Ontario Health (OTN)

Technical Service Level Agreement

Updated: January 12, 2021

Ontario Health
OTN

Table of Contents

1 Preface

The purpose of this document is to:

- Provide a clear and succinct description of the support services that Ontario Telemedicine Network (OTN) provides its Members.
- Clarify the roles, responsibilities, and expectations of OTN, and its Members, with respect to the delivery of quality care through telemedicine.

This document is intended for new, current, and prospective Members of OTN and should be read by Telemedicine Coordinators, Network Administrators, IT Technical Support staff (including Audio Video Support and Telemedicine Coordinators) to understand their commitment and obligations as part of the OTN network.

The latest version of this document is located online in the Resource Library: *https://support.otn.ca/sites/default/files/otn-tsla.pdf*.

Copyright Notice

2 Connecting to OTN

Part of OTN's mission is to develop and operate a world class technical environment to enable our Members to deliver telemedicine practice of the highest caliber of security, quality and reliability. This is only possible if all sites/Members adhere to established OTN standards for hardware, software, processes, and network architecture. This enables Members to connect to one another and access OTN services reliably. At the same time standards enable OTN to support our Members and provide a consistent user experience.

From a technical perspective, OTN standards apply to the following:

- Network architecture
- Videoconferencing equipment
- Security compliance
- Computer systems

These technical standards are addressed in the following sections.

2.1 Network Architecture

Network design and support is one of the most important factors in ensuring secure, reliable, high-quality telemedicine. Network connections between site(s) and OTN are configured in various ways, depending on needs, chosen service providers and the type of equipment a Member plan to use. This section provides an overview of the available connection options. A representative from the OTN Adoption Team, and/or an OTN technical staff will help a Member to choose the right option for their business applications.

2.1.1 On-Net Connections

If a Member plans to deploy telemedicine carts or room-based systems, the On-Net connection is the preferred architecture. An On-Net system requires OTN to install a router at a Member site and use this device to connect the videoconferencing systems to the OTN network. This operation will allow OTN Technical Support staff to configure, manage and support remotely the videoconferencing systems.

On-Net Connections require the provision of a VLAN or dedicated video LAN cabling within a site's local network, allowing extension of the OTN address space from the installed OTN demarcation router directly to the installed endpoints (see diagram on page 5). This type of connection is provisioned over any suitable backhaul network including eHealth Ontario, ORION, a community network, a private Bell MPLS connection, or the Internet.

The demarcation device requires one interface to be addressed natively on the external network and one interface to be included in the VLAN provided to the site. The demarcation device will provide the default gateway for all OTN systems located on the dedicated VLAN. Redundant VPN tunnels are established from the demarcation device to OTN central
VPN concentrators to enable core redundancy.

All traffic is encrypted from the demarcation device outward and all OTN devices are addressed with OTN address space.

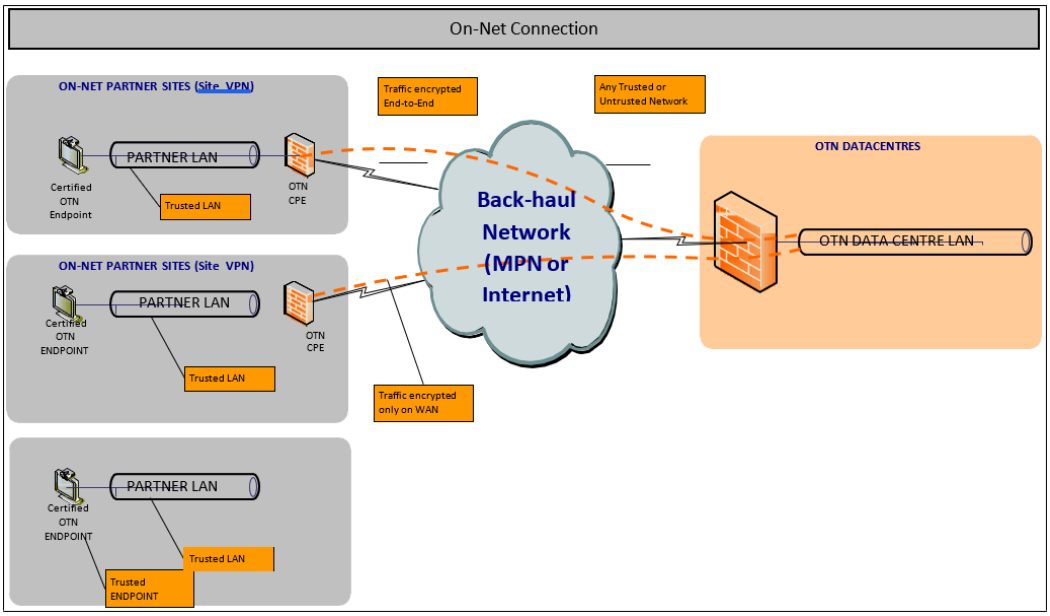


Figure 1: On-Net Connection Architecture

Requirements:

- Configuration of a dedicated VLAN or physical LAN for use by OTN equipment.
- Installation of an OTN router.
- Provision of a native address on the backhaul network.

Limitations:

- All devices must be on a dedicated VLAN (This may require configuring to specific ports for VLAN membership or employing 802.1x automatic VLAN assignment).
- OTN endpoint monitoring services will not be available until the endpoint is powered on and connected to the dedicated VLAN.

2.1.2 OTN "Off-Net" IP Gateway Video Conferencing Service

As described above, the On-Net Connection architecture connects a site's videoconferencing system to OTN's VPN for a highly managed and reliable telemedicine service.

Although there are many advantages to the On-Net Connection architecture, it may not be appropriate if:

- The site's videoconferencing equipment or medical peripherals are not among the makes and models supported by OTN. (See the *List of Standard Equipment*.)
- The site regularly connects to endpoints outside of OTN.
- The site will connect to OTN via a private network not among those supported by OTN.
- For these situations, OTN offers an IP Gateway service.

The OTN IP Gateway videoconferencing service is currently deployed at a small number of Member locations. These are organizations that, for the most part, operate and maintain independent videoconferencing infrastructure. They wish to have access to the OTN videoconferencing network, while maintaining the flexibility and autonomy of operating an independent service.

The IP Gateway service is deployed across an organization's existing connectivity; usually an Internet service or an ORION/CANARIE research network service. In this instance, OTN does not provide any support for network connectivity. The Member's site is also responsible for making any firewall/security changes related to the facilitating of OTN videoconferencing connectivity. OTN does provide a firewall traversal appliance at the edge of the OTN network to provide access to the internal videoconferencing service.

Member sites are responsible for the following:

- Purchasing videoconferencing systems and maintaining ongoing vendor support agreements for their systems, if desired.
- Providing their own first level technical support for their systems.
  Note: OTN does not provide any support for the videoconferencing systems and only provides support for issues with videoconferences that are occurring with the OTN network. OTN performs basic system connectivity and certification test to confirm the site's IP Gateway system(s) will connect to the OTN network.

Videoconferencing calls are point-to-point (two systems), or multipoint (three or more systems). In all cases, IP Gateway site systems cannot call into the OTN network, and all videoconferences (point-to-point and multipoint) are initiated by OTN's bridging infrastructure.
This ensures OTN's security and network integrity, since OTN has no control over the security of the site's network, nor of the site's videoconferencing systems.

OTN IP Gateway sites do not have access to some of the advanced services that OTN offers to On-Net sites.

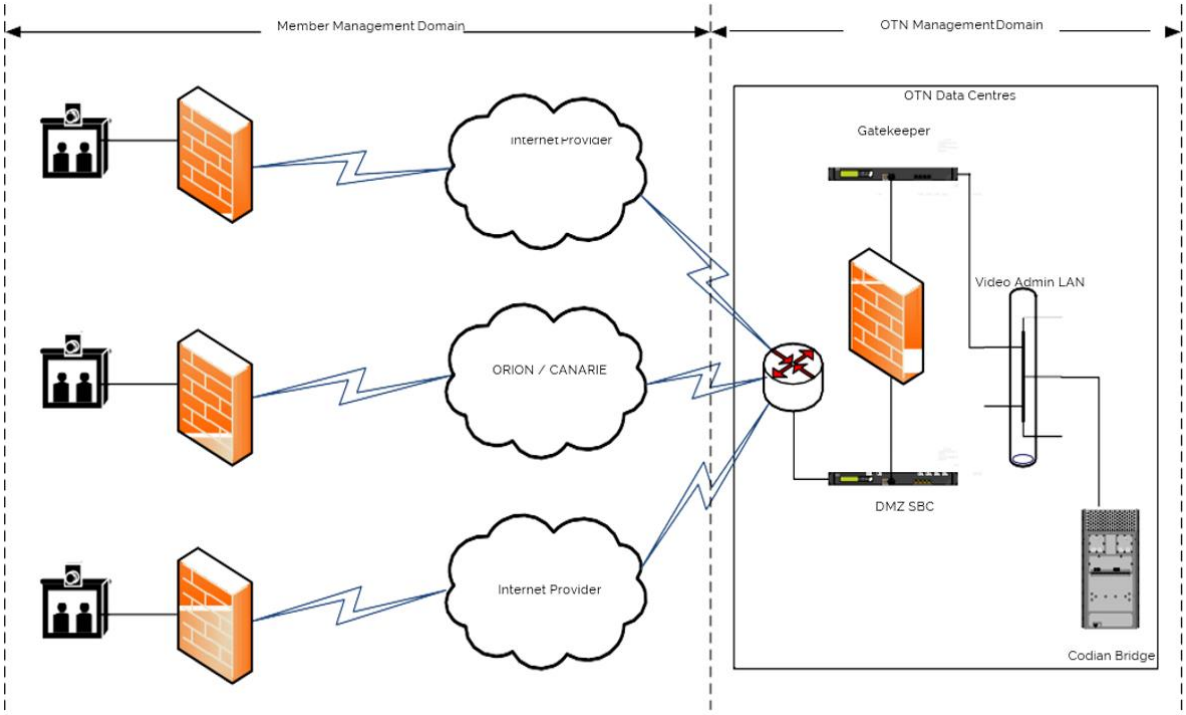


Figure 2: Network diagram

Off-Net IP

OTN maintains a Session Border Controller (SBC) infrastructure to facilitate IP connectivity to sites that are not in the OTN Virtual Private Network (VPN) but do have suitable alternate network connectivity. All systems that wish to participate in Off-Net IP calls must support standards-based encryption to participate in events as an Off-Net system.

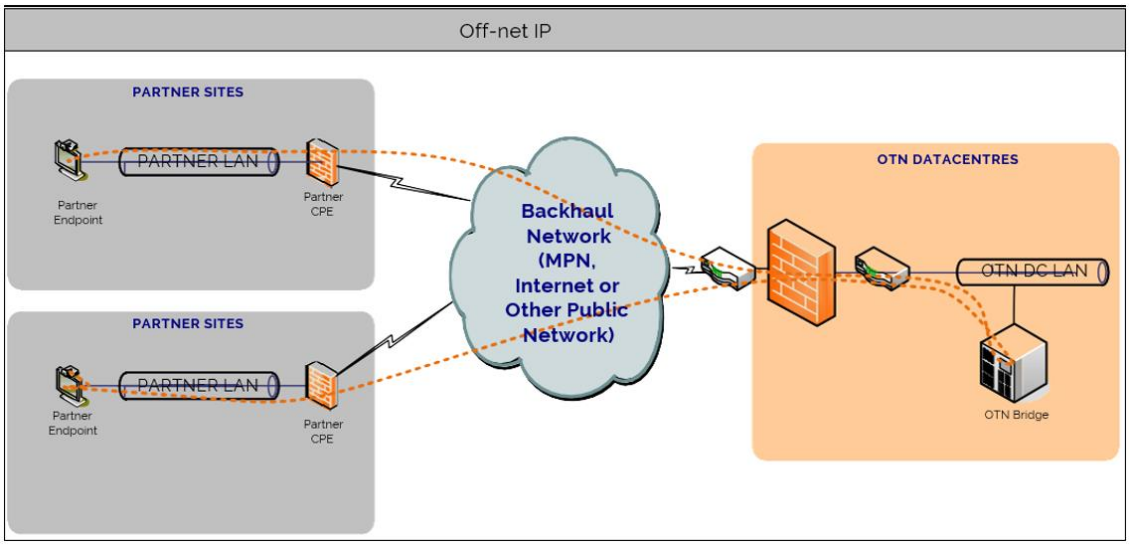


Figure 3: Off-Net IP Connection Architecture

Requirements:

- Sites must provide suitable network connectivity through the Internet, eHealth Ontario or other publicly available networks.
- Sites must either maintain a suitable SBC solution or appropriate access to endpoints through corporate firewalls.
- Systems in use should support DNS-based dialing.
- Systems in use must support standards-based video conferencing encryption (AES).

Limitations:

- All events must be scheduled through the OTN Contact Centre.
- OTN Technical Support can provide only very limited troubleshooting, since there is no direct visibility into endpoints connected via ISDN. The site's technical resources must provide first-level support for these systems.
- The OTN GAB (Global Address Book) is not available for these endpoints.

ISDN Services

ISDN is a very well-defined and mature standard of connectivity. OTN maintains a bank of ISDN (Integrated Service Digital Network) PRI (Primary Rate Interface) lines to facilitate connectivity to the public telephone network. To connect via ISDN the site must have ISDN lines (BRI (Basic Rate Interface) or PRI (Primary Rate Interface)) installed and must use ISDN-capable video systems.

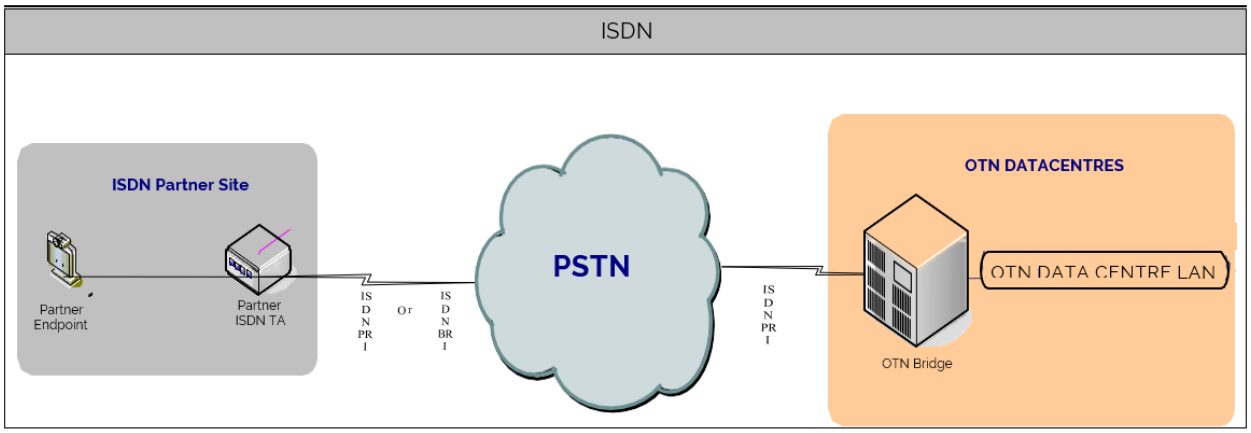


Figure 4: Off-Net ISDN Architecture

Requirements:

The site must maintain ISDN capacity in the form of BRI (Basic Rate Interface) or PRI (Primary Rate Interface) circuits.

Endpoints must be ISDN compatible.

Limitations:

All events must be scheduled through the OTN Contact Centre.

The OTN Technical Support team can provide only very limited troubleshooting, since there is no direct visibility into endpoints connected via ISDN. The site's technical resources must provide first-level support for these systems.

The OTN GAB (Global Address Book) is not available for these endpoints.

2.1.3 Network Bandwidth

Network bandwidth requirements for videoconferencing over the Internet are listed in the table below[1]. These requirements apply to each room-based video system at the site. If a site has more than one system sharing an Internet connection, the bandwidth required must be multiplied accordingly.

For example, if a site plans to use two videoconferencing systems sharing a single Internet connection, the available upload bandwidth would need to be at least 1.6 Mb (2 x 800 Kb/s). Download bandwidth would not need to be increased if it is at least equal to upload bandwidth. Monthly data transfer would also need to be doubled, to 200 Gb.

Dedicated Internet Connectivity Requirements:

Service Parameter	Requirement
Service Type	High-Speed Internet
Bandwidth Allocation	Dedicated Business
Download Speed	> 2000 kbps
Upload Speed	> 2000 kbps
Monthly Data Transfer	> 100 Gb
Technical Support	24/7
Mean Time to Repair	24 hours or less
# of Dynamic IPs	1

Considerations when using the Internet for Videoconferencing:

The quality of service available from ISP (Internet Service Providers) to Internet users can fluctuate significantly, depending on the number of users sharing the service, the volume of activity, the number of intermediary networks traversed, and other factors beyond the user's control. Since real-time applications such as videoconferencing are highly sensitive to network conditions, it is very important to carefully manage any Internet circuit used to deliver telemedicine. Here are some tips:

- Run only one videoconferencing session at a time over an Internet connection that is designed to support only one session.
- It is best practice to have a dedicated Internet connection for a videoconferencing session. Sharing the Internet connection with other Internet applications and users may degrade the video quality or may lose the video connection if there is insufficient bandwidth to support the

[1] Future OTN services may require a reassessment of bandwidth requirements.
Each videoconferencing session requires the same amount of available bandwidth, regardless whether the endpoint is a hardware appliance (such as a telemedicine cart) or a software client running on a PC. Following this practice will significantly increase the video experience.

demand. It is a good practice to have a backup plan in the event of an Internet outage, if the Internet connection is used for a clinical practice or other critical applications.

- If a member encounters problems with the On-Net Internet circuit, they should contact OTN Customer Care at 1-855-654-0888. If the connection is through a Member's own provider, they should call the Internet Service Provider directly.

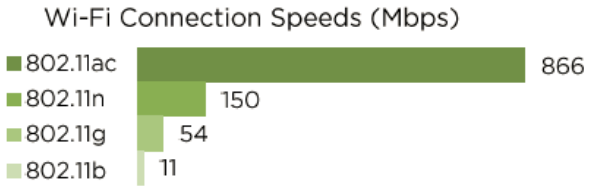
2.1.4 Cellular / Mobility

OTN's telemedicine solutions rely on private and public network carriers and the strength of their signal to successfully support virtual care. A stable network connection and a minimum bandwidth of 0.7-1.0 Mbps upload and download are required for an optimal mobile video call. Depending on the method of connection, here are a few things to keep in mind to ensure the best experience.

Wireless

Connection (801.11b/g/n/ac)

- Connecting to your wireless network using more recent protocols will result in better quality video.



Signal Strength

- A strong Wi-Fi signal will increase the stability of your call.

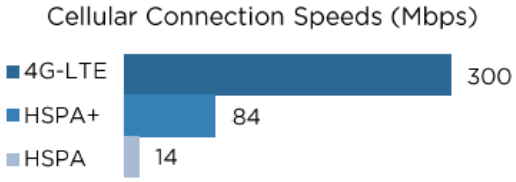
Internet Speed

- The faster your internet connection, the sharper you video and clearer your audio will be.

Cellular

Connection (HSPA, HSPA+, 4G-LTE)

- Using 4G-LTE will provide optimal video and audio quality.



Signal Strength

- A strong cellular signal will increase the stability of your call.

Data Speed

- Connecting over 4G-LTE with a strong signal will provide the necessary bandwidth for high-quality video and audio.
- To check the strength of your internet connection, try a test at *speedsmart.net*, *fast.com*, or *speedtest.net*.

2.1.5 Network Performance Standards

Service	Provider Network	Connection Type	Bandwidth (Up/Down)	Packet Loss	Latency	Jitter
Hardware-based videoconferencing (Standard Definition)	eHealth Ontario, ORION, K-Net, Internet	On-Net, Off-Net, ISDN	800 kbps minimum per system	<.5%	<150 ms	<50 ms
PC-based Videoconferencing	eHealth Ontario, ORION, K-Net, Internet	Off-Net	800 kbps minimum per concurrent session	<.5%	<150 ms	<50 ms
Telestroke (Consultant Site)	Internet	On-Net	800 kbps minimum	<.5%	<150 ms	<50 ms
Telehomecare	PSTN	n/a	n/a	n/a	n/a	n/a
Telehomecare (video enabled)	Internet	Off-Net	800 kbps	<.5%	<150 ms	<50 ms
Webconferencing	eHealth Ontario, ORION, K-Net, Internet	On-Net, Off-Net	128 kbps	<2%	<300 ms	<100 ms

2.1.6 Bring Your Own Circuit (BYOC)

OTN is no longer a primary circuit provider for videoconferencing systems. OTN provides Members with the support and options they need to procure and manage their own connectivity through their existing Internet Service Providers. Members have the following options:

- Using a circuit already in place at their organization.
- Increasing the capacity of an existing circuit if necessary, or
- Securing a dedicated circuit for videoconferencing.

If securing and managing their own circuit is not possible, Members will still have the contingency option of paying OTN a monthly cost-recovery fee to retain an OTN-provided circuit.

2.1.7 Wireless Networks

A growing number of OTN Members are exploring the possibilities of telemedicine over wireless networks within the healthcare site. Wireless technology offers significant advantages in terms of mobility and convenience, for applications such as PC-based videoconferencing, mobile real-time collaboration, or clinical consultations via a mobile telemedicine cart. However, before a Member introduces wireless technology into the telemedicine practice, they should be aware of its inherent risks.

Risks to the privacy and security of personal health information:

Privacy and security risks are inherent in the use of wireless technology in the telemedicine environment. A wireless system is more difficult to secure than an equivalent wired system for the following reasons:

- Wireless signal propagation. In a wired system, a communication signal is confined to the wire on which it is transmitted. To intercept the signal, a receiving device must be attached directly to the wire. In a wireless system, a communication signal is broadcast over an extended spatial area and anyone within that area using an appropriate receiving device can intercept the signal.
- Encryption requirements. To preserve the confidentiality of information transmitted over the wireless medium (which is inherently susceptible to eavesdropping), the information must be encrypted. A secure wireless encryption scheme is difficult to design and implement, leading to the frequent absence of encryption capabilities in real-world wireless systems, as well as numerous weaknesses in systems that do provide these capabilities.
- Interference and jamming. Because wireless signals propagate over an extended spatial area, it is easy for two signals to interfere with each other, causing both to become corrupted. Interference may be caused by other wireless sources in the area, leading to degradation in the performance of a wireless system. Furthermore, a malicious attacker may intentionally generate a strong wireless signal designed to interfere with a wireless system to prevent it from operating.

As a health information custodian, a Member is required under the Personal Health Information

Protection Act (PHIPA) to take reasonable steps to ensure the security and privacy of personal health information. These steps would include ensuring that policies, procedures, and technical safeguards are in place at a Member's organization to protect data transiting wireless networks.

If a Member is planning to use wireless networking technology to access OTN events or services, they should contact their Account Manager for assistance. OTN has developed a Position Paper on Wireless Technology which explains inherent risks in wireless networking and outlines recommended best practices for the use of wireless technology in the healthcare environment. Should a Member decide to move forward with the wireless implementation, they will be asked to sign a Memorandum of Understanding (MOU) attached to their Membership Agreement. The MOU serves to document that a Member is aware of and comply with PHIPA requirements, as set out in the June 2007 order by Ontario's Privacy and Information Commissioner.

2.2 Videoconferencing Equipment

OTN supports a wide range of videoconferencing equipment for clinical telemedicine applications, as well as healthcare education and administration. This equipment includes telemedicine carts for mobile diagnostics and treatment, room-based systems designed to host multi-participant virtual meetings, and desktop systems for personal consultations. OTN also supports a variety of peripherals such as exam cameras, document cameras and ENT scopes, chosen for their functionality, ease-of-use and compatibility with our telemedicine carts. OTN Vendor Management can help to select the right videoconferencing systems and medical peripherals for the site's specific needs. For a full list of supported equipment, see the *List of Standard Equipment*.

Figure 5: Telemedicine Cart

OTN's List of Standard Equipment represents the videoconferencing equipment and peripherals certified by OTN as well as a snapshot of End of Life/End of Service (EOL/EOS) equipment. Since most Members purchase their own equipment, OTN does not interfere in the organization's procurement policies and processes.

OTN's commitment to service quality requires that all endpoints connected to the OTN network be capable of error-free communication with all other endpoints. Videoconferencing products and

software systems supported by OTN are rigorously tested to ensure interoperability with each other and with OTN's core infrastructure, providing a consistent, high-quality user experience. As our Vendors of Record introduce new products, we subject these to the same extensive testing to ensure seamless compatibility with equipment currently in use on the OTN network. Equipment that meets these criteria is certified and added to the List of Standard Equipment.

As equipment manufacturers introduce new products into the telemedicine market, old products are eventually discontinued. The service life of videoconferencing systems is typically eight years. After about five years of production, the manufacturer will declare the system End of Life (EOL).

EOL products are still supported but are no longer developed which means new features and functions are not introduced for these systems. Four or five years after reaching the EOL date, a product will be declared End of Service (EOS). At this point, the manufacturer discontinues any support for the product. The manufacturer will not warrant the product, provide software patches, or bug fixes, guarantee the availability of replacement parts, or accept trouble tickets for EOS systems.

OTN is notified by our Vendors of Record when products are EOL/EOS. OTN communicates these changes to members in an annual inventory statement detailing equipment and EOS dates at each site, with a "best practice" message.

Note: OTN offers limited technical support for approved models of EOS systems on the network. A list of supported and unsupported equipment can be found at the *List of Standard Equipment*.

EOS systems may pose interoperability issues, degrade the quality of service for other Members, or reduce the functionality of our core infrastructure. Since manufacturers do not support EOS systems, we are unable to rectify these problems or to deliver on the commitments of our Service Level Agreement. Should an EOS system be causing repeated issues on the network, be interfering with quality of events for other participants or prevent OTN from completing necessary upgrades, OTN will notify the member and deactivate the system immediately.

Although we make every reasonable effort to work with our Members to find acceptable solutions for EOS replacements, it is the Member's responsibility to work directly with their vendors to be aware of EOS dates and arrange for replacement equipment. OTN reserves the right to exclude from the network any device that does not comply with its standards, as defined by the current List of Standard Equipment.

The List of Standard Equipment specifies not only hardware makes and models, but software revision levels for the operating systems that run on the videoconferencing equipment. Software revisions address known issues and bugs for the equipment and ensure interoperability with other systems. It is very important that all systems on the network are maintained at the correct software revision levels. This is not always the most current release but is the version that OTN has tested and certified.

It is advisable to keep the equipment under the manufacturer's warranty for the OTN Technical Support to install the correct software revisions on the videoconferencing systems. Often this step

is required to address a reported issue. OTN requires administrative rights to the room-based videoconferencing systems to make configuration changes, gather performance metrics and trouble-shoot issues.

Note: Remote access and support from Technical Support is only possible with On-Net systems.

Always check with the OTN Account Manager before purchasing new telemedicine equipment, to ensure the equipment is supported on the OTN network.

2.3 Security Compliance

OTN uses a variety of techniques to safeguard the security of video traffic and patient data traversing the network. The VPN architecture, explained above, uses the encryption capabilities of our Member-site routers to provide secure transport over many different physical networks, including eHealth Ontario's ONE network and the public Internet. In addition, OTN employs end-point encryption to secure data as it traverses Member's local network infrastructure, and to ensure that all sites are secure, even if an OTN router is not deployed. All OTN videoconferencing systems are configured to use Advanced Encryption Standard (AES), a symmetric key algorithm that is an accepted encryption standard in North America.

To ensure that AES is enabled on all active systems across the network, OTN performs active monitoring of endpoints at various times:

- Daily: OTN routinely scans active systems on the network to verify that AES encryption is enabled. This activity is performed off-hours through an automated remote process. Results of the automated scanning are captured in a data log, which records the identification numbers of the systems scanned, model and software revision levels (when available) and the status of AES settings (for example, "ON", "OFF", "AUTO").
- At registration time: The OTN "gatekeeper" is a server that authorizes systems to participate in OTN events. When a system is powered on, it automatically registers with the gatekeeper, which determines its connection speed and other call control characteristics. During this automatic registration process, OTN detects and records AES encryption settings. If AES encryption is disabled, Technical Support is notified for follow up with the Member.
- During System Certification: During certification or maintenance of videoconference systems, OTN Technical Support checks the system's AES encryption settings, and enables AES if required.
- At Event Initiation: A scan of AES settings is performed on each system participating in an event, at call initiation.

If one of the systems is out of compliance with OTN encryption standard, an OTN Technical Support representative will contact the site and help resolving the issue.

2.4 Personal Computers and Software

A growing number of OTN services are delivered on a personal computer platform. These include:

- Ncompass – OTN's web-based scheduling system.
- Personal Computer Videoconferencing.
- Telestroke – emergency stroke diagnosis based on PC download of CT scan imagery.
- eConsult – various clinical applications that allow a specialist to download and review
- diagnostic data from a central server.
- Web conferencing – live meetings, document sharing, and presentations delivered over the OTN network or public Internet.

Depending on the required level of remote technical support, some applications need OTN to directly manage the PC client and the PC to be logged onto the OTN domain. This allows the OTN Technical Support team to troubleshoot the PC and install software upgrades and fixes. It also prevents from inadvertently compromising the application by installing conflicting software or by changing essential configuration settings.

The table below summarizes configuration data for various OTN PC applications.

Application	Admin	O/S	Minimum Specifications	Client Software	Special Requirements
Telestroke	OTN	Windows 7, 8+ and 10	Minimum i3 processor/4GB RAM	Merge eFilm	OTN Domain
Analogue Stethoscope	OTN	Windows 7, 8+and 10	Minimum i3 processor/4GB RAM/Serial – RS232 Port)	AMD SmartSteth	Serial Port (RS-232) OTN Domain
Telesteth (FUTURE)	OTN	Windows 7, 8+ and 10	Minimum i3 processor/4GB RAM	3M Telesteth	USB 2.0+/Bluetooth
Teleophthalmology	OTN	Windows 7, 8+ and 10	Minimum i3 processor/4GB RAM	Merge	OTN Domain
Telederm	User	Windows 2007, 10 OTN does not provide PC)	Minimum i3 processor/4GB RAM	Medweb	OTN Domain

Application	Admin	O/S	Minimum Specifications	Client Software	Special Requirements
Web Streaming	User	Windows 7, 8+ and 10 MAC OSX most current version and previous 2 versions	Minimum i3 processor/4GB RAM	IE9 or later with Silverlight. Firefox 31 or later with Adobe Flash and or Silverlight. Chrome 46+ with Adobe Flash	
Webconferencing	User	Windows 7, 8+ and 10	Minimum i3 processor/4GB RAM	Adobe Connect Active X	
Telestroke	OTN	Windows 7, 8+ and 10	Minimum i3 processor/4GB RAM	Merge eFilm	OTN Domain
Analogue Stethoscope	OTN	Windows 7,8+ and 10	Minimum i3 processor/4GB RAM/Serial – RS232 Port)	AMD SmartSteth	Serial Port (RS-232) OTN Domain
Telesteth (FUTURE)	OTN	Windows 7, 8+ and 10	Minimum i3 processor/4GB RAM	3M Telesteth	USB2.0+/Bluetooth
Teleophthalmology	OTN	Windows 7, 8+ and 10	Minimum i3 processor/4GB RAM	Merge	OTN Domain
Telederm	User	Windows 2007, 10 OTN does not provide PC)	Minimum i3 processor/4GB RAM	Medweb	OTN Domain
Web Streaming	User	Windows 7, 8+and 10 MAC OSX most current version and previous 2 versions	Minimum i3 processor/4GB RAM	IE9 or later with Silverlight. Firefox 31 or later with Adobe Flash and or Silverlight.Chrome 46+ with Adobe Flash	
Webconferencing	User	Windows 7, 8+ and 10	Minimum i3 processor/4GB RAM	Adobe Connect Active X	

Application	Admin	O/S	Minimum Specifications	Client Software	Special Requirements
Personal Computer Video Conferencing	User	Windows 7, 8+and 10 Mac OS, most current version and previous 2 versions	Minimum i3 processor/4GB RAM	Vidyo	Refer to PCVC *Technical Readiness document*
OTN Connect (mobile video conferencing)	User	iOS 8 through iOS 9.3.4	iPhone 5 and later versions. iPad 3rd generation.	OTN Application	

3 Technical Support

Using advanced network and system management tools, OTN monitors continuously the site's network connection and scanning for problems that might affect the service. If a problem is detected at the site, technicians will either correct the problem remotely, or work with the site's technical resources to resolve the issue.

3.1 Technical Support

Figure 6: OTN Customer Care

The OTN Technical Support team is the Member's first point of contact for all technical issues and requests relating to OTN telemedicine services. Staffed by customer support professionals and backed by networking and telemedicine experts, OTN's Technical Support can help diagnose and resolve issues.

Technical Support is fully staffed during regular hours of operation (see section 3.1.1), with OTN Emergency Services on-call coverage after hours. Services provided by the Technical Support Team include:

- On the spot troubleshooting
- User technical support
- Software upgrades
- Remote diagnostics
- Service bulletins and Member communication
- Session monitoring (by request)
- User account management
- Event management – for example, conference extensions, participant add/drops, audio muting
- Media recording
- OTN Technical Support can be reached through a toll-free telephone number, 1-855-654- 0888, or by e-mail (for non-critical requests) at *technical support@otn.ca*.

3.1.1 Hours of Operation

Please check the current *Ontario Health (OTN) contact information* and hours of operation.

3.1.2 Reporting Issues

All technical support requests and problem reports should be directed to the OTN Technical Support Team, by phone or email. The responding technician will log the call in the ticketing system and give the requestor a service ticket number. If a Member calls back regarding the same issue, it is helpful to provide the service ticket number for quick reference.

Whenever a Member contacts OTN Technical Support, they should provide the site and system numbers, contact information, and the reason for the call. If a Member is calling about a specific videoconferencing event, they should also have the event ID available. This enables the Technical Support team to retrieve the event information, and to check the status of participating systems.

If a Member is calling for help with any of OTN's emergency clinical services, including Telestroke, Teletrauma, Telewound, Virtual Critical Care, and RCCR, they should advise the technician answering the call.

Note: Any time OTN is experiencing a prolonged or widespread technical issue, the Technical Support team updates the Emergency Notification, which is a brief recorded message reporting the status of the network. To hear the Emergency Notification, call OTN Customer Care and listen for the message just before the voice menu options are presented.

3.1.3 Equipment Procurement

OTN employs technical experts who can help selecting the appropriate equipment for telemedicine needs. Whether Members are planning to purchase videoconferencing systems, telemedicine carts, medical peripherals, or other telemedicine devices, OTN technical specialists can assist selecting the right equipment to meet the site's needs and to ensure interoperability with other OTN services.

OTN continues to work for its Members in obtaining competitive pricing from vendors who provide videoconferencing equipment and medical peripherals. This will guarantee competitive market pricing from the Vendors of Record on telemedicine equipment purchases and related services. It will save time and expense of issuing an RFP each time a Member needs to acquire or replace equipment. OTN updates the list of VORs (Vendors of Record) every 3 to 5 years to insure OTN Members receive the best costs for equipment and services.

3.1.4 Equipment Installations

In addition to equipment pricing, OTN also negotiates competitive pricing on equipment installation and on extended warranties for selected hardware and software. OTN recommends all Members to purchase installation services from one of the OTN Vendors of Record that provide "OTN Certified" installation of telemedicine equipment.

3.1.5 Remote Support

OTN's Technical Services Delivery group can aid in isolating technical problems a Member have logged with the Customer Care Centre. The team will contact the requestor and use our remote diagnostic tools to investigate the situation to isolate the problem. If the team identifies the problems are caused by hardware, they will clearly identify the problem and the Member will be instructed on the next steps in receiving replacement equipment if the equipment warranty is up to date. If the equipment warranty is expired the Member will get the option on renewing the warranty with one of the OTN VORs and process the RMA (Return Merchandise Authorization) claim after the warranty is reinstated.

OTN strongly suggests Members to purchase appropriate extended warranty services when purchasing new equipment and take the initiative to train our VORs (Vendors of Record) about OTN practices regarding installation and services. If a Member chooses not to purchase extended warranty services when buying new equipment, they can still contact one of the VORs or any other vendor to provide the services after the purchase.

Once the equipment is repaired and services restored, OTN will work with the Member to remotely re-certify the equipment.

3.1.6 Escalation

At OTN we pride ourselves on providing the best customer service possible to Members. Whenever a Member encounters any technical issues with OTN services, they should follow these steps to get them resolved:

STEP 1 Contact the Technical Support team and report the issue, providing as much information as possible (Site Name, Site ID/System ID, Contact Name, Email, Phone No, a detailed explanation of the equipment fault).

STEP 2: If a Member is not satisfied with any aspect of the customer service experience, please email *voiceofcustomer@otn.ca*

STEP 3: The Member will receive a response from one of our Customer Experience Team Managers within 4 hours.

The table below summarizes OTN's service level commitments to our Members. In some cases, specific SLA targets may be modified, added, or deleted as part of a separately negotiated agreement with a Member or group. In these cases, a Memorandum of Understanding is drafted and signed by OTN and the relevant Member(s).

Note: OTN's service is heavily dependent on various 3rd party providers, such as network vendors and equipment manufacturers. OTN cannot guarantee the quality or availability of our services that is beyond OTN's direct control.

SLA Service Item	Worst Case Value	Units	Conditions
Service Quality			
Service Desk on call	7/24/365	days	100% of the time
Service Desk availability	99.9	%	
Service Desk telephone on hold time not to exceed	60	seconds	80% of the time during business hours
Service Desk resolves incident without escalation	80	%	
Communications			
Time to notify Members of Priority 1 Incident is posted within: (see next section for priority definitions)	30	minutes	90% of the time
Availability of videoconference bridge	99.5	%	During Business Hours
Availability of media streaming service	99.5	%	During Business Hours
Availability of Emergency Telemedicine services	99.9	%	At all times
Availability of PCVC service	99.5	%	During Business Hours

Priority Definitions

The tables below define how OTN classifies incidents based on the urgency and impact to establish the incident

Incident Urgency

Incident Urgency	
Category	Description
1. Critical	All Members are immediately affected
2. High	Degradation affects a large percentage and/or multiple number of Members
3. Medium	One site/location with multiple users affected
4. Low	One site/one location affecting a single session or event

Incident Impact

Incident Impact	
Category	Description
1Extensive	The entire service is unavailable or severely degraded leaving it unusable
2. Significant	A component of the service is unavailable
3. Moderate	Degradation of quality and functionality to the service is being accessed
4. Minor	Single-site or user affected

Incident Urgency Priority Matrix

		Impact			
		Extensive	Significant	Moderate	Minor
Urgency	1. Critical	Critical	Critical	High	High
	2. High	Critical	High	High	Medium
	3. Medium	High	Medium	Medium	Medium
	4. Low	Low	Low	Low	Low

4 Member Responsibilities

4.1 Incident Reporting

Members should report all technical issues to the OTN Customer Care Centre. When reporting an issue relevant to a videoconferencing event, it is most helpful if the requestor can provide the event ID. This enables the Technical Support team to quickly retrieve information about the event and the participating sites.

It is especially important to report recurring problems or persistent quality issues to Customer Care. The Technical Support team has the necessary tools for monitoring network traffic and identifying transmission errors that can lead to degraded performance. However, OTN cannot do anything to resolve an issue that has not been reported.

4.2 Equipment Maintenance

4.2.1 Service Life

As an OTN Member ensure any telemedicine equipment connected to the OTN network, or used to receive an OTN telemedicine service, complies with OTN hardware and software standards and requirements as specified in the *List of Standard Equipment*.

It is recommended that sites replace aging equipment as it reaches the manufacturer's EOS date, which indicates that the product is no longer supported by the manufacturer and may have limited OTN technical support. At this point the EOL/EOS systems are moved into a different section of the List of Standard Equipment.

Although systems may function normally after the EOS date, potential issues can arise with their continued use:

- Manufacturers will not respond to service requests or problem reports on EOS systems. The OTN Technical Support team will attempt to help but will be very limited in the service it can offer.
- Replacement parts become scarce or unavailable, so that it may become impossible to repair faulty or damaged EOS systems.
- New peripherals (including monitors, speakers, and medical devices) may not physically connect to older systems.
- Software patches and upgrades are no longer provided by the manufacturer, which means known issues and software bugs cannot be addressed anymore.
- New equipment might not interoperate properly with older systems. Some telemedicine events involving EOS systems may be degraded in quality or fail entirely.
- New features and functions introduced into the OTN network may not work properly or an all with EOS systems, and may cause EOS systems to malfunction.

Members will receive an annual inventory statement detailing the status of all equipment at the site including the EOS status.

Note: OTN reserves the right to remove from the network any system that does not comply with the hardware and/or software requirements as set out in the current List of Standard Equipment. EOS systems will be decommissioned from the network if they cause inter-operability issues.

4.2.2 System Management

The following list of Member's responsibilities applies to any devices (videoconferencing system, PC, peripheral) that connect to or receive OTN services:

- Ensure that the equipment is physically secure when not in use and is accessible only by authorized persons.
- Turn on videoconferencing system ½ hour prior to any scheduled videoconference.
- Provide physical access to OTN and vendor technicians when required.
- Ensure OTN-connected telemedicine systems are maintained at the correct software revision as specified in the *List of Standard Equipment*.
- Refrain from making any changes to the configuration of videoconferencing systems, personal computers, routers, or other devices used to deliver OTN telemedicine services.
- Check with the OTN Account Manager before purchasing equipment to connect to OTN network.
- Inform OTN of any lost, stolen, or damaged equipment as soon as possible.

4.2.3 Networking

OTN relies on Member's local IT resources to provide network connectivity from the OTN demarcation point (usually an OTN router located in the site's switch room or wiring closet) and the endpoint of the LAN. Specifically, OTN needs a site's IT department to:

- Designate a local on-site technical resource capable to help with basic on-site system and network troubleshooting (e.g., primary system configuration, cable issues, modem/router, etc.).
- Maintain local wiring infrastructure or wireless networks used to connect to OTN in good working order.
- Maintain an appropriate environment for telecommunications equipment.
- Secure connectivity via VLAN or physical isolation of video LAN network.
- Ensure that security of LAN or wireless LAN is tested through vulnerability assessments and intrusion detection.
- Advise OTN of any changes that may potentially affect or impact telemedicine services, security or reliability (such as physical changes to wiring, potential environmental disturbances, renovations, moves, etc.).
- Ensure that switching gear can support video/real-time traffic (no network hubs), also switch settings are configured for video/real-time traffic (Full Duplex/Half Duplex).

4.2.4 Warranty Coverage

The main and most expensive components of a site's videoconferencing-based telemedicine system are the codec with the camera and the medical peripherals. Through warranty the equipment is protected against failure and the functionality and performance is kept at par through regular updates. Continuing interoperability with other telemedicine devices and centralized services (such as video bridges) and serve to stave-off technological obsolescence and the need for early replacement of the equipment. It is extremely important that a Member maintains the equipment under manufacturer's warranty to ensure problem-free use for these systems. Warranty coverage enables OTN to address software updates or bugs, interoperability issues and component failures. Without this coverage, OTN Technical Support can do very little to help in case of faulty equipment.

Note: As an OTN Member, it is strongly suggested that you maintain videoconferencing systems, medical peripherals and/or PC-based videoconferencing software under a full manufacturer's warranty (hardware and software). Failure to maintain warranty coverage may result in interrupted service.

It is the sole responsibility of the Member to track the warranty end dates of their equipment through their vendor and buy new warranty for their systems once the warranty expires.
Please note, warranty does not cover any damage to the equipment caused by misuse, negligence, of theft after the point of acceptance at delivery.
Any questions about the warranty coverage, the Member should contact the reseller of the equipment or warranty.

4.3 Acceptable Use

Telemedicine equipment, medical peripherals and PC systems at Member sites usually belong to the Member and are out of OTN's direct control. While OTN cannot dictate how Members may use their own equipment, we must require adherence to certain rules of acceptable use. Only this way OTN can provide a reliable and sustainable service to all our Members.

The following regulations apply to the use of telemedicine equipment which is used to connect to OTN or to receive OTN services:

- The Members should not modify the OTN standard configuration settings of videoconferencing systems, medical peripherals, telemedicine PCs or network equipment.
- The Members should not bypass or attempt to bypass security measures configured on equipment or on the OTN owned routers or switches located at the site.
- Own bridging hardware should not attach to the OTN router or switch located at the site.
- The Members should not attach any recording device or recording software to the OTN-connected videoconferencing system or use a PC-based videoconferencing software to record sessions.

- The Members should not attempt to use OTN-services for any function or application other than those specifically supported by OTN, as listed in Section 1 above.

If Members have any questions or concerns about appropriate use of their telemedicine equipment, they should contact the Customer Care Centre or their Account Manager.

Failure to adhere to these regulations may result in suspension of a Member's OTN membership.

5 Appendix A: List of Standard Equipment

The *List of Standard Equipment* is located here:
https://support.otn.ca/sites/default/files/6_appendix_a_-_list_of_standard_equipment.pdf