

## The Private Physician Network (PPN) Primer

Date Created: August 1, 2008

Last Updated: September 9, 2010

Final Version: V1.2





## **Disclaimer**

The Province of British Columbia cannot guarantee the accuracy of this document's contents. By proceeding with the information in this document, each reader waives and releases the Province of British Columbia, its employees, representatives and contractors, to the full extent permitted by law from any and all claims related to the usage of material or information made available. In no event shall the Province of British Columbia, its employees, representatives or contractors, be liable for any incidental or consequential damages resulting from the use of this material.

Copyright © Province of British Columbia

All rights reserved



## Table of Contents

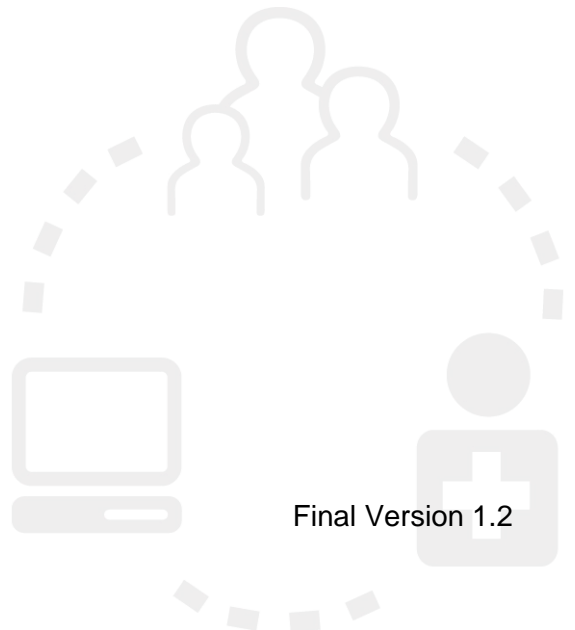
<a href="#">1.0</a>	<a href="#">BC's eHealth Information Highway</a>	<a href="#">7</a>
1.1	The Private Physician Network	7
1.2	The eHealth Network Gateway	7
1.3	The TELUS Extranet	8
1.4	The Big Picture	8
<a href="#">2.0</a>	<a href="#">PPN Overview</a>	<a href="#">9</a>
2.1	Immediate Benefits	9
2.2	PPN Service Features	9
2.2.1	PPN Core Network Features	9
2.2.2	Practice Connections	10
2.2.3	EMR Vendor Connections	11
2.2.4	Connecting Outside the Practice	12
2.2.5	Internet Access	13
2.3	Cost for the Service	13
2.4	Support	13
2.4.1	PPN Support	13
2.4.2	Practice LAN Support	14
2.5	Service Levels	14
2.5.1	PPN Service Levels	14
2.5.2	PPN Maintenance	15
<a href="#">3.0</a>	<a href="#">Implementing the PPN</a>	<a href="#">16</a>
3.1	Implementation and Transition Support Program (ITSP)	16
3.2	Preparing for the Service	16
3.2.1	Practice Profile	16
3.2.2	Building Wiring and Practice LAN	17
3.2.3	Selecting a Live Date	17
3.3	Installing the Service	18
3.3.1	TELUS Router Equipment	18
3.3.2	Migration to the PPN	18
<a href="#">4.0</a>	<a href="#">Using the PPN</a>	<a href="#">19</a>
4.1	Connecting At the Practice	19
4.2	Connecting from Home	19
4.3	Connecting to Email	19
<a href="#">5.0</a>	<a href="#">Key Responsibility Summary</a>	<a href="#">20</a>
5.1	TELUS Responsibilities	20
5.2	EMR Vendor Responsibilities	20
5.3	Practice Responsibilities	20
	<a href="#">Appendix A - Definitions</a>	<a href="#">22</a>

## Figures

Figure 1 Key Network Connections	8
----------------------------------	---

## Tables

Table 1 TELUS Router Sizing Options	11
Table 2 PPN Network Service Level Targets	15





## Purpose of This Document

This document provides a detailed description of the Private Physician Network (PPN) service offered by the Ministry of Health Services, as part of the Physician Information Technology (PITO) program.

This document can be used by PITO relationship managers, physicians and practice staff as well as EMR vendors and other involved parties to inform their efforts to install, set up and use the PPN.

**Note:** The information in this document does not apply to Practices connecting to the PPN through a gateway at their local Health Authority (including Northern Health Physician Connect Network and Vancouver Coastal Health's Diamond Centre). These Practices should, instead, refer to the ***“PPN Health Authority Gateway Primer”***,

## Related Documents

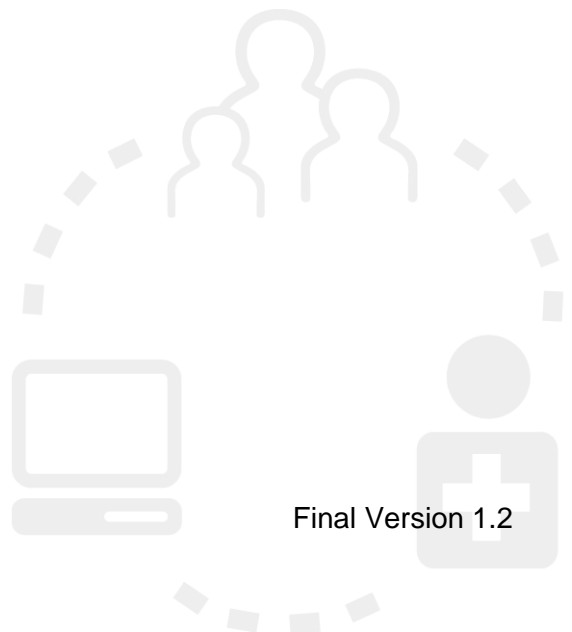
The following PPN documents are available on the PITO website at [www.pito.bc.ca](http://www.pito.bc.ca) under the 'Document Links' section:

- Welcome to the PPN: A summary for physicians and staff of key PPN features;
- EMR and PPN Implementation Checklist: Identifies the key activities involved in implementing a PITO-qualified EMR application and the PPN at a practice. It identifies which party is responsible for performing and managing each activity as well as the expected timeline to complete;
- EMR and PPN Support Quick Reference: A summary for physicians and staff about the support available to them through their EMR vendor and TELUS;
- EMR and PPN Support Responsibility Matrix: A detailed description of the roles and responsibilities of all parties involved in supporting EMR and PPN implementations through PITO;
- PPN Firewall Change Request Form: A form for practices to submit requests for additional Internet based applications to be allowed through the PPN core firewall.
- PPN Technical Reference: Provides key technical information and considerations for preparing, configuring and connecting the practice network to the PPN. This document is primarily intended to be used by the person(s) providing technical support services for the practice's local computer environment. The person(s) in the practice who is leading the migration to the PPN should also be aware of the key technical activities required to prepare for its installation; and

- Remote Access to the PPN: A user guide for setting up and using the VPN service for staff who connect to the PPN from outside of the practice (e.g. home).

Practices that connect to the PPN through a gateway at their local Health Authority, including Northern Health's Physician Connect Network or Vancouver Coastal Health's Diamond Centre should review the documents specific to the gateway approach for accessing the PPN:

- PPN Health Authority Gateway Primer: A complete description of the PPN service and key practice responsibilities for practices connecting to the PPN through a gateway from Northern Health's Physician Connect Network or Vancouver Coastal Health's Diamond Centre; and
- PPN Health Authority Gateway Support Quick Reference: A summary for physicians and staff outlining the support available to their practice through their Health Authority, EMR vendor and TELUS for their connection to the PPN through their Health Authority gateway.

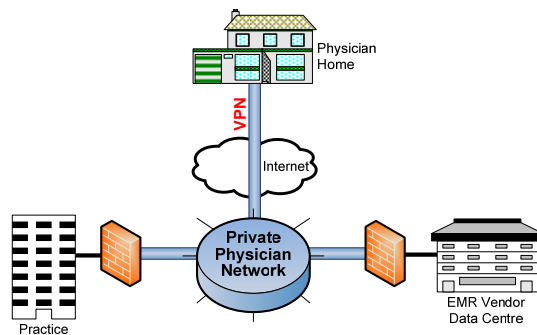
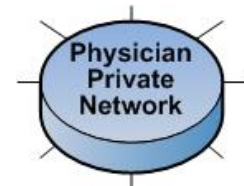




## 1.0 BC's eHealth Information Highway

### 1.1 The Private Physician Network

The PPN is the private, high-speed network that will be installed in physician practices when they register and are accepted into the PITO program. It is a key component of the suite of products and services being offered to British Columbian physicians through PITO. For many practices, the PPN will replace the Internet connection they already pay



for from existing network providers. The Ministry of Health Services has contracted with TELUS to build and operate this network.

The PPN enables physicians and practice staff to access the clinical information in their PITO-qualified Electronic Medical Record (EMR) systems. It also enables them to securely access their EMR through a Virtual Private Network (VPN) Web Portal from outside their practice using a computer

with Internet access. The PPN ensures that physicians and practice staff have a private and reliable way to access the patient information in their EMR from their office or home, and also provides them with a reliable, high speed line to the public Internet.

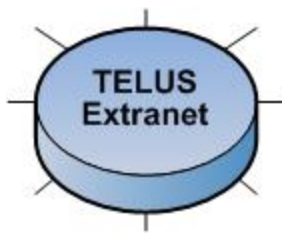
Physicians in the Northern Health region that currently connect to the wireless Physician Connect Network or are located in Vancouver Coastal Health's Diamond Centre, will continue to use their existing Health Authority (HA) network services. A network gateway has been put in place to allow these physicians to access their PITO-Qualified EMR through the PPN from their existing HA network.

### 1.2 The eHealth Network Gateway

The eHealth Network Gateway (eNG) is a new network replacing the Provincial Network Gateway or "PNG", which links the six health authorities. The eNG shares a secure connection to the PPN. This link will enable physicians to access their EMR when working in health authority facilities.



### 1.3 The TELUS Extranet



The TELUS Extranet provides secure, private interconnection between separate health sector related networks. TELUS is contracted to provide this service. Currently, the TELUS Extranet interconnects the PPN to the six EMR vendor data centres. As other health sector related systems are implemented in the future, they will be interconnected to the PPN via the TELUS Extranet. This will support physician access to a broader range of clinical information and services (e.g. prescriptions, lab test results, diagnostic images) through their PITO-Qualified EMRs.

### 1.4 The Big Picture

The diagram below shows the key network connections that physicians and practice staff will utilize when connecting to the PPN from their practice or remote locations. Some of these connections are available now and some will be enabled over the next few years as BC's province-wide Electronic Health Record (EHR) becomes a reality.

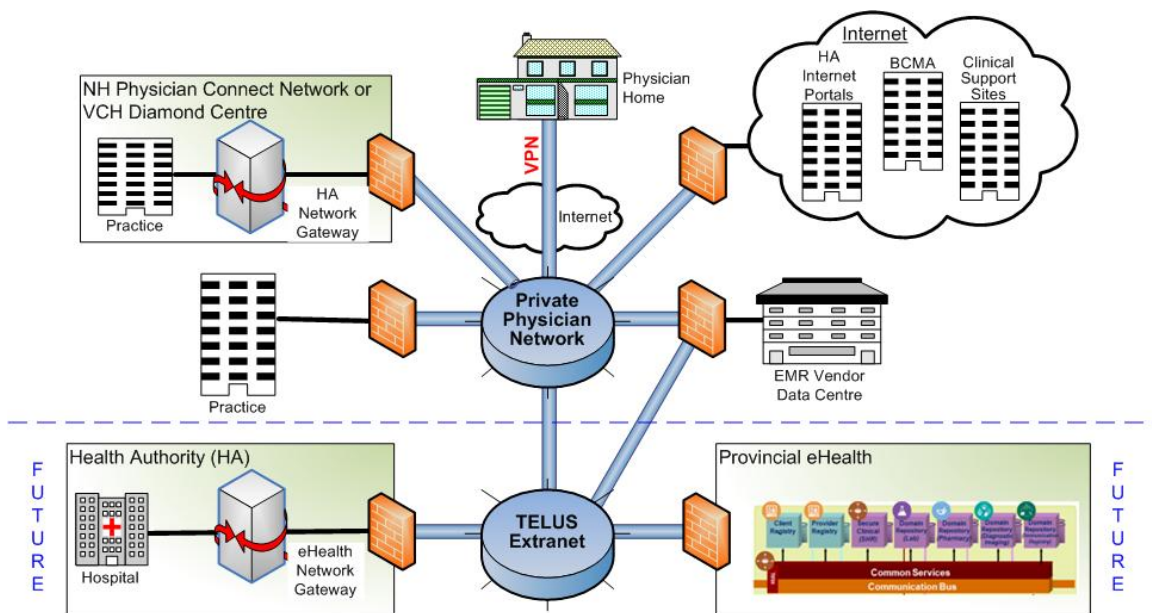


Figure 1 Key Network Connections



Access to Health Authority portals from a practice will continue to be via the Internet. Opportunities to access Health Authority portals privately from the PPN through to the eNG will be explored with each Health Authority, and will be subject to their policies and financial resources.



## 2.0 PPN Overview

### 2.1 Immediate Benefits

The PPN is the physicians' private lane on BC's eHealth information highway. For many practices, the PPN will replace the Internet connection they have with existing network vendors. Physicians and their staff will use the PPN to:

- Connect the computers in their practice to their selected EMR application;
- Access clinical reference tools available on the public Internet and clinical applications from health authorities;
- Access their EMRs for periodic use from a home computer with Internet access, or other locations outside their practice, over a strongly encrypted VPN; and
- Eventually access information in other provincial health sector systems such as PharmaNet.

The PPN is a TELUS managed network tailored to physician needs, and it has many advantages over existing consumer-grade networks such as:

- Professionally and centrally managed firewall, anti-virus, intrusion prevention and intrusion detection systems;
- High service levels for network availability and problem resolution;
- Help desk support integrated with the PITO-Qualified EMR vendor help desks; and
- No PPN monthly costs because the network is funded by the Ministry of Health Services through PITO.

### 2.2 PPN Service Features

The PPN is built and maintained by TELUS through a Master Services Agreement signed with the Province of British Columbia. The Agreement provides for the following infrastructure and services to physician's practices.

#### 2.2.1 PPN Core Network Features

The PPN Core is a private network that all physician practices and remote users connect into. Its key features are:

- **Security:** Provides industry best practice and robust firewall, anti-virus, and intrusion protection network services that protects it, and the practice networks connecting to it, from external threats coming from the public Internet. As well, it protects from internal threats coming from practice Local Area Networks (LANs).
- **Private:** Network traffic between the practices and their EMR vendor data centers is private because it does not travel over the public Internet. As well, each practice's network traffic is not visible to other practices. Any network traffic

- destined for the public Internet will be directed through the PPN Core security devices before being routed back to the originating practice;
- **High Availability:** Network traffic passing through the PPN Core can be directed through two separate, redundant geographic paths - one in the interior and the other in the lower mainland. A network outage in one geographic area will result in traffic being routed through the other providing high availability for the PPN Core network;
  - **High Speed:** Utilizes standard high speed network technologies; and
  - **Extensible:** Initially, provides practices with network access to the EMR vendor that they have selected and the public Internet. Eventually, the PPN will provide access to other BC health sector systems (provincial, health authorities, and other health organizations' systems).

## 2.2.2 Practice Connections

### 2.2.2.1 'Last Mile' Connection

A private and highly reliable dedicated connection (termed 'last mile') will be installed between the nearest TELUS Central Office and the practice location. TELUS will provide and install PPN router equipment (a router and a modem) at the chosen location in the practice. Typically, this will be in the practice's telephone room within proximity of their LAN switch, or in the case of buildings with more than one practice, the building's telephone room.

The exception to the above is for practices that will continue to use their existing HA network (see next section) to connect to their PITO-qualified EMR through a PPN gateway installed at their HA.

The TELUS router is equipped with LAN interface ports (with Ethernet input) that each practice LAN will plug into. A dial up modem is installed in tandem with each router to provide TELUS with another channel for managing their PPN router at each practice location. The modem plugs into a standard phone line, and is for monitoring and troubleshooting the router if the network is unavailable.

The TELUS router equipment is the '*demarcation point*' – the boundary between the TELUS-provided services and the practice network. TELUS is responsible for trouble-shooting and support from the router back into the PPN Core network, while the practice is responsible for trouble-shooting and support for their LAN including the cable connecting into the TELUS router.

The capacity or bandwidth of the connection for each practice is based on the size of the practice. The PITO relationship manager (RM), working with practice staff, will determine the *number of concurrent users* who will on average be using the network connection at any one time. Standard sizing rules have been designed to select the appropriate TELUS router capacity, which are listed in the table below. Note that this '*concurrent*' number does not include staff working remotely outside of the practice location.

Table 1 TELUS Router Sizing Options

TELUS Router Type	Approximate Bandwidth	# of Physicians	# of Concurrent Users
PPN-1 – Asymmetric <sup>1</sup> (one ADSL router)	1 - 5 Mbps <sup>2</sup>	1 – 4	1 – 8
PPN-2 – 2 X Asymmetric <sup>1</sup> (two ADSL routers)	1 - 5 Mbps (for each router)	5 – 8	9 – 16
PPN-3 – 10Mbps	10 Mbps	9 - 100	17 – 199
PPN-4 – 100Mbps	100 Mbps	101 +	200+

### 2.2.2.2 Health Authority Gateways

For practices in the north already connected to the Northern Health’s wireless Physician Connect Network or those practices that are located in Vancouver Coastal Health’s Diamond Centre, there will not be a requirement to install a ‘last mile’ PPN network router at the practice. A network gateway has been put in place which routes PITO physician network traffic to the PITO-Qualified EMRs through the PPN. Access to the Internet and HA systems/services will continue to be provided through the existing HA network and will not change.



Practices that use Northern Health’s wireless Physician Connect Network or are located in Vancouver Coastal Health’s Diamond Centre practices should review the “PPN Health Authority Gateway Primer” for their overview on accessing the PPN.

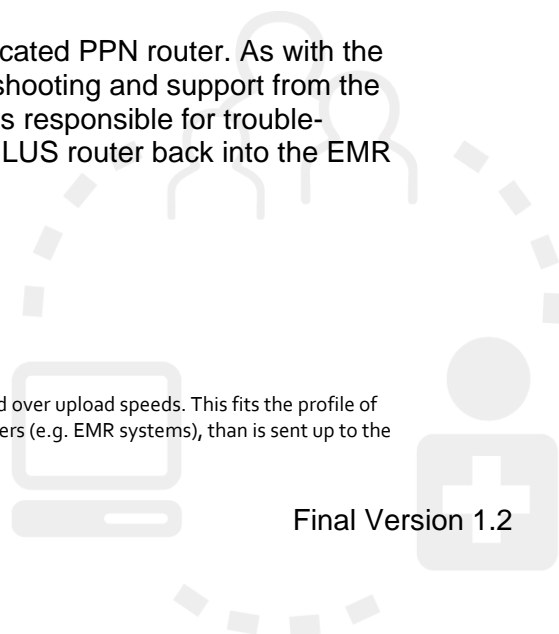
These practices should dialogue directly with their HA for any information they require regarding their existing HA network including support, service levels, and remote access.

### 2.2.3 EMR Vendor Connections

At the EMR vendor data centre, TELUS will install a dedicated PPN router. As with the practice-based router, TELUS is responsible for trouble-shooting and support from the data centre router back into the PPN. The EMR vendor is responsible for trouble-shooting and support from the cable plugging into the TELUS router back into the EMR data centre.

<sup>1</sup> These access options are asymmetric access based, which provides faster download over upload speeds. This fits the profile of typical network use, where significantly more data is pulled down from internet servers (e.g. EMR systems), than is sent up to the servers.

<sup>2</sup> Millions of Bits Per Second.



## 2.2.4 Connecting Outside the Practice

The PPN can be accessed from a computer outside of the practice, with an Internet connection, using an Internet browser, such as Internet Explorer or Mozilla Firefox. The Ministry of Health Services has contracted with TELUS to maintain two VPN portal sites, one in Kelowna (<https://vpn2ppn.bc.ca>) and the other in Vancouver (<https://vpn1ppn.bc.ca>). Two factor authentication is required to log in to these “VPN Web Portal” sites.

Since the PPN is accessed over the Internet from a remote computer, it is very important to understand how the information is traveling through the VPN. When signed into the VPN Web Portal all of the data sent from the remote computer over the Internet to the PPN is in an encrypted format. Once the data reaches the PPN, its security components provide further protection through its firewall, anti-virus, and intrusion protection systems.

The cost of the Internet connection used for remote access outside of the practice is not funded by PITO or the Ministry of Health Services.



An EMR vendor may choose to provide its own VPN service to practices wishing to remotely access the EMR application. The practice will need to dialogue with their vendor to choose the VPN service which best meets their practice needs.

### 2.2.4.1 Virtual Private Network (VPN) Concepts

VPNs maintain data privacy by encrypting data before transmitting it over a network. The data is encrypted by software at the sending end and then at the receiving end. This technology provides a secure “tunnel” for transmitting information that is not accessible to unauthorized users. VPN encryption would be in addition to the encryption already in place with EMR and health authority applications (among others).

Once a user has signed into the VPN Web Portal and launched their EMR or other Internet based application(s), all traffic over the Internet is contained within the secure “VPN” Tunnel” and is encrypted for added security.

### 2.2.4.2 Two Factor Authentication

Two factor authentication is a security process in which a user provides two means of identification (or “factors”) to logon to a computer application. Using two factors provides a more secure method of authentication compared to providing a single password alone. The two factors involved are sometimes spoken of as “*something you have*” and “*something you know*”. The “*something you have*” is typically a physical token, such as a smart card or a one time password generator (e.g. key fob), and the “*something you know*” is something memorized, such as a security code or password.



The PPN uses a one time generated password from the TELUS-supplied RSA SecurID token (as shown on the left) as the “*something you have*” factor. The token displays a ‘*tokencode*’ that changes every sixty seconds. The “*something you know*” factor is a personal identification number (PIN) that TELUS assigns and is provided to the user.



The “Remote Access to the Private Physician Network” document provides instructions for accessing and using the VPN service.

### 2.2.5 Internet Access

The PPN enables physicians and their staff to access the public Internet through the PPN Core network. A gateway to the public Internet is part of the Core. Network traffic passing out to and returning from the Internet is automatically scanned by firewall, anti-virus and intrusion detection software that helps to protect practice systems from Internet threats.

## 2.3 Cost for the Service

Installation of the TELUS router equipment at the practice and its ongoing use are fully funded by the Ministry for the designated router size for the practice (see Table 1 above). This includes the PPN core network and VPN remote access service.

Practices are responsible for funding their computer equipment and LAN, office software and network connections up to the point where they connect into the TELUS router equipment.



Visit the PITO website at [www.pito.bc.ca](http://www.pito.bc.ca) for more details about PITO's reimbursement policies.

## 2.4 Support

### 2.4.1 PPN Support

The first line of support (known as 'Tier 1 support') for practices when they are having trouble accessing their EMR application, PPN network and its related services, is the practice's EMR vendor help desk. This includes problems encountered when using:

- The PPN, including its secure gateway to the public Internet; and
- The VPN for remote access to an EMR including the RSA SecurID Tokens used for authentication.

The EMR Tier 1 helpdesk will triage any technical problems received from a practice and will take the following actions:

- If the problem is with the TELUS router equipment at the practice, the PPN Core network, the secure gateway to the public Internet, or the VPN service, the EMR Tier 1 helpdesk will:
  - Open a 'problem ticket' with TELUS Tier 2 support;
  - Monitor progress on the ticket, and where required, initiate escalation actions;
  - Once the problem is resolved, contact the person who logged the problem to ensure it is resolved to their satisfaction, notify TELUS Tier 2 helpdesk and close the ticket;
- If the problem is with the EMR data centre or application, the EMR Tier 1 helpdesk will open an internal "problem ticket" and resolve it within their support organization; or
- If the problem appears to be originating in the practice's computer environment, the EMR Tier 1 helpdesk will advise the practice to further investigate and resolve the problem with their designated computer support contact.

Practices will have a formal agreement in place with their EMR vendor for Tier 1 support, including hours available and protocols for use.

*Note: All support calls from the practice to the Tier 1 helpdesk will be counted towards the call limit outlined in your agreement with your EMR vendor. Charges to the practice may apply if the limit is exceeded.*

## 2.4.2 Practice LAN Support

Practices are responsible for organizing the technical support they require for their local computers, printers and LAN. This includes:

- Local practice hardware such as computers, laptops, printers, scanners; software such as voice recognition software and computer security software (e.g. firewall, anti-virus); and LAN equipment up to the connection into the TELUS-provided router equipment;
- Clinical reference tools available on the public Internet or clinical applications available from health authorities. The organizations managing such tools and applications will need to be contacted directly for support;
- Laptops or computers outside of the practice (e.g. home) and their Internet connections (e.g. Shaw, TELUS) when used by physicians and staff to remotely connect to the VPN; and
- 3<sup>rd</sup> party email services (e.g. Shaw, Yahoo, Gmail) including configuring laptops or computers to initially access the email service, or other ongoing usage issues.

It is recommended that practices contract with a computer support vendor or their EMR vendor for technical support services for their local computer environment.



Note that additional information about the technical support available with the PPN is provided in the:

- “EMR and PPN Support Quick Reference”: A quick reference summary for physicians and staff about the technical support they can expect to receive when experiencing EMR and PPN related problems, as well as what they are responsible to resolve; and
- “EMR and PPN Support Responsibility Matrix” for a detailed description of the roles and responsibilities for all parties involved in supporting EMR and PPN implementations through PITO.

Both documents are available on the PITO web site at [www.pito.bc.ca](http://www.pito.bc.ca) under the ‘Document Links’ section

## 2.5 Service Levels

### 2.5.1 PPN Service Levels

While TELUS does not guarantee trouble free operation of the PPN service, the Master Services Agreement in place with the Ministry of Health Services sets out service level targets for TELUS’s service which will be measured and monitored.

Targets for PPN network availability are:

*Table 2 PPN Network Service Level Targets*

Network Portion	Description	Availability
PPN Physician Circuit	From physician office to TELUS central office ('last mile')	99.90% or better
PPN Core Network		99.95% or better

The PPN network availability of each practice is measured separately for each month, and reported by TELUS to the Ministry of Health Services for ongoing monitoring.

For PPN network failures either in the PPN core, or at a specific practice location, TELUS's target to restore the service is within 4 hours. For rural or remote locations, travel time is added to this target.

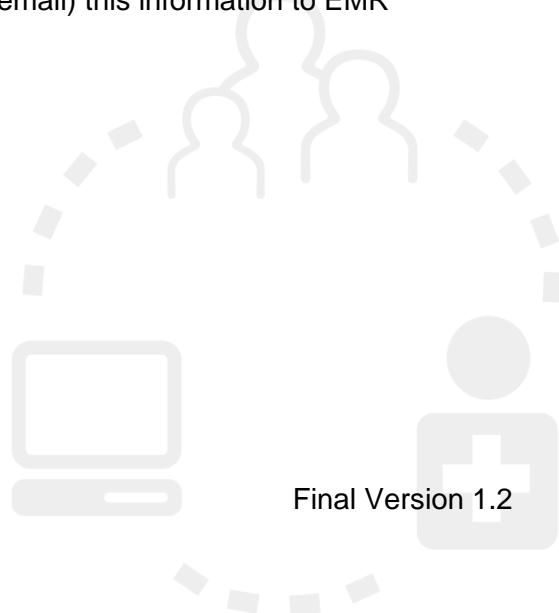
### **2.5.2 PPN Maintenance**

To maintain the PPN network in proper working order, TELUS has standard, designated maintenance windows for performing changes. PPN, email or VPN services may not be available during these windows. The standard maintenance window times are:

- PPN-1 and PPN-2 Services:
  - Daily from 23:00 to 07:00 (AM) PST
- PPN Core, PPN-3 and PPN-4 Services:
  - Sunday: from 00:00 (midnight) to 06:00 (AM) PST
  - Tuesday: from 05:00 to 07:00 (AM) PST

TELUS typically provides 10 day advance notice of changes. The Ministry will forward (by email) notices of TELUS scheduled changes to each EMR vendor, who can then notify each of their associated practices about the planned activity.

If TELUS needs to make changes at other times, that will make PPN services unavailable, they will provide advance notice to the Ministry unless they classify the changes as an emergency. The Ministry will forward (by email) this information to EMR vendors.





## 3.0 Implementing the PPN

### 3.1 Implementation and Transition Support Program (ITSP)

The PITO relationship manager works with each practice to complete the ITSP activities required to implement the practice's EMR, and facilitates the installation of the PPN network and services with the Ministry of Health Services and TELUS. Full details on the program are available on the PITO website at [www.pito.bc.ca](http://www.pito.bc.ca). Practices will sign a Registration Agreement with PITO, which includes agreeing to ongoing conformance with PITO's privacy and security policies and acceptable use policies, documented in the PITO Policies attachment to the agreement.

As part of the PITO registration process practices will apply for PPN network access and associated services.

### 3.2 Preparing for the Service

#### 3.2.1 Practice Profile

Each practice will work with their PITO relationship manager to:

- Determine the PPN router equipment capacity based on the expected number of concurrent users within the practice (see section 2.2.2 above);
- Identify where TELUS will install the router equipment at the practice 'demarc location'. The practice's technical support resource must collaborate in ensuring a high availability service by choosing a suitable and secure location for the TELUS equipment, typically in an existing telephone or wiring closet;
- Determine which practice staff (typically each physician and the lead office manager) require RSA SecurID Tokens for accessing the PPN outside of the practice (e.g. home);
- Assess the Internet based applications the practice uses that may require updates to the PPN firewall. As a standard security measure, the PPN firewall is locked down to a core set of applications using standard Internet ports and protocols. This includes:
  - PITO qualified EMR vendor applications;
  - General Internet sites (e.g. Google) available through standard protocols/ports;
  - Clinical Internet sites (e.g. Chronic Disease Management toolkit) available through standard protocols/ports;
  - Health Authority Internet portals;
  - Email clients (e.g. MS Outlook) using standard mail protocols; and
  - Additional applications included on a case by case basis.



See the "PPN Technical Reference" document for further technical details on: 1) preparing the demarc location for installation of the TELUS router equipment in a practice, 2) the current list of applications allowed through the PPN Core firewall, and 3) how to request additional applications required by the practice to be allowed through the firewall.

The PITO RM will pass on the practice profile information to the Ministry of Health Services and TELUS for implementation of the PPN service.

### 3.2.2 Building Wiring and Practice LAN

Practices are responsible for:

- Obtaining and arranging for all rights of way, permissions, and/or third party consents for TELUS to install or upgrade any required PPN network wiring within their property to the practice demarc location. This wiring will be either copper or fibre depending on the router selected for practice;
- Any costs for installing or upgrading conduit required to run TELUS wire or cable from the building entrance to the practice's demarc location; and
- Arranging for all of their LAN network equipment and wiring.



See the “PPN Technical Reference” document for further technical details on the practice responsibilities for: 1) building wiring, 2) practice LAN requirements, and 3) guidelines on practice LAN preparation.

### 3.2.3 Selecting a Live Date

In consultation with their PITO RM and chosen EMR vendor, each practice will select a live date to begin using their PITO-Qualified EMR application over the PPN network. The target live date chosen must consider the lead times for preparing for and installing the TELUS router equipment into their practice, as outlined in the steps below.

PITO works in collaboration with the Ministry and TELUS to ensure the practice profile information is completely documented and to establish due dates that are achievable for PPN equipment installation.

The practice migration plan must be re-evaluated at these key milestones to assess impact to the target live date:

1. As a first step, a request is made to TELUS to ‘pre-qualify’ or confirm that the necessary router equipment (see Table 1) can be installed at the practice location. TELUS will assess the type of router being installed, the distance from their local Central Office and, especially for rural or remote locations, whether the network service is available in the area. In most cases, TELUS will affirm the preferred network router can be installed. On an exception basis, TELUS will advise that another router/service needs to be selected – this can delay standard install timelines. This pre-qualification step typically takes 1-2 weeks to complete.
2. With a successful pre-qualification result, the order to install the PPN router is sent to TELUS. Once signed orders are sent from the Ministry, TELUS guidelines for installing PPN routers are:
  - For PPN-1 and PPN-2 (copper/ADSL based services): 27 business days for urban locations and 37 days for rural;
  - For PPN-3 and PPN-4 (fibre based services): currently takes an average of 3 months to install;

Once a signed order is received, TELUS will book the installation into their provisioning system and provide a due date back to the Ministry. In some cases this due date could be longer than standard

timelines, so the EMR implementation plan for a practice needs to include contingency for possible PPN installation delays.

Other key timeline factors to consider are:

1. EMR vendors require the PPN TELUS router equipment to be installed ahead of the EMR live date. These lead times vary by vendor and can range from 3 to 6 weeks. Check with the EMR vendor for their preferred timing; and
2. If the practice has to undertake any site readiness activities (e.g. LAN wiring, building wiring, etc.), they must determine the time required for this and build it into their plan.



See the “EMR and PPN Implementation Checklist” for estimated timelines for implementing the PPN.

### 3.3 Installing the Service

#### 3.3.1 TELUS Router Equipment

Key milestones for installing the service are:

- Approximately ten days after receipt of the PPN installation order, the TELUS coordinator will phone the main practice contact to confirm that the assigned install due date will work for the practice, and if not, will negotiate a revised date;
- For fibre based services (PPN-3 and PPN-4): after the router equipment has been ordered with TELUS, they will initiate a ‘pre-field’ inspection to ensure that conduit is in place to install the fibre cable from the building entrance to the practice demarc location. The practice will be informed if they need to arrange for any upgrades;
- Five to ten days prior to the install due date, a TELUS coordinator will phone the main contact in their practice to arrange for office access on the day of installation; and
- On the scheduled day, the TELUS installer will arrive on site, expecting all of the practice’s site preparation responsibilities to be completed. The installer will install the TELUS router equipment in the designated demarc location, test the installation, and capture performance metrics, TELUS does additional work back at their local office to complete the router configuration (which can take approximately 2 additional business days), after which they will notify the practice contact, along with PITO and the Ministry, of successful completion. The performance metrics are provided to the Ministry, and are also made available to the practice’s EMR vendor. These metrics provide a baseline PPN performance profile for each practice that can be referenced by the EMR vendor Tier 1 helpdesk staff if a practice reports any performance issues in the future.

#### 3.3.2 Migration to the PPN

If a practice is already connecting to an EMR through an existing Internet connection, the PITO EMR vendor will work with the practice to migrate to the PITO-Qualified EMR application over the PPN. This will involve updating the software settings on practice workstations, connecting the practice LAN to the PPN router and testing all required applications can be accessed. The practice’s technical support resource for their local computer environment will be engaged in these migration activities. Physicians should also be aware that their assistance with testing and verifying they can access necessary applications is a critical part of the migration process.



## 4.0 Using the PPN

### 4.1 Connecting At the Practice

Once the PPN connection has been successfully installed, tested and implemented, it will be the practice's network connection to the outside world.

The EMR vendor will provide each practice with the details for accessing their EMR application over the PPN.

### 4.2 Connecting from Home

The practice PPN contact will receive RSA SecurID Tokens for each of the designated (and approved) staff in their practice directly from TELUS by courier,

A welcome letter, user guide, assigned user names and PINs (personal identification numbers) will be sent to the practice PPN contact by TELUS. This package will contain all of the information needed to connect from outside the office to the VPN service.



See the "Remote Access to the Private Physician Network" for instructions on accessing and using the VPN service.



PITO has policies for securing data accessed on mobile devices such as laptops. See the PITO Policies document at [www.pito.bc.ca](http://www.pito.bc.ca) under the 'Document Library' section.

### 4.3 Connecting to Email

For practice email, the PPN allows for standard email clients (e.g. MS Outlook, Thunderbird) to access their external mail services (e.g. Shaw, Yahoo, etc). The PPN also supports web access (e.g. webmail) to external mail services that provide this feature.



See the "PPN Technical Reference" for further information on re-configuring the practice's preferred email client for accessing their email service over the PPN.

Most physicians maintain more than one existing email account (e.g. health authority, practice, academic, personal), so it will be important for a practice to test each of these email services as part of their migration to the PPN.



## 5.0 Key Responsibility Summary

Each group involved in setting up and using the PPN has a set of key responsibilities. They are:

### 5.1 TELUS Responsibilities

- Provide the TELUS router equipment, PPN core, and two factor authentication VPN services;
- Maintain the PPN service infrastructure in proper working order, and perform maintenance in scheduled windows;
- Provide Tier 2 and 3 help desk support for resolving TELUS router equipment, PPN core, and 2 factor authentication VPN services related problems as reported through the practice's EMR vendor support line; and
- Comply with all obligations outlined in the Master Services Agreement with the Province of British Columbia.

### 5.2 EMR Vendor Responsibilities

- Provide Tier 1 help desk support for any EMR or PPN problem. For the PPN, this includes: TELUS router equipment, PPN core, and 2 factor authentication VPN services related problems; and
- Comply with all obligations outlined in their Master Services Agreement with the Province of British Columbia.

### 5.3 Practice Responsibilities

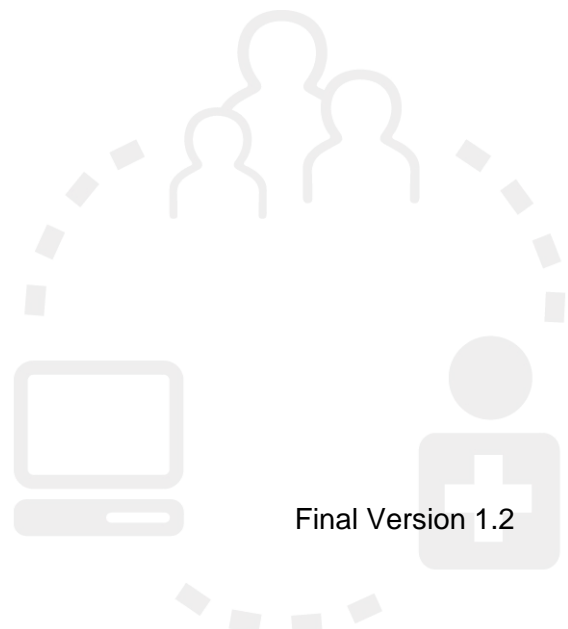
- Understand and comply with PITO Privacy, Security and Acceptable Use policies;
- Obtain and arrange for all access, rights of way, permissions, and/or third party consents for TELUS to install, upgrade or maintain any required PPN network wiring within the property up to the practice's demarc location;
- Cover any costs for the installation or upgrading of conduit required to run TELUS wire or cable from the property line to the practice's demarc location;
- Continue to be responsible for all of the practice computer related hardware, software and network infrastructure, including its security, up to the point of connection into the TELUS-provided router equipment (Ethernet input);
- Maintain the security of all VPN related user IDs and passwords assigned to practice staff;

- Prior to start of any PPN install or maintenance activities, as an industry best practice, it is highly recommended that existing files residing on your practice computers be backed up to a different device; and
- Ensure the latest version of reputable anti-virus software and virus definition files are installed on all practice computers and kept current by automatic updates. This includes computers from remote locations such as from home, which will be used to access the PPN using the TELUS provisioned VPN service.



New viruses and worms are being developed within the global Internet community daily. Automatic virus updates are required to ensure that the practice network and the PPN are protected against them.

Should at any time your practice network become infected with a virus, it could directly affect the entire PPN. TELUS will, if required, disconnect your practice from the PPN until you are able to clean your entire network of serious virus or worm outbreaks.





## Appendix A - Definitions

**Anti-Virus:** In the context of computer systems, anti-virus software is a computer program that attempts to identify, neutralize or eliminate malicious software. This type of software is so named because the earliest examples were designed exclusively to combat computer viruses; however most modern anti-virus software is now designed to combat a wide range of threats, including worms, phishing attacks, root kits, Trojan horses and other malware.

**Bandwidth:** See 'network bandwidth' definition below.

**Circuit:** In the context of computer networking, a physical communication cable or wireless transmission facility between two locations. For the PPN, a circuit connects the PPN router installed at the physician premises to the nearest TELUS central office.

**Customer Interface Unit (CIU):** The TELUS router equipment that provides a LAN interface port into which the physician office connects their office network into. The CIU, or router, is usually located in a master telephone closet in the physician practice or building.

**Demarcation Point:** The point at which the PPN router is installed and connects with the wiring at the physician premises. This point marks where the PPN ends and the practice LAN begins.

**Electronic Medical Record (EMR):** Is a computer-based patient medical record, which is supported by the clinical and practice management system.

**Extranet:** In the context of the PPN, it is a private network that securely extends connectivity to other health sector stakeholders including EMR vendors. In the future, this will also extend to health authorities, and other 'eHealth' initiatives. The Extranet is not available to the general public.

**Firewall:** A dedicated appliance, or software running on a computer, which inspects network traffic passing through it, and denies or permits passage based on a set of rules.

**Intrusion Detection System (IDS):** An IDS generally detects unwanted manipulations of computer systems, mainly through the Internet. The manipulations may take the form of attacks by network hackers. An intrusion detection system is used to detect several types of malicious behaviors that can compromise the security and trust of a computer system. This includes network attacks against vulnerable services, data driven attacks on applications, host based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and malware (viruses, Trojan horses, and worms).

**Last Mile:** Is the final leg of delivering network connectivity from a communications provider to a customer. With regards to the PPN, it is the private and highly reliable dedicated network connection installed between the nearest TELUS Central Office and the practice location.

**Live Date:** The time at which the EMR is “turned on” for use in day-to-day care and the practice physician(s) and staff begin regular use of the EMR (i.e. after implementation, testing, and training).

**Local Area Network (LAN):** The network within the walls of the physician’s office that connects the computers and printers to the Private Physician Network.

**Master Standing Agreement (MSA):** An overall agreement or contract between the Province of BC and external vendors (such as TELUS or EMR vendors) that sets out the terms for their participation in the PITO initiative.

**Network Bandwidth:** The amount of data that can pass through the network circuit to the physician’s office (i.e. “the size of the pipe”).

**PITO Solution Offering:** The full suite of products and services available to eligible BC physicians through the Physician Information Technology Office (PITO) including:

- Electronic Medical Record (EMR);
- Hardware;
- Network;
- Other Implementation Costs; and
- PITO Implementation & Transition Support Program (ITSP).

See the PITO website at <http://www.pito.bc.ca/> for the most up to date offering details.

**PITO Privacy and Security Checklist:** A checklist completed by the physician and PITO resource to ensure that critical privacy and security issues have been properly addressed.

**PITO-Qualified EMR:** An EMR which has passed conformance testing with the Ministry of Health Services to ensure it meets all core requirements as stated in the Request for Proposals procurement process initiated in February 2007.

**Private Physician Network (PPN):** The private network provided by the Ministry of Health for access from the physician’s office to the EMR and Ministry or health authority systems. The physician may also access the PPN from outside their office using a Virtual Private Network (VPN) service provided by the PPN.

**Quality of Service (QOS):** In the context of computer networking, QOS refers to a network’s capability to either assign a different priority to the transmission of different network data types (e.g. HTML, FTP, etc), or guarantee a level of performance.

**Registration Agreement:** The legal agreement between the physician and the Ministry of Health Services that establishes the stipulations for funding and participation in PITO.

**Router:** Is a network hardware device that directs, forwards or routes network traffic.

**Server:** A type of computer designed to store files and software for access from other computers on a network (e.g. a “file server”, “web server”).

**Tier 1 Helpdesk:** Provides the initial support for all end user issues relating to a) the complete EMR offering, b) any other products and services provided by the vendor, c) client-side hardware and software, and (d) related PPN network connectivity. The specific services offered include a) the initial triage and assessment of the problem and a determination of the area of scope in which the problem resides, b) an assignment of a unique identifier, c) initial attempts to resolve the issue by phone or email, and d) routing

of the problem to the appropriate area of scope (e.g., physician office IT support, TELUS, EMR Tier 2, etc.).

**Tier 2 Helpdesk:** Address those incidents and issues that a) directly relate to the complete EMR offering and PPN network connectivity and b) are too complex to resolve via the Tier 1 Help Desk services.

**Uninterruptible Power Supply (UPS):** Battery units which allow a computer or other device to continue operating for a short period during a power outage.

**Virtual Private Network (VPN):** An authentication and encryption mechanism which allows connection from outside the physician office to their EMR over the Internet with enhanced security.

