Provincial Health Services Authority
Province-wide solutions. Better health.

PRIVACY AND SECURITY DECLARATION

Pharmacist Access to the Provincial eHealth Viewer ("CareConnect")

CareConnect access from your pharmacy worksite will provide you and your staff with direct access to a significant amount of clinical data about your patients from within BC Health Authorities and Ministry of Health systems. This clinical data, along with data from your own information system (e.g., pharmacy operating system, electronic medical record), (the "Data") can be targeted by organized criminals, and Data breaches can have a significant impact on your worksite and the wider system, potentially harming your reputation and reducing patient trust. Implementing appropriate privacy and security safeguards reduces this risk of patient information breaches.

This Privacy and Security Declaration details the requirements for granting of access to CareConnect and is informed by provincial privacy legislation (the BC *Personal Information Protection Act* "PIPA" or *Freedom of Information and Privacy Protection Act* "FOIPPA"), the College of Pharmacists of BC, the Office of the Information and Privacy Commissioner, the Ministry of Health, and by the Provincial Health Services Authority ("PHSA") Privacy and Security resources. *More information on each requirement is available in the Appendix.*

I declare that:

☐	1. The member of my worksite staff who is ultimately responsible for our privacy and security policies is: □ Myself □ Other (name)_____
☐	2. Documented privacy and security policies are communicated to all staff and external parties (e.g. vendors, suppliers, and partners) who have access to the worksite's computer system.
☐	3. Security awareness training is provided to worksite staff and yearly reviewed.
☐	4. My staff are aware of malicious emails and have been informed not to click links or open attachments that appear suspicious.
☐	5. My staff are aware of risks associated with using USB drives and other portable devices that may compromise my network.
☐	6. My staff are aware that passwords used for access to CareConnect are not permitted to be shared with other individuals or re-used for other services, and that the "Save password" feature in the browser is not used to access CareConnect.
☐	7. My worksite agrees to notify the CareConnect Team when a member of my staff no longer requires CareConnect access (as detailed in the enrolment package and the Appendix).
☐	8. My worksite will retain a record, for two years, of the support activities (i.e. invoice/receipt with name of vendor and date of service) of all technical support provided by external vendors that have been conducted on computers that access CareConnect or my worksite's network, either directly or remotely.
☐	9. I declare that my IT Support team and/or myself have completed the '*Non-Health Authority Worksite IT Security Checklist'* and ensured all technical requirements for accessing CareConnect have been addressed.

Physical Access Control for Worksite Access*

☐ (If applicable) Worksite is equipped with a monitored alarm system

☐ Server/Network equipment is physically secured from public access

* A worksite is any location from which you are accessing CareConnect be it a pharmacy practice, clinic or home office. This must be in place for all locations where rapid access from an EMR is granted.

Working Remotely: Refer to DTO's document

☐ Ensure you follow remote access guidelines which include:
- Secure your working environment
- Lock your device
- Be vigilant against phishing emails
- Be cautious when connecting to Wi-Fi

User Account

☐ Each user has a unique account and password to access your network

☐ User accounts are not shared among multiple users

☐ A separate user account is used for system administration

Password Management

☐ Minimum password length is 8 characters

☐ Passwords contain characters from three of the following categories (Uppercase characters, Lowercase characters, Numerals, Non-alphanumeric keyboard symbols)

☐ Passwords are changed at a minimum semi-annually

Wi-Fi Network

☐ SSID, WPA2/WPA3 and Wi-Fi password settings are as required

☐ Guest Wi-Fi access is completely isolated from the worksite LAN/Wi-Fi network

Anti-Virus Software

☐ Anti-virus software installed and enabled for auto update *(screenshot of configuration must be attached)*

Operating System

☐ There are no legacy/end-of-support operating systems in use (Windows XP, Windows 7, MacOS older than the latest 3 versions)

☐ The Operating System is enabled for auto updates or manually patched at a minimum semi-annually

Application Patching

Where it doesn't conflict with my pharmacy operating system or electronic medical record system requirements,

☐ Desktop software, e.g. MS Office/other applications are configured for automatic patching or patched at a minimum quarterly

☐ Browser plugin (PDF, Java, etc.) are patched at a minimum semi-annually; uninstall Adobe Flash from the computer

☐ Such patching conflicts with my EMR system requirements