OTN Services and Safeguards

eVisit

Description of Services

OTN brings virtual care innovation to the healthcare system so that the people of Ontario can get the care they need when and where they need it most: at home, in their community or in hospital. For more than a decade, OTN has increased access to health care and education across the province with one of the world's most extensive telemedicine networks. Working with its many partners and leveraging its unique knowledge of health care and digital technology, OTN addresses challenges by introducing and spreading new ways of delivering care that benefit patients, care providers and the healthcare system. An independent, not-for-profit organization, OTN is funded by the Government of Ontario.

OTN is committed to protecting personal health information consistent with the requirements of the '*Personal Health Information Protection Act,* 2004' (PHIPA) and Ontario Regulation 329/04. "Personal Health Information" is any information that can identify an individual and that relates to the health care services they received. This includes (but is not limited to) name, address, telephone number, health card number, health care provider's name, the reason one was referred for a telemedicine appointment and any examination results.

OTN and members who self-schedule, use personal health information to arrange and enable a videoconference appointment. This may require OTN and members to provide personal health information to hospitals and/or health care providers involved in the appointment and to inform patients about those arrangements. Just like a face-to-face appointment, when using OTNs eVisit program, permission is granted to authorize a health care professional to submit a claim through Ontario Health Insurance Plan (OHIP). OHIP uses this information for payment and for auditing purposes. To learn more about OHIP, please visit www.health.gov.on.ca.

How The Technology Works

OTN's eVisit program enables the use of videoconferencing for initial and/or follow-up patient consultations from the convenience of a personal computer, laptop or OTNconnect App on iOS or Android device. eVisit supports clinical, non-clinical and education events using OTN's scheduling tool; Telemedicine Service Manager (TSM)/Ncompass. eVisit enables the Healthcare professional to see patients, case-conference, participate in distance learning, and attend meetings in Ontario.

After Physicians have been granted access to eVisit, they can use videoconferencing in the three following convenient ways:

1. On a mac or PC:
    - Using a personal computer (PC or Mac) which provides a similar, lower-cost, and mobile alternative to traditional room-based videoconferencing. You can eliminate the barriers of time and distance, by videoconferencing with peers or patients from a PC or Mac, connected to OTN's private and secure network.

2. OTNconnect App on iOS or Android device:
    - Healthcare professionals using OTNconnect can make and receive private and secure videoconference calls from their iPhone, iPad, or iPod touch to anyone on the OTN network.

3. Room-based video systems located in healthcare organizations across the province:
    - With OTNhub membership, Healthcare professionals have access to over 3020 room-based video systems in hospitals, clinics and other allied health organizations to help connect Ontario to care. This eliminates the barriers of time and distance, by offering a whole new level of convenience, efficiency and independence by videoconferencing with peers or patients connected to OTN's private and secure network.

eVisit's Directory feature allows Healthcare professionals to locate telemedicine sites around the province, either by individual or institution. Once identified, the pertinent person or organization can be added to a Favourites list.

The Calendar feature displays by day all Healthcare professional pre-scheduled telemedicine events. Date to review future appointments can be changed and the option to print the daily schedule is also made available.

eVisit Benefits

Conducting an eVisit offers convenience, efficiency, and mobility; for healthcare, education, for access to patients and a wide network of healthcare professionals.

- Increase the reach of Healthcare professional specialized services;
- Eliminate costly and time consuming long-distance travel for patients;
- Reduce Healthcare professional down-time and lost productivity due to travelling for education and/or meetings; and
- Patient care provided through OTN is billable through OHIP, at a premium.

How does eVisit work via OTNinvite

OTNinvite is a functionality of eVisit and works using an email address, the internet, a webcam and a computer or tablet with a speaker and microphone. Patients can connect with Healthcare professionals at their convenience, in their home, thus avoiding costly travel and time.

To ensure sufficient and high quality videoconferencing, patient's need to meet the following minimum technical requirements: Click here for Technical Requirement document.

- Computer - Windows 7/8 or Mac OS X and at least 1 GB RAM.
- Firewall - Ensure you have the correct firewall ports open for high-quality videoconferencing.
- Bandwidth Business-grade Minimum 768 Kbps – 1 Mbps per call.
- Camera should support "high definition" (HD) video quality.
- Speakerphone with "echo cancellation" or a headset is mandatory.
- Patients will need to download Vidyo to connect via eVisit OTNinvite. Healthcare professionals may need an IT person to install Vidyo depending on IT Department's policies. One can download the Vidyo application after getting access to eVisit.

The person arranging the video visit may do two things:

1. Give the patient a Personal Identification Number (PIN). This may be optional.
2. Send an email invitation (which contains a link).

After the patient receives the email invitation and at the scheduled date and time, open the email and click the link. The patient will be asked to enter the PIN they may have been given, their name and then click a join button.

A video window opens on the computer and the personal, private appointment begins.

Privacy and Security

OTN follows industry best practices (e.g. ISO security standards) and legislative requirements (e.g. 'the Personal Health Information Protection Act, 2004' and Ontario Regulation 329/04; "PHIPA"). The Privacy and Risk, and Networking, Videoconferencing and Security Operations Teams play an active role in building and managing privacy and security within OTN products and services. The only OTN employees who are granted access to personal and personal health information are those with a business 'Need-to-know' and whose work duties reasonably require such information.

OTN has a comprehensive privacy program in place that addresses the privacy rights of patients in accordance with PHIPA. As a Health Information Network Provider (HINP), Service Provider and Agent under PHIPA and its regulation, OTN provides comprehensive, privacy mature services to its members and Telemedicine users, who are health information custodians (HICs) as well as non-custodians, to enable them to exercise their privacy responsibilities and obligations under PHIPA and other privacy legislation.

Privacy Governance at OTN

OTN has established a comprehensive privacy governance structure and has full time dedicated privacy employees to address privacy and information management requirements and issues.

Description of Safeguards

OTN monitors, reviews and updates its practices to ensure the privacy and security of confidential information (Including personal health information and personal information), processed on its systems and transmitted over its network are safe and secure. OTN uses a variety of physical, administrative, and technological safeguards to protect confidential information from unauthorized access, use, copying, modification or disclosure including contractual agreements with all of its Members.

OTN's eVisit program safeguards include, but are not limited to:

Administrative Safeguards

- Privacy and Security policies and procedures are governed under the OTN Policy Office as set out in frameworks. Staff are trained on policy in accordance with PHIPA, Ontario Regulation 329/04 and any other applicable law and regulation.
- Privacy Impact Assessments (PIAs) are conducted in accordance with OTN's PIA Policy.
- Employees sign an Employment Agreement; as well as an annual Confidentiality Agreement, in addition to having to comply with various OTN HR/Privacy/Security Policies outlining User Responsibilities.
- OTN Staff are required to complete mandatory privacy and security training courses upon hire.
- OTN employs role-based access controls.
- Roles & Responsibilities of Members and Participating Organizations are provided in OTNhub Terms of Serivce and User Agreement; which also addresses use of antivirus software on non-OTN eVisit endpoint clients.
- eVisit production servers are hosted in highly secure data centres. Access to and removal of the equipment is subjected to strictly defined procedures and approvals from the management.
- OTN leverages a Project Gating Methodology to support the development and lifecycle of all eVisit initiatives, as well as any related hardware and software procurement activities. OTN has established Project Gating and Change Management processes and any upgrades to eVisit must be done in accordance with these procedures.

- All access to all eVisit systems and its components requires a unique username or a OneID Identifier and password.
- eVisit Users go through a formal registration process that includes identity verification via eHealth's OneID.
- All eVisit accounts are set to lock within 90 days of registration if not being used and then, after initial login, after 1 year of account inactivity.
- eVisit user accounts get locked out for 15 minutes after 10 incorrect login attempts, and after 30 minutes of inactivity.
- eVisit's front end (sso.otn.ca) enforces strong password policy, requiring at least 8 characters. Complexity requirements are enforced requiring at least one number and one special character in addition to alphabetic characters.
- Locking meeting rooms before staring the conference and after confirming all invitees have joined, prevents unauthorized access to PI and PHI in transit.

Physical Safeguards

- Production Servers are located in highly secure Cogeco managed Data Centres with strict physical access controls, including but not limited to, mantraps, cameras, security guards and where access is granted on a list of pre-approved OTN Staff Members.
- Access to OTN Offices includes; access cards, security guards, cameras, etc.
- Through its Agreements with Cogeco OTN's rented Data Centre space provides temperature and humidity control, fire suppression controls, power conditioning equipment, uninterruptible power supplies, as well as on-site assistance and incident management.

Technical Safeguards

- Releases are tested for interoperability with videoconferencing infrastructure, before being implemented into production environment.
- OTN Laptops used to administer eVisit have encryption enabled.
- OTN provided laptops and desktops that are used to manage eVisit components have Symantec Endpoint Protection installed.
- eVisit servers are located in segregated VLANs separated by Firewalls which further prevent the spread of malware.
- Encrypting PHI, PI or other SI During Transmission:
    - Codec-based video streams are encrypted using AES based encryption.
    - Web based communication (including authentication and video streams over HTTP) use TLS encryption.
    - With secure Videoconferencing system option enabled, the VidyoPortal automatically establishes an encrypted HTTPS channel with the each Vidyo endpoint that attempts to access the system and performs certificate exchange, issued by Third Party certifying authority.
    - HTTPS based communication relies on TLS protocol based handshaking methods and network based packet acknowledgement receipts.
    - All internet connections to EVISIT are secured by Transport Layer Security (TLS) encryption. Older, insecure encryption protocols (SSLv1,

SSLv2, SSLv3) are not supported.Insecure SSL ciphers have been disabled on OTN's SSL offloading server (F5 Load Balancer).
    - Sensitive information such as user names and passwords are transmitted between the Vidyo clients or VidyoRoom and the VidyoPortal by establishing signalling links. These signalling links are secured using TLS encryption.
- eVisit leverages network/transport layer protocols to ensure the integrity of information.
- Password data stored on all systems is encrypted in a one way, salted hash format.
- OTN implements network segregation via use of VLANs, Firewalls, and Access Controls.
- eVisit Users are authenticated via a Single-Sign-On solution before being granted access.
- During authentication process, the user is required to input username and password which are confirmed for validity by the Identity Provider and Authenticaion Services.
- OTN has adopted a High Availability approach to mitigate the impact of eVisit outage.
- eVisit leveraged components (Middle-Tier, Backend, and Database servers), as well as the supporting network and video infrastructure have High Availability/Redundancy in place.
- eVisit and leveraged components are backed up nightly. allowing systems to be restored to their previous state.
- CDR logs record and maintain information about which users participated in videoconferencing sessions.
- VidyoPortal, VidyoManager, VidyoRouter and VidyoGateway log all administrative actions performed including: Login Successful/Unsuccessful, Logoff, Add/Delete/Modify.

Safeguards Specific to OTNinvite

- Emails generated do not contain any identifiable information (Such as the Physician's or the Clinic's name or email), which may be considered PHI in the context of a clinical event.
- Users are asked to confirm the name and the email address when generating invites to ensure that the email is sent to the correct recipient.
- PIN information is never included in the email notification for clinical events. (This means that an intercepted email will not include enough information for a Third Party to join an event protected by a PIN.) The eVisit organizer can provide the PIN to an invitee during their initial consultation or over the phone.

Where can I get more information about OTN's Privacy Practices?

Please contact the OTN Privacy Office should you have any questions:

Ontario Telemedicine Network
Privacy Office
438 University Avenue, Suite 200, Toronto, ON M5G 2K8
Email: privacy@otn.ca | Tel: 416-446-4110 / 1-855-654-0888 / TTY: 1-855-368-6889