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

PRIVACY AND SECURITY DECLARATION

Community Based Providers Access to the Provincial eHealth Viewer ("CareConnect")

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"), the Privacy and Security Toolkit created by the Doctors of BC, the College of Physicians and Surgeons, 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 clinic/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 clinic/worksite's computer system. N/A for virtual physicians.
☐	3. Security awareness training is provided to clinic/worksite staff and yearly reviewed. (Supplemental training can be found here)
☐	4. My staff is/I am aware of malicious emails and have been informed not to click links or open attachments that appear suspicious.
☐	5. My staff is/I am aware of risks associated with using USB drives and other portable devices that may compromise my network.
☐	6. My staff is/I am 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 clinic/worksite agrees to notify the CareConnect Team when I/one of my staff no longer requires CareConnect access (as detailed in the enrolment package and the Appendix).
☐	8. My clinic/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 clinic/worksites' network, either directly or remotely. N/A for virtual physicians.

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. A worksite includes using remote access.

General Work Guidelines:

☐ Ensure staff follow general access guidelines which include:
- Securing their working environments
- Locking their devices
- Being vigilant against phishing emails
- Being cautious when connecting to Wi-Fi

User Account

☐ Passwords are not saved on workstations or prompted for autofill to prevent unauthorized access

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

*Refer to 'Physician Office IT Security Guide' pages 24-26

Wi-Fi Network

☐ SSID, WPA2/WPA3 and Wi-Fi password settings are as per DTO Technical Bulletin*
☐ Guest Wi-Fi access is completely isolated from the worksite LAN/Wi-Fi network

*Refer to Doctors Technology Office (DTO) Technical Bulletin: 'Wireless – Reduce Risks and Improve Performance'

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 EMR's 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

OR

☐ Such patching conflicts with my EMR system requirements (Select this if your EMR prevents such patching)