed.
- The CAC is responsible for creating and removing user accounts on the VPN network, CPCSSN Core Servers.
- Data Managers are responsible for user accounts on third party services such as Google Drive and Atlassian Bitbucket.
- The SRE Administrator is responsible for creation of user accounts on the CPCSSN SRE.
- Upon termination of employment or contract the ITM or, where applicable, the regional Data Manager shall terminate access privileges of each employee or contractor who had been

authorized to access CPCSSN. The ITM shall determine who shall be responsible for terminating access rights, as well as ensuring that such rights have been terminated.

Privileged Accounts

Every server has a root user or administrator user who can execute any command. Because of the power it has, the administrator account can be very dangerous if it is exposed.

- The CAC and CPCSSN Data Managers must not use the System Administrator (Windows) or root (Linux) account, rather their user accounts must have administrator level privilege. This ensures that all changes to the system can be logged for audit purposes.
- Direct login over a Remote Access connection using the system Administrator or Root account should be disabled on all servers.

Password Requirements

Passwords used to access CPCSSN computing systems must be strong.

A strong password is one that is more secure by virtue of being difficult for a machine or a human to guess. Password strength can be achieved by incorporating the following characteristics:

- A minimum of 12 characters
- A mixture of both uppercase and lowercase letters
- A mixture of letters and numbers
- Inclusion of at least one special character, e.g., ! @ # ?]

Password Expiration Policy

Passwords should not be set to expire. Expiration encourages the re-use of passwords and adding number at the beginning or end of the password. Passwords should be changed when a breach is suspected.

Password Best Practices

The following are considered best practices for password management:

- Accounts, logins, credentials, passwords, authentication keys or certificates must never be shared with others

- Firstly, be mindful where you store passwords. Do not write them on pieces of paper and hide them around the office.
- Do not use personal information like your birthday, hometown, pet names and other things that can connect you, the user, to the password. These are extremely easy to guess, especially by people who know you personally.
- Finally, do not use the same password for multiple accounts. By recycling passwords, you put yourself at significant risk. If an unauthorized user manages to get access to a single account, all other accounts with the same password may be in danger.

Use of a password manager such as LastPass, 1Password, KeePass, Keeper, Dashlane, etc. is strongly recommended. This allows the use very complex passwords that are impossible to guess or remember.

Intrusion Detection

The Queen's CAC employs intrusion detection on firewalls. As it is impossible to access the CPCSSN Servers without first accessing the Queen's CAC VPN and Firewall, additional intrusion detection systems are not needed on the CPCSSN Servers.

Auditing

File System Auditing

Where possible, CPCSSN shall have file auditing enabled to assist in detecting unauthorized changes or access to files.

- All CPCSSN record creation, access, updates, and changes on the central database shall be audited and logged in a secure audit trail.
- All logins to and logouts from a CPCSSN system shall be audited and logged in a secure audit trail.
- All secured audit trails shall be protected from unauthorized access or modification.
- All CPCSSN record creation, access, updates, and audit logging is done on the central CPCSSN data server and the accuracy of its clock synchronization shall be managed by Queen's Computing Centre.
- Windows File Auditing shall be enabled on all Windows Servers.

Service Auditing

Service auditing explores what services are running on the server, their protocols, and which ports they are communicating through. Being aware of these specifics helps configure attack surfaces in the system.

- Data Managers should review server configurations annually and disable or shutdown any services (IIS, FTP, etc.) that are not required.

Backup Policies

File servers and database servers housing CPCSSN data shall have backup regimes formalized in appropriate procedures that include regular backup of information, software, and operational logs.

Much of the data stored on CPCSSN Servers are subject to data retention and destruction policies of the academic institution, project, or province. .

Security in Development and Support Processes

Change Control Procedures

To minimize the corruption of information systems, there must be strict control over the implementation of changes. Therefore, formal change control procedures shall be enforced. These procedures shall ensure that:

- A formal agreement and approval for any change is obtained
- The proposed changes are reviewed to ensure that they will not be compromised by the changes
- The affected systems and software are identified
- Developers and system testers are given access only to those parts of the operational system necessary for their work
- Implementation is carried out in such a way as to minimize network disruption
-
- The system and operating documentation set is updated on the completion of each change and that old documentation is archived or disposed of
- A log of all changes is maintained

Restrictions on Changes to Software Packages

CPCSSN staff shall be responsible for maintaining software on their regional servers.

The CPCSSN SRE Administrator is responsible for the updating and maintaining software licenses within the SRE.

Compliance

CPCSSN complies with the privacy and security requirements of applicable federal and provincial privacy and health information protection laws.

CPCSSN management and staff shall ensure that all security procedures within their area of responsibility, including but not limited any contractors, are followed and that the provisions of this Policy and CPCSSN's Privacy Policy and Standard Operating Procedures for Privacy and Security Compliance are upheld.

Compliance Verification

Prior to major upgrades of software or systems, technical compliance checking, including where practical, vulnerability assessment and penetration testing, shall be carried out.

Technical compliance checking will involve the examination of operational systems to ensure that hardware and software controls have been correctly implemented. This compliance will be performed manually (supported by appropriate software tools, if necessary) by an experienced system security engineer or by an automated software package that generates a technical report for subsequent interpretation by a technical specialist.

Information Systems Audit Considerations

The CAC shall maintain an audit trail of all access to CPCSSN servers. The audit trail shall enable an auditor to identify the CPCCSN authorized staff, researchers, stakeholders, and contractors who accessed CPCSSN, as well as any unauthorized access, including the time and date of system access.

Policy Review

This Policy shall be reviewed:

- When there is a significant change in the scope or management of CPCSSN
- Prior to major upgrades of software, systems, or procedures
- In response to significant security incidents, new vulnerabilities, or major changes to the organizational or technical infrastructure of CPCSSN
- Annually.