

PPN TECHNICAL SUPPORT GUIDE FOR CLINICS

Summary

This guide provides technical information and suggestions regarding the use of the **Private Physician Network (PPN)** by private practice clinics in BC.

Contents

SUMMARY	1
CONTENTS	1
PPN FREQUENTLY ASKED QUESTIONS (FAQS)	2
WHAT IS THE PPN?	2
WHAT ARE THE BENEFITS OF THE PPN?	2
WHAT ELECTRONIC MEDICAL RECORD (EMR) SOFTWARE CAN BE USED ON THE PPN?	2
WHO DO I CONTACT TO LEARN MORE OR SIGN UP FOR THE PPN?.....	2
DTO SUPPORT FOR THE PPN	3
PPN SUPPORT MODEL.....	3
ESCALATING PPN ISSUES	3
PPN SERVICE SPEEDS	4
PPN ASYMMETRICAL SERVICE	4
PPN SYMMETRICAL SERVICE	4
PPN CLINIC SETUP AND CONFIGURATION	4
PPN TRANSITION CONSIDERATIONS	4
PPN INSTALLATION.....	5
<i>Pre-Field Visit</i>	5
<i>Pre-Go-Live Testing</i>	5
PPN HARDWARE AND NETWORK RECOMMENDATIONS	5
<i>Devices</i>	5
<i>LAN (Local Area Network)</i>	6
<i>Telus Router</i>	6
PPN SOFTWARE RECOMMENDATIONS.....	6
<i>Optimize web browser</i>	6
<i>Security configuration</i>	6
<i>SMTP (Simple Mail Transfer Protocol)</i>	6
<i>Anti-virus and OS updates</i>	6
PPN TROUBLESHOOTING	6
REMOTE ACCESS.....	7
RESOURCES	7

PPN Frequently Asked Questions (FAQs)

What is the PPN?

- The PPN is the private, high-speed network available to physicians and practice staff to access clinical information in their qualified electronic medical record (EMR) systems.
- **Provincial Health Services Authority (PHSA)** offers this PPN service as part of a province-wide initiative.
- As of 2019, the PPN supports approximately 900+ clinics supporting 4500+ clinicians.

What are the benefits of the PPN?

- Professionally and centrally managed firewall, anti-virus, intrusion prevention and intrusion detection systems.
- High service levels for network availability and problem resolution.
- Access to some provincial eHealth system integrations.
- No PPN monthly costs because the network is funded by the Ministry of Health Services.

What Electronic Medical Record (EMR) software can be used on the PPN?

- Any ASP-model (cloud-based) EMR may be used on the PPN.

Who do I contact to learn more or sign up for the PPN?

- Send an email to the PHSA Private Physician Network Administrator, at ppnadmin@phsa.ca

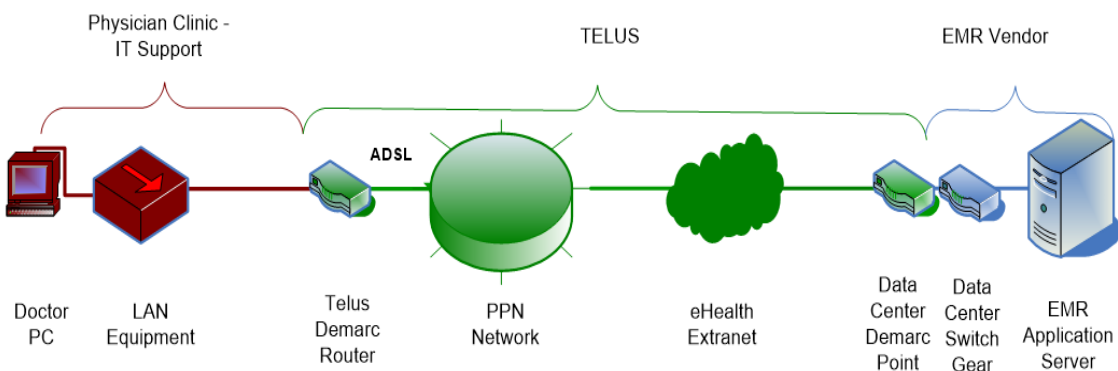
DTO Support for the PPN

Doctors Technology Office (DTO) provides leadership, guidance, expertise, and alignment of emerging and current health technology and information needs for private practice physicians across BC. In terms of support the PPN, this means that DTO gets involved when the clinic has gone through the support model but is not able to be resolved or the issue isn't being resolved in a timely manner.

Common DTO PPN Support Examples:

- Poor performance
- Application not working
- E-Mail not working
- Advice on applications

PPN Support Model



Escalating PPN Issues

The common escalation path for PPN-related issues is **Clinic (or Clinic IT) > EMR Vendor > TELUS > PHSA**

Doctors Technology Office (DTO) becomes involved if issues cannot be resolved through the expected PPN escalation path.

Common issues for DTO escalation (stakeholders):

- Improper installations (*TELUS/PHSA/DTO*)
- Improper IP addressing (*EMR/DTO*)
- Poor local area network (LAN) design or related issues that cannot be resolved (*Clinic IT/DTO*)
- Poor wide area network (WAN) performance (*EMR/Clinic IT/DTO*)
- Security concerns (*Clinic IT/DTO*)

PPN Service Speeds

The PPN provides different service speeds depending on many factors which are determined by PHSA after a PPN application is received. The PPN services available as of summer 2019 are:

PPN Asymmetrical Service

- **PPN1 (25x5)** delivers an asymmetrical download speed of **25 Mbps** and an upload of **5 Mbps**

PPN Symmetrical Service

- **PPN3** delivers symmetrical upload and download speeds of **10 Mbps**
- **PPN3-30** delivers symmetrical up and download speeds of **30 Mbps**
- **PPN3-100** delivers symmetrical up and download speeds of **100 Mbps**
- **PPN-NaaS** delivers symmetrical up and download speeds of **150 Mbps (pilot phase)**

PPN Clinic Setup and Configuration

To meet the privacy and security requirements of the PPN and ensure optimal performance when using the PPN with your EMR applications, a number of considerations and guidelines should be followed. For specific details of your current PPN or other eHealth viewer access requirements, refer to your PPN Agreement documentation, provided by PHSA or Health Authority.

PPN Transition Considerations

When moving on to the PPN network for the first time, a clinic and their IT support provider should be aware of the following considerations:

- Public IP address of the clinic will change (no longer under local clinic control)
- Lease time for public IP addresses - 1 hour for first DHCP connection, days after that
- The available network addresses are split between 70% dynamic and 30% static IPs
- The top 3 IP addresses of the subnet are reserved (gateway, switch and diagnostic device)
- Any email service at the clinic must use TELUS for outgoing SMTP (smtp.telus.net)
- References to old local IP addresses may no longer function
- The local LAN must not be connected to any other commercial internet provider service (ISP)
- Firewall rules will be in place to and from the internet (some applications may not work initially)
- Internet and/or network speeds may be different than previously used

PPN Installation

Pre-Field Visit

TELUS will perform a pre-field visit prior to the PPN install date. This visit will consist of an on-site inspection to verify installation conditions for customer premise equipment (CPE) and fiber requirements. Access will be required to all rooms where there is hardware including the demarcation point (area where the TELUS service enters the building). When necessary, the clinic's PPN contact will need to make arrangements with landlords for access to these areas.

Following this visit, a report indicating the area(s) where further work may need to be completed in preparation for the installation of the PPN circuit will be provided to the clinic's PPN contact and copies to the MOH. Approximate duration of this appointment is 3 hrs. The clinic should involve local IT to determine install location. The clinic may be required to provide a proper mounting structure.

Pre-Go-Live Testing

With the help of the EMR vendor, organize a pre-go-live turn-up test.

During the test, the local IT would need to:

- Check WAN-LAN interface errors (packet loss, CRC, etc.)
- Site to site connectivity (if there is one)
- Application connectivity (all applications)
- Verify WAN metrics (latency, throughput, packet loss, etc.)

The EMR vendor would need to:

- Make security changes to allow your new PPN line to access the EMR servers.
- Be notified of your turn-up test and go-live dates to coordinate those security changes.

PPN Hardware and Network Recommendations

Clinic and network hardware used with the PPN should meet or exceed the recommended requirements of all the applications being used by the individual. Consumer-grade wireless solutions should be avoided.

Devices

- Dynamic IP addresses can be used for workstations, static IPs should be used for printers, scanners, and servers, etc.
- Set defaults for scanning sizes to be appropriately-sized for electronic medical records (small in size as possible while still being legible for printing and digital viewing).

LAN (Local Area Network)

- LAN Switch - Use a business class, programmable layer-2 switch for local LAN connections.
- Reduce unnecessary LAN traffic such as media streaming or other non-business network use.

Telus Router

- The DNS and DHCP are provided by the PPN. If local name resolution is required and/or clinic would like to use their own DHCP server PHSA must be notified, clinic must use IP scope assigned and clinic must forward local DNS server to the PPN DNS.
- Do not use NAT (Network Address Translation).

PPN Software Recommendations

Optimize web browser

- Remove browser toolbars or other unnecessary add-ons.
- Disable auto-detect network proxy, use "no proxy" setting.

Security configuration

- Use a unique administrator account.
- Use unique, appropriately restricted accounts for each user of the system.
- Use strong, unique passwords for all accounts.
- All software should be kept up to date to protect from vulnerabilities.

SMTP (Simple Mail Transfer Protocol)

- Use Telus SMTP for the outgoing email server: smpt.telus.net or mail.telus.net

Anti-virus and OS updates

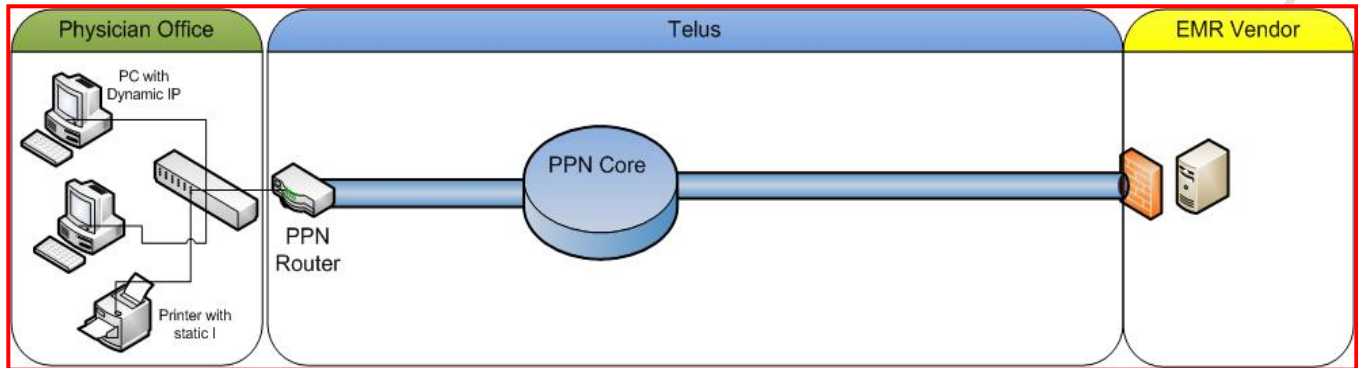
- Implement regular schedules of anti-virus, operating system updates, and system maintenance and set them to run outside of business hours.

PPN Troubleshooting

Consider the escalation paths detailed earlier in this guide while troubleshooting issues that may be PPN-related:

Clinic (or Clinic IT) > EMR Vendor > TELUS > PHSA

This graphic shows main areas of the clinic-PPN architecture grouped by the responsible party for that area:



- DTO is in a unique position to be able to assist and support across all three areas and work with the primary stakeholders; physician office, Telus, PHSA, and the EMR vendor.

Remote Access

Remote access to EMRs that do not have built-in web-based access can be facilitated through secure tokens provided by PHSA. This remote access is only for EMR access and does not provide access to clinic computers.

Resources

Physician Office IT Security Guide	<p>A DTO guide detailing best practices to enhance privacy and security at the clinic level based on requirements and information from the Personal Information Protection Act (PIPA), College of Physicians and Surgeons of BC, the Office of the Information and Privacy Commissioner for British Columbia (OIPC) for protecting information.</p>
Clinic IT Support Community	

For more information, guidance, or support please contact:

Doctors Technology Office

☎ 604 638-5841

✉ DTOinfo@doctorsofbc.ca

🌐 www.doctorsofbc.ca/doctors-technology-office