Ministry of Health

British Columbia
Professional and Software Conformance Standards

Electronic Health Information Exchange

Policy for Secure Remote Access to PharmaNet

Version 1.1 2020-09-21

Security Classification: Low Sensitivity

Document Details

Author: Ministry of Health

Last Updated: 2020-09-21

Version: 1.1

Document Version History

Release	Date	Details
v1.0	April 2020	Initial public release.
V1.1	September 2020	Policy name change.

Policy for Secure Remote Access to PharmaNet

Remote access to PharmaNet must be done via a laptop or desktop computer only.

Mobile devices such as tablets and smartphones are not permitted.

The PharmaNet software vendor must ensure that all the requirements below are met when:

- offering remote access to their PharmaNet application; and
- supporting their client organization and end-users to meet the requirements.

Vendor Requirements

The vendor must:

1. Provide a secure remote access technology (VPN), such as Cisco AnyConnect, or equivalent protection for the remote access session, and it must meet/support the following requirements (see Note 1 at the end of this section):
    - If not using VPN, the proposed protective technology must be approved in writing by the Ministry of Health **before it is deployed for remote access**.
    - In order to have their technology evaluated, PharmaNet software vendors must contact the Ministry's Conformance and Integration Services at:
        - HLTH.CISSupport@gov.bc.ca
2. Advise the organization's end-users on how to configure laptops or desktop computers to use VPN or other approved secure remote access technologies.

3. Ensure that:

    a. End-to-end encryption (minimum AES-256 bit) is used for transmission of information;

    b. VPN sessions will be disconnected after no more than one hour of inactivity;

    c. Internet addresses are geofenced to ensure all remote access occurs from within BC only;

    d. Remote access session audit and monitoring controls are enabled;

    e. Unique, identifiable user IDs are used to establish the remote access connection;

    f. Remote access user IDs, accounts and/or credentials are not shared;

    g. Good practices regarding password renewal are used;

    h. The remote access technology software is currently supported, up-to-date and has the latest patched applied;

    i. Only users authorized by the Ministry of Health are permitted to use remote access to PharmaNet; and

    j. Multi-factor authentication must be used (see Volume 2 – Privacy and Security).

Note 1: If you are following the Physician Private Network (PPN) requirements for remote access to your electronic medical record (EMR), this policy extends those requirements to remote access to PharmaNet, in addition to requirements here that are not included in the PPN requirements.

Organizational (Site) Requirements

Organizations are responsible for ensuring that:

1. Users must subscribe to an Internet Service Provider (ISP) who uses industry-standard privacy and security best practices for providing reliable Internet services.

2. Users have installed and are using the secure remote access technology (VPN), supplied by the vendor, such as Cisco AnyConnect, or equivalent protection as authorized by the Province.

3. User's devices that will be used for remote connection will have the following:

    a. Up-to-date malware protection is enabled and actively scanning for threats;

    b. Anti-virus software that is current, active in real time, and patched/updated as soon as updates are available;

    c. An operating system (e.g., Windows 10) that is currently supported by the vendor (e.g., Microsoft) with security patches and updates;

    d. A local firewall installed, active and kept up-to-date – must have intrusion detection;

    e. Encrypted data storage – minimum AES 256 (e.g., Bitlocker or equivalent);

    f. Any removable media (e.g., DVDs, USB flash drive) used with the device (e.g., laptop) must be encrypted to AES 256;

    g. Screen saver time-out after a set, reasonably short, period of inactivity (no more than 15 minutes); and

    h. The remote access solution has the latest system patches installed as soon as they are available.

User Requirements

Remote access requirements for the organization's end-user (e.g., physician, pharmacist, nurse practitioner).

If you are accessing PharmaNet remotely, you must:

1. Subscribe to ISPs who use industry-standard privacy and security best practices for providing reliable Internet services.

2. Ensure that the device (e.g., laptop) that is used for remote access has:

    a. Anti-virus software that is current and active.

        i. Typically, anti-virus software provides a visual status indicator via an icon in the taskbar usually found at the bottom of the screen.

    b. The anti-virus software configured to check and download definition updates daily.

        i. Periodically check the date when the definition files were last updated, to ensure that updates are being automatically installed.

    c. A virus scan job that is configured to scan the entire computer for viruses on a weekly basis.

    d. A firewall that is enabled, active and set to the highest settings possible.

        i. For example, on a Microsoft Windows 10 computer:

            1. Go to "Start" (Windows logo),

            2. Select "Settings" (the cog wheel icon),

            3. Select "Update & Security",

            4. Select "Windows Security",

            5. Select "Firewall & network protection", and

            6. Ensure that the "ON" option(s) are selected.

3. Ensure that you use a secured home network:

    a. Contact your ISP to ensure that the following are in place:

        i. The firewall/wireless router is not using the default password (as default passwords are often published on the Internet, which would allow anyone to reconfigure the device without your knowledge).

        ii. The strongest encryption (e.g., "WPA2-Personal" encryption) is being used ("WPA-Personal" encryption is acceptable).

        Note 2: If the encryption is "WEP" or "No encryption," you need to change it to WPA2-Personal. Contact your ISP's technical support for assistance.

4. Ensure that your VPN session is automatically set to disconnect after one hour of inactivity.

    a. If there is no automatic time-out function, then you must manually disconnect the VPN session after one hour of inactivity.

5. Ensure that the computer that you are using has:

    a. Up-to-date malware protection that is enabled and actively scanning for threats.

    b. Anti-virus software that is current, active in real-time, and patched/updated as soon as updates are available.

    c. An operating system (e.g., Windows 10) that is currently supported by the vendor (e.g., Microsoft) with security patches and updates that are installed as soon as they are available.

6. Ensure that when you are accessing PharmaNet remotely:

    a. PharmaNet information is not stored locally on the end-user's device or on removable media or printed at the remote location.

    b. That after a short period of inactivity (no more than 15 minutes), your computer will automatically lock and display a "screen saver" to protect the information from accidental access or viewing by unauthorized individuals.

        i. For example, on a Microsoft Windows 10 computer:

            1. Go to "Start" (Windows logo),

            2. Select "Settings" (the cog wheel icon),

            3. Select "Personalization", and

            4. Select "Lock screen" to check the screen saver time-out settings.

    c. You shut down the VPN when you are not using it.

    d. Your VPN session for PharmaNet is ended before other use is made of the VPN.

    e. PharmaNet information is NOT visible to other users on a shared desktop or application (e.g., Skype for Business allows a desktop to be shared with others).

    f. You do not allow remote control of the desktop while connected to VPN (as this may expose unauthorized users to the displayed information).

        i. If you require remote desktop control for an issue not involving your PharmaNet application, ensure that the PharmaNet session is closed before allowing remote desktop control.

        ii. Technical support for your PharmaNet application must follow the requirements of Section 6 of the Information Management Regulation (Access to PharmaNet for technical purposes), including requirements for your supervision of the access.

7. If the computer will be used by family members or others that do not have access to PharmaNet, you need to ensure that these individuals will have separate user accounts, storage and access.

8. You ensure that the VPN is only used by an authorized PharmaNet user.

9. You only access PharmaNet when physically located within BC.