

Private Physician Network (PPN) Health Authority Gateway Primer

Date Created: June 20, 2009
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

1.0	BC's eHealth Information Highway	5
1.1	The Private Physician Network	5
1.2	The eHealth Network Gateway	5
1.3	The TELUS Extranet	6
1.4	The Big Picture	6
2.0	PPN Overview	7
2.1	Immediate Benefits	7
2.2	PPN Service Features	7
2.2.1	PPN Core Network Features	7
2.2.2	Connecting Inside the Practice	8
2.2.3	Connecting Outside the Practice	9
2.3	Cost for the Service	9
2.4	Support	10
2.5	Service Levels	10
2.5.1	PPN Service Levels	10
2.5.2	PPN Maintenance	11
3.0	Connecting to and Using the PPN	12
3.1	Connecting to the PPN	12
3.2	Using the PPN	12
3.2.1	Connecting At the Practice	12
3.2.2	Connecting from Home	12
3.2.3	Connecting to Email	13
4.0	Key Responsibility Summary	14
4.1	Practice Responsibilities	14
4.2	TELUS Responsibilities	14
4.3	EMR Vendor Responsibilities	14
4.4	Health Authority Responsibilities	14
	Appendix A - Definitions	15

Figures

Figure 1 Key Network Connections	6
--	-------------------

Tables

Table 2 PPN Network Service Level Targets	11
---	--------------------



Purpose of This Document

This document provides information to practices participating in the Physician Information Technology (PITO) program where the practice resides on one of the following Health Authority (HA) managed networks:

- Northern Health's (NH) Physician Connect
- Vancouver Coastal Health (VCH) Diamond Centre

Practices on these specific networks will connect to their PITO-Qualified EMR through a gateway installed at their Health Authority which then connects to the Private Physician Network (PPN) service.

This document should be used by PITO local relationship managers (LRMs), physicians, practice staff, EMR vendors and other involved parties. Its purpose is to inform them in their efforts to connect to the PPN from a gateway connected practice.

Related Documents

The following document is available on the PITO website at www.pito.bc.ca under its 'Document Library' section and is applicable to PPN gateway connected practices at both NH Physician Connect and VCH Diamond Centre:

- **PPN Health Authority Gateway Support Quick Reference:** A summary for PPN gateway connected practices physicians and staff that describes the support available to them through their EMR vendor, TELUS and the local Health Authority.

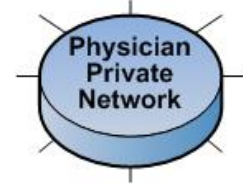
The other PPN documents available on the PITO website at www.pito.bc.ca under its 'Document Library' section are **not** applicable to PPN gateway connected practices. They are only applicable to PITO practices that connect to the PPN through a router installed by TELUS at their practice.

1.0 BC's eHealth Information Highway

1.1 The Private Physician Network

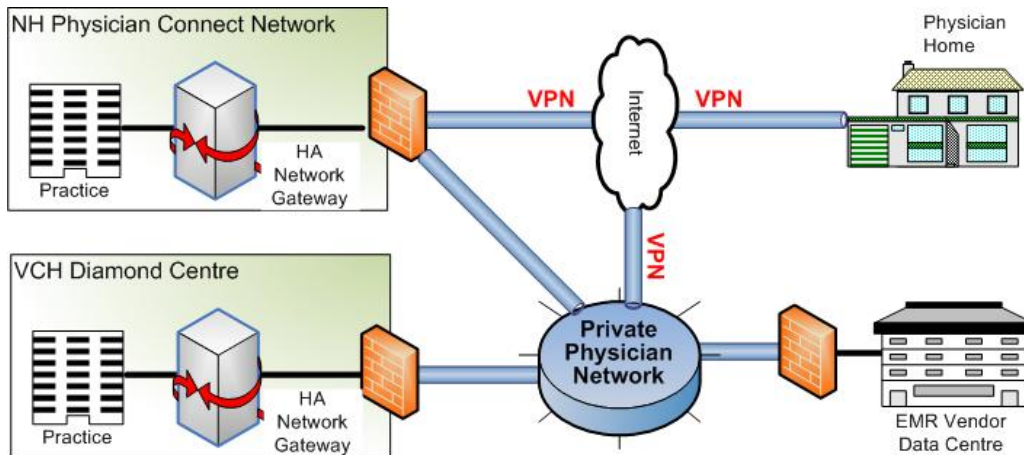
The PPN is the private, high-speed network that is available to physician practices when they register and are accepted into the PITO program. It is a key component of the suite of products and services being offered to British Columbian physicians through PITO.

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



The PPN enables physicians and their staff to privately access the clinical information in their PITO-qualified Electronic Medical Record (EMR) systems. It also provides an option for secure access to 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.

Physicians in the Northern Health region that currently connect to the wireless Physician Connect Network, as well as those residing in Vancouver Coastal's Diamond Centre building will continue to access their existing Health Authority (HA) network services. A network gateway has been put in place to allow NH Physician Connect and VCH Diamond Centre physicians to access their PITO-Qualified EMR through the PPN over the existing network supplied by their local Health Authorities.



1.2 The eHealth Network Gateway

The eHealth Network Gateway (eNG) is another new network, which is replacing the Provincial Network Gateway or "PNG" that currently links the six health authorities. When inter-connection with the PPN is



complete, the eNG will share a secure connection to the PPN to allow 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 five EMR vendor data centres. As other eHealth 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 gateway-connected physicians and their 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.

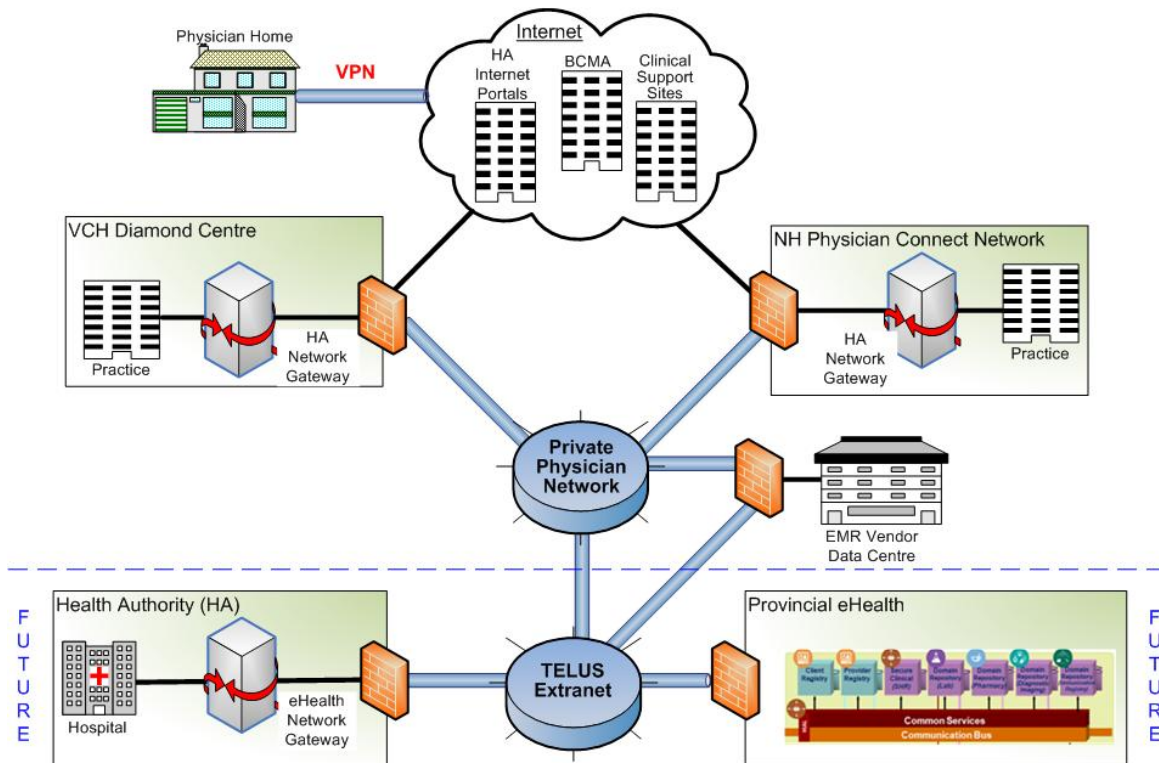


Figure 1 Key Network Connections



2.0 PPN Overview

2.1 Immediate Benefits

The PPN is the physicians' private lane on BC's eHealth information highway. Physicians and their staff will connect through their PPN gateway to:

- Access their selected EMR application;
- 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 eHealth 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 additional 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 sections below describe the infrastructure and services provided to physician's practices through this Agreement.

2.2.1 PPN Core Network Features

The PPN Core is a private network used for PITO-qualified EMR access. Its key features are:

- **Security:** Provides industry best practice and robust firewall, anti-virus, and intrusion protection network services that protects it from external threats coming from the public Internet. As well, it protects from internal threats coming from gateway-connected practices.
- **Private:** Network traffic between the gateway connected practices and their EMR vendor data centers is private because it does not travel over the public Internet;
- **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. Eventually, the PPN will provide an option for access to other provincial eHealth systems such as PharmaNet.

While the PPN does have a secure gateway to the public Internet, NH Physician Connect and VCH Diamond Centre practices will continue to utilize the Internet connections provided by their local Health Authority network.

2.2.2 Connecting Inside the Practice

2.2.2.1 Northern Health Physician Connect

Northern Health (NH) has overcome the geographic challenges of its region and has connected many of the region's practices to its Physician Connect Network. In rural locations, shared radio transmission is the predominant network technology.

For practices in the north that are already connected to the NH network, a network gateway has been put in place which routes physician network traffic to their PITO-Qualified EMRs through the PPN. Only EMR network traffic from practices participating in the PITO program is allowed through this gateway. The network routing and security controls for this are managed by NH. Access to the Internet and NH systems/services will continue to be provided through the Northern Health's Physician Connect Network and will not change.



Northern practices using the NH Physician Connect Network should dialogue directly with NH for any information they require on Physician Connect's features, support, service levels, or remote access.

2.2.2.2 Vancouver Coastal Diamond Centre

Vancouver Coastal Health (VCH) has installed and manages the network in the Diamond Centre building in Vancouver. At each practice, a connection point, providing Internet services, is available to this network. A PPN network gateway has been installed in the Diamond Centre building which routes PITO physician network traffic to their PITO-Qualified EMRs through the PPN. Only EMR network traffic from practices participating in the PITO program is allowed through this gateway. The network routing and security controls for this is managed by VCH. Access to the Internet and VCH systems/services will continue to be provided by Vancouver Coastal Health and will not change.



VCH Diamond Centre practices using the building network should dialogue directly with VCH for any information they require on its features, support or service levels.

2.2.3 Connecting Outside the Practice

2.2.3.1 NH Physician Connect

NH Physician Connect practices will continue to use NH's remote access service, with its Two Factor authentication approach. This service currently provides remote access to NH specific sites and resources. It will also provide access to the practice's PITO-qualified EMR.



Northern practices using the NH Physician Connect Network should dialogue directly with NH for any information they require on gaining access or using its remote access services.

2.2.3.2 VCH Diamond Centre

VCH Diamond Centre practices can opt to use the PPN's remote access service for accessing their PITO EMR from outside their practice (e.g. home).



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



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

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.

2.3 Cost for the Service

The Ministry funds the following components for PPN gateway connected practices:

- Installation of the TELUS router equipment at the local Health Authority site, used by practices to access their PITO-qualified EMR;
- PPN core network; and
- PPN's VPN remote access service (for VCH Diamond Centre practices only).

Gateway connected practices will continue with any funding arrangements they have with PITO for:

- Computer equipment and LAN; and
- Office software.

Practices will continue any funding arrangements they have with their local Health Authority for:

- Network connections within their practice location provided by NH Physician Connect or VCH Diamond Centre networks; and
- NH Physician Connect VPN remote access service (for NH practices only).

2.4 Support

A summary of key support responsibilities for practices connecting through their HA gateway to the PPN is provided below.

- EMR Vendor: Provides Tier 1 help desk support for the EMR application. For the VCH Diamond Centre only, Tier 1 also includes support for 2 factor authentication VPN service related problems;
- Health Authority: Provides Tier 1 help desk support for the PPN as well as for the HA-provided network. In cases where the HA determines that the problem originates with the PPN their network support group will contact TELUS directly for resolution. For the Northern Health only, support will include resolution of problems with their own 2 factor authentication VPN service;
- TELUS: Provides Tier 2 and 3 help desk support for resolving PPN network, and 2 factor authentication VPN services related problems as reported through the Tier 1 support lines; and
- Practice: Organizes the technical support services required for the practice's local computers, printers and LAN up to the connection into the Health Authority provided network equipment.



Further details on technical support available when connecting through the HA gateway to the PPN is provided in:

- "PPN Health Authority Gateway Support Quick Reference"

This document is available on the PITO web site at www.pito.bc.ca under its 'Document Library' 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. These 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 Health Authority gateway router to TELUS central office ('last mile')	99.90% or better
PPN Core Network		99.95% or better

For PPN network failures either in the PPN core, or at the TELUS router installed as the PPN gateway at the Health Authority site, TELUS's target to restore the service is within 4 hours.

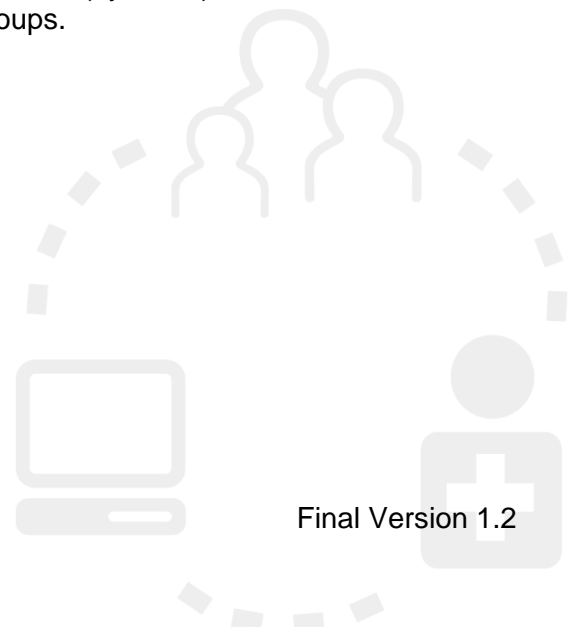
2.5.2 PPN Maintenance

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 and local Health Authority.

If TELUS needs to make PPN service impacting changes outside of standard maintenance times, they will provide advance notice to the Ministry unless they classify the changes as an emergency. Again, the Ministry will forward (by email) this information onto EMR vendors and local Health Authority support groups.





3.0 Connecting to and Using the PPN

3.1 Connecting to the PPN

In order to connect to a practice's EMR through a PPN gateway, the PITO local relationship manager (LRM) will facilitate a request through to the Ministry of Health Services and Health Authority. Security restrictions are in place to only allow PITO authorized practices to connect through the gateway network to their PITO EMR application.

For the VCH Diamond Centre only, each practice will also work with their PITO LRM to 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).

Once access through the PPN gateway is in place, the practice will work with either their local computer (IT) support and/or EMR vendor to test/confirm the access to their EMR application. Other implementation activities, with associated timelines, for the practice's live migration to the EMR through the PPN gateway will be co-ordinated through the EMR vendor.

3.2 Using the PPN

3.2.1 Connecting At the Practice

Once the security has been implemented to allow the practice to connect through to the PPN gateway, the EMR vendor will provide the practice with the details for accessing their EMR application over the PPN. All other network access provided by your Health Authority, including Internet, will remain unchanged.

3.2.2 Connecting from Home

3.2.2.1 NH Physician Connect

For NH, the practice will use their VPN remote access service. Practices should contact NH directly for details on their service.

3.2.2.2 VCH Diamond Centre

For VCH Diamond Centre, the practice PPN contact will receive RSA SecurID Tokens for each of the designated (and approved) staff in the practice directly from TELUS by courier.



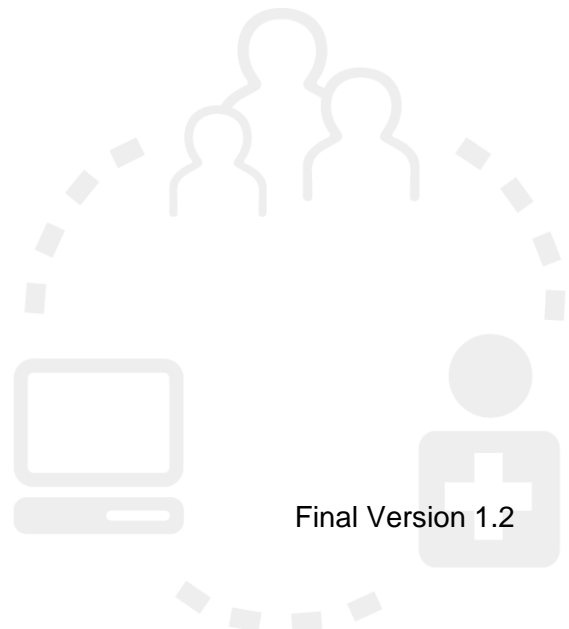
A "Remote Access to the Private Physician Network" guide with instructions for accessing and using the PPN VPN service is provided at the time RSA SecurID tokens are distributed to the practice. As some instructions vary by EMR application, a separate document is provided for each EMR Vendor.



PITO has policies for securing data accessed on mobile devices such as laptops.
See the PITO Policies document at www.pito.bc.ca under its 'Document Library' section.

3.2.3 Connecting to Email

Existing arrangements for accessing email either from the HA or practice specific provider (e.g. Shaw, TELUS, gmail, hotmail, etc) will not change.





4.0 Key Responsibility Summary

Each group involved in providing access to a PITO-qualified EMR from a HA network through to the PPN has a set of key responsibilities. They are:

4.1 Practice Responsibilities

- 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 local Health Authority network; and
- Understand and comply with PITO Privacy, Security and Acceptable Use policies.

4.2 TELUS Responsibilities

- Maintain the PPN service infrastructure in proper working order, and perform maintenance in scheduled maintenance 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 local HA network support group; and
- Comply with all obligations outlined in the Master Services Agreement with the Province of British Columbia.

4.3 EMR Vendor Responsibilities

- Provide Tier 1 help desk support for any EMR problem. For VCH Diamond Centre only, also provide Tier 1 support for 2 factor authentication PPN VPN services related problems;
- Co-ordinate the implementation of the EMR (through the PPN) at the practice; and
- Comply with all obligations outlined in their Master Services Agreement with the Province of British Columbia.

4.4 Health Authority Responsibilities

- Provide Tier 1 help desk support for any HA or PPN network problems. For NH Physician Connect only, NH will also provide Tier 1 support for its 2 factor authentication VPN services related problems; and
- For network problems that originate in the PPN, contact TELUS Tier 2 help desk to report, and own the problem until its final resolution.



Appendix A - Definitions

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).

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.

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.

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.

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").

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.

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.

