Ontario Health (OTN Business Unit) Services and Safeguards

Video Visit

Description of Services

Ontario Health (OTN Business Unit) (OH) brings virtual care innovation to the health care 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, OH has increased access to health care and education across the province with one of the world's most extensive virtual care networks. Working with its many partners and leveraging its unique knowledge of health care and digital technology, OH addresses challenges by introducing and spreading new ways of delivering care that benefit patients, care providers and the health care system.

OH is committed to protecting personal health information (PHI) consistent with the requirements of the '*Personal Health Information Protection Act,* 2004' (PHIPA) and Ontario Regulation 329/04. PHI is any information that can identify an individual and that relates to the health care services they receive. 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 virtual care appointment and any examination results.

OH and members who self-schedule, use PHI to arrange and enable virtual care appointments. This may require OH and members to provide PHI to hospitals and/or health care providers involved in the appointments and to inform patients about those arrangements. Just like a face-to-face appointment, when using Video Visits, 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

OH's Video Visit program enables the use of videoconferencing for initial and/or follow-up patient consultations from the convenience of a personal computer, laptop or the OTNconnect App on an iOS or Android device. Video Visits support clinical, non-clinical and education events using OH's scheduling tool Telemedicine Service Manager (TSM)/Ncompass and applications available directly on the OTNhub. Video Visits enable the health care professionals to see patients, case-conference, participate in distance learning, and attend meetings in Ontario.

After health care providers have been granted access to Video Visits through the OTNhub, they can use videoconferencing in the three following convenient ways:

1. Direct to Patient Video Visits on a mac or PC:

- Using a personal computer (PC or Mac) connected to OH's private and secure network. This provides a similar, lower-cost, and mobile alternative to traditional room-based videoconferencing.

2. Direct to Patient Video Visits using the OTNconnect App on an iOS or Android device:
   - Healthcare professionals using OTNconnect can make and receive private and secure videoconference calls from their iPhone, iPad, or Android device to anyone on the OH network.

3. Hosted Video Visits using room-based video systems located in healthcare organizations across the province:
   - With OTNhub membership, health care professionals have access to video systems in hospitals, clinics and other allied health organizations to provide Video Visits to Ontario patients.

The OTNhub Directory feature allows health care professionals to locate individuals and institutions offering Video Visits in Ontario.

Video Visit Benefits

Video Visits offers convenience and efficiency for both patients and healthcare providers. Benefits include:

- Increasing the reach of health care providers offering specialized services
- Eliminating costly and time consuming long-distance travel for patients
- Reducing health care provider down-time and lost productivity due to travel for education and/or meetings

How do Direct to Patient Video Visits Work?

Direct to Patient Video Vists work by sending an email invitation to patients and by using the internet, a webcam, a computer or tablet with a speaker and microphone, and by downloading the Pexip app. Patients join their Video Visit by clicking the link in their email invitation on the scheduled date and time. Health care providers may also opt to use a PIN to further secure the Video Visit. The PIN is then provided to the patient separately (e.g., by phone) and the patient will be prompted to enter the PIN to join the Video Visit.

Privacy and Security

OH follows industry best practices (e.g. ISO security standards) and legislative requirements (e.g. PHIPA). The Privacy and Information Security teams play an active role in building and managing privacy and security within OH products and services. Only those OH employees with a business "need to know" and whose work duties reasonably require it are are granted access to personal and personal health information.

OH 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, OH provides comprehensive services to its members and users, including health information custodians (HICs) and non-custodians, to support them in meeting their obligations and responsibilities under PHIPA and other applicable privacy legislation.

Privacy Governance at OH

OH 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

OH monitors, reviews and updates its practices to ensure the privacy and security of confidential information (Including PHI and personal information) processed on its systems and transmitted over its network. OH 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.

OH's Video Visit program safeguards include, but are not limited to:

Administrative Safeguards

- OH has implemented a comprehensive suite of privacy, security and human resources policies and procedures which outline employee responsibilities.
- Staff are trained on privacy and security policies as well as applicable legislation, including PHIPA and Ontario Regulation 329/04. New hires complete mandatory privacy and security training within four weeks of their start date and all staff complete a privacy refresher training annually.
- Privacy Impact Assessments (PIAs) are conducted in accordance with OTN's PIA policy.
- Employees sign a Confidentiality Agreement. Employees also refresh their acceptance of the Confidentiality Agreement each year via click-through.
- OH employs role-based access controls.
- Roles, responsibilities and obligations for members and users are documented in the OTNhub Terms of Serivce for Member Organizations and the OTNhub User Agreement. These agreements also address use of antivirus software on non-OH Video Visit endpoint clients.
- OH leverages a project gating methodology and change management processes to support any upgrades and the development and lifecycle of all Vido Visit initiatives.
- All access to Video Visit systems and their components requires a unique username or a OneID identifier and password.
- OTNhub users go through a formal registration process that includes identity verification via eHealth's OneID. OH may also issue credentials after a validation process for users in certain circumstances.

Physical Safeguards

- On-premise production servers are located in highly secure Cogeco managed data centres with strict physical access controls, including but not limited to, mantraps, cameras, and security guards. Access is granted only to pre-approved OTN staff members.
- Cloud-based servers are located in the Amazon Web Services (AWS) Canadian data centres that have a comprehensive suite of security controls and certifications in place.
- Access to OH offices requires an access card.
- Through its agreements with Cogeco, OH'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 release into the production environment.
- OH laptops used to administer Video Visit have encryption enabled.
- OH-provided laptops and desktops that are used to manage Video Visit components have Symantec Endpoint Protection installed.
- Video Visit servers are hosted in the AWS Cloud and are protected using Amazon's extensive suite of security protocols and technologies.
- PHI, personal information and other sensitive information are encrypted during transmission as follows:
    - Codec-based video streams are encrypted using Advanced Encryption Standard (AES)-based encryption.
    - Web-based communications (including authentication and video streams over HTTP) use Transport Layer Security (TLS) encryption.
    - HTTPS-based communication relies on TLS protocol-based handshaking methods and network based packet acknowledgement receipts.
    - All internet connections to OH-hosted services are secured by TLS encryption. Older, insecure encryption protocols (secure sockets layer (SSL)v1, SSLv2, SSLv3) are not supported. Insecure SSL ciphers have been disabled on OH's SSL offloading server (F5 Load Balancer).
- Password data stored on all systems is encrypted in a one way, salted hash format.
- OH implements network segregation via use of VLANs, firewalls, and access controls.
- Video Visit users are authenticated via a single sign-on (SSO) solution before access is granted.
- During the authentication process, the user is required to input their login credentials which are validated by the Identity Provider and Authentication Management service.
- OH has adopted a high availability approach to mitigate the potential impact of outages.

- Video Visit-leveraged components (middle-tier, back end, and database servers), as well as the supporting network and video infrastructure have high vailability/redundancy in place.
- Visit Visit and leveraged components are backed up nightly, allowing systems to be restored to their previous state if needed.
- Call Detail Record (CDR) logs record and maintain information about which users participated in Video Visits.
- Pexip logs all administrative actions performed including:
    - Login successful/unsuccessful
    - Logoff
    - Add/delete/modify
- OTNhub accounts are configured to expire after a pre-defined period of account inactivity.
- OTNhub user accounts are temporarily locked when a threshold of unsuccessful attempts is reached.
- The OTNhub's front end (sso.otn.ca) enforces a strong password policy requiring at least 8 characters. Complexity requirements include at least one number and one special character in addition to alphabetic characters.

Safeguards Specific to Direct to Patient Video Visit

- Emails generated do not contain any identifiable information (e.g., physician or clinic name and contact information) which may be considered PHI in the context of a clinical event.
- Users are asked to confirm the name and the email address of participants 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 so that, in the event of an intercepted email, the invitation alone will not include enough information for a third party to join an event protected by a PIN. The Video Visit host may provide the PIN to an invitee during their initial consultation or over the phone.
- The Video Visit appointment links included in email invitations are single use and are set to expire automatically after a set time period.

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

Please contact the Privacy Office should you have any questions:

Ontario Health (OTN Business Unit) 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