# Virtual Visits Solution Requirements

Version 1.0

March 2020

Ontario

## Table of Contents

## i. Acknowledgements

The requirements listed in this document are informed by several provincial initiatives, including the *eVisit Primary Care* and *Partner Video* pilots, and have been reviewed by a number of health care organizations and clinician leaders.

OTN would like to thank the following individuals and organizations for their extensive contributions to this document.

Dr. David Kaplan, Ontario Health Quality
Dr. Duncan Rozario, Oakville Virtual Care Program
Dr. Kevin Samson, East Wellington Family Health Team
Dr. Marco Lo, Magenta Health
Dr. Danielle Martin, Women's College Hospital
Andriana Lukich, St. Joseph's Healthcare Hamilton
Brendan Kwolek, Halton Healthcare
Eva Serhal, Centre for Addiction and Mental Health
Jonathan Tunstead, Centre for Addiction and Mental Health
Denise Canso, Centre for Addiction and Mental Health
Keith Chung, Magenta Health
Philippe Marleau, Montfort Hospital

Association of Family Health Teams of Ontario
eHealth Centre of Excellence
Ontario Health
OntarioMD
Ontario Medical Association
Sunnybrook Hospital

# 1. Introduction

This document describes general functional and non-functional requirements for digital solutions used by health care organizations and clinicians to support virtual clinical encounters ("virtual visits") with patients.

This document addresses two types of virtual visit solutions:

- Videoconferencing
- Secure Messaging

This document provides guidance on the minimum technical requirements that virtual visit solutions should demonstrate. This technical guidance may be used to develop an expanded set of solutions that can be used as part of the Ontario Virtual Care Program. Please see the Ontario Virtual Care Program billing manual and recent INFOBulletins for up-to-date information about virtual care services which are eligible for reimbursement and any associated requirements.

The requirements in this document apply to virtual visits solutions that are available in Points of Service systems (PoS) such as certified Electronic Medical Records (EMR) or Hospital Information Systems (HIS), as well as stand-alone third-party solutions intended to interoperate with PoS systems.

This document has also been prepared to provide guidance to health care organizations, including Ontario Health Teams, who are interested in procuring a virtual visit solution other than OTN video solutions.[1]

This document references several external sources, including the Ministry of Health's *Digital Health Policy Guidance Document*[2] and the College of Physician and Surgeons of Ontario's published policies on telemedicine[3] and medical record-keeping[4] .

A companion document - *Adopting and Integrating Virtual Visits into Care: Draft Clinical Guidance* – is also available which provides additional guidance to health care providers.

## 1.1 Definitions

The purpose of this section is to provide a standard definition of virtual visits and related concepts.

***Virtual Visits***

For purposes of this standard, a virtual visit is defined as a digital interaction where one or more clinicians, including physicians, nurses or allied health, provide health care services to a patient or their caregiver.

Several virtual visit pilots across Ontario have demonstrated how virtual visits can improve clinical outcomes and improve patient satisfaction and convenience[5].

A virtual visit can be supported using one or more modalities, including videoconferencing and secure messaging, and may involve one or more digital transactions.

---

1 The Provincial Digital Health Services Catalogue is published within the Ministry of Health's Digital Health Playbook. Please see: http://health.gov.on.ca/en/pro/programs/connectedcare/oht/docs/dig_health_playbook_en.pdf

2 Please see: http://health.gov.on.ca/en/pro/programs/connectedcare/oht/docs/dig_health_playbook_en.pdf (August 2019)

3 https://www.cpso.on.ca/Physicians/Policies-Guidance/Policies/Telemedicine

4 https://www.cpso.on.ca/Physicians/Policies-Guidance/Policies/Medical-Records

5 The Home Video Visit pilot (ended November 2019) evaluated direct-to-patient video visits. The eVisit Primary Care pilot (also known as Enhanced Access to Primary Care) evaluated patient-initiated virtual visits by videoconferencing, secure messaging or audio calls in primary care. eVisit Primary Care pilot evaluation results are available on OTN's website.

This is demonstrated in the following three use cases:

1) A specialist performs a post-surgical follow-up assessment of a patient during a video visit previously scheduled by phone. The specialist asks the patient questions about their recovery and visually inspects the surgical site for signs of infection. The specialist documents the visit in a Hospital Information System and a claim is generated for the visit.

2) A patient logs into an EMR-integrated patient portal and sends a secure message concerning a new rash to their primary care physician and includes an attached image of the affected area. The primary care physician reviews the message and image and provides advice in a written response. The following day, the patient sends a follow-up question, which the physician answers before closing the visit. The full secure messaging thread and image attachment are automatically saved in the patient's medical record. The physician marks the visit as "billable," which initiates a claim for the visit.

3) A patient uses an online booking solution to schedule a routine video visit with a Registered Nurse as part of a remote monitoring program for Chronic Obstructive Pulmonary Disorder (COPD). During the video visit, the nurse reviews a summary of the biometric data recorded over the previous 30 days and has a discussion about COPD management strategies with the patient. Using a secure file transfer service, the nurse sends a COPD brochure to the patient. When the visit ends, the nurse documents the visit.

***What is not a virtual visit?***

- Use of an online appointment scheduling or patient documentation solution
- Manual or digital reviews or triage of patient requests
- Posting lab rest results and other patient records on a patient portal
- Responses to administrative questions or clinical requests that require an in-person assessment
- Missed, cancelled or abandoned video visits before health care services are provided
- Digital interactions between two clinicians concerning a mutual patient[6]
- Collection of biometric data by a remote monitoring device

***Virtual Visit Solutions***

A virtual visit solution refers to one or more digital tools that support virtual visit services.

Some PoS systems, such as certified Electronic Medical Records or Hospital Information Systems support virtual visit services through embedded videoconferencing or messaging solutions that rely on the Point of Service system's scheduling, patient portal or application, clinical documentation and claims processing capabilities.

Other stand-alone virtual visit solutions are intended to interoperate with Point of Service systems. These solutions may have their own independent scheduling, patient applications, documentation and claims processing services.

In Ontario, the benefits of interoperable solutions have been well-established in provincial digital and virtual care initiatives[7]. To support the efficient delivery of high-quality care, this document outlines minimum interoperability requirements with PoS systems.

6 This includes eReferrals, eConsults and case conferencing encounters. However, case conferencing encounters can be supported by videoconferencing solutions that meet the requirements outlined in this document.

7 For example, the eVisit Primary Care pilot evaluation found secure, EMR-integrated platform with an asynchronous messaging feature is critical for success in uptake and spread of virtual care.

While this document is limited to virtual visit solutions, health care organizations and clinicians are encouraged to consider solutions that can support clinical services beyond virtual visits. For example, a secure messaging service can support both virtual visits (patient encounters) and provider-provider collaboration.

## 1.2 Key Audiences

Key audiences for this document include:

- Ontario Health Teams
- Health care organizations
- Physicians
- Videoconferencing and secure messaging solution providers
- Point of Service application providers (i.e. EMRs, HIS vendors)

## 1.3 Scope

This document outlines requirements for digital solutions that support virtual visit services, through videoconferencing, secure messaging or a combination of modalities.

It is applicable to virtual visit solutions that support virtual visit services delivered by primary care, specialist, hospital and community service providers.

The document is divided into different sections:

- Section 2 outlines general requirements that apply to *all* virtual visit solutions
- Section 3 outlines requirements *specific* to videoconferencing solutions
- Section 4 outlines requirements *specific* to secure messaging solutions
- Section 5 outlines data requirements for *all* virtual visit solutions

Requirements may refer to one of the following users:

- Patient / caregiver users
- Clinical users (e.g. physicians, nurses, allied health professionals)
- Organizational users (e.g. Administrative staff)

All requirements are either mandatory “M” or recommended “R”.

***Out of Scope***

This document does not address the use of videoconferencing or secure messaging solutions for any of the following activities:

- Administrative activities
- Educational services
- Provider to provider communication
- Provincial eServices (eConsult or eReferral)

This document does not define requirements for telephone (audio-only) visits. However, virtual visit solutions offering voice over IP (VoIP) audio visits should comply with Section 2.0 (general virtual visit requirements).

## 2.0 GENERAL VIRTUAL VISIT REQUIREMENTS

This section outlines general solution, privacy and security requirements that apply to all virtual visit solutions.

When selecting a virtual visit solution, health care organizations and clinicians should consider several factors, including clinical suitability, workflow, patient preferences, as well as relevant professional standards.

Key professional requirements[8] that should be considered when selecting a virtual visit solution include the ability for clinicians to:

- Identify patients accurately
- Manage a patient's informed consent to receive care virtually[9]
- Ensure patient information obtained virtually is sufficiently reliable and high quality
- Protect patient privacy and confidentiality
- Document virtual visit information in a medical, hospital or clinical record
- Ensure virtual visit information is readily accessible for quality assessments, investigations and billing reviews

Health care organizations and clinicians should consider patient needs when selecting a solution. Key considerations include educating patients about the service and solution they are using, enabling caregivers and other care team members to support or join the visit, and ensuring technical support services are available and easily accessible in the event a visit is interrupted.

An important part of the province's vision for virtual care is the meaningful integration of stand-alone solutions into providers' existing Point of Service systems. The minimum interoperability requirements below align with initiatives underway to improve Ontario's digital health infrastructure[10]. Virtual visit solutions that demonstrate more mature levels of integration with Point of Service systems offer significant provider workflow benefits and support high-quality delivery of virtual care.

Health care organizations and clinicians should also consider whether solutions can support an appropriate level of patient and provider identity verification. Over time, approved solutions are expected to integrate with any future provincial identity services, such as a patient digital identity authentication and authorization (IAA) service.

8 See, for example, the CPSO's Telemedicine Policy. https://www.cpso.on.ca/Physicians/Policies-Guidance/Policies/Telemedicine (November 2019)

9 For example, the Canadian Medical Protective Association's has advised physicians to document a patient's informed consent for using videoconferencing to discuss sensitive patient health information. See: "Videoconferencing Consultations: When is it the right choice?" (October 2015). https://www.cmpa-acpm.ca/en/advice-publications/browse-articles/2015/videoconferencing-consultation-when-is-it-the-right-choice

10 Please see the Ministry of Health's Digital Health Information Exchange Policy (August 2019) for more information

## 2.1 General Solution Requirements

*Priorities: (M)andatory; (R)eccomended*

| # | Requirement | Priority | Notes |
|---|---|---|---|
| 2.1.1 | Will provide patients and their caregivers with secure access to virtual visit services | M | Solutions must enable patients and their caregivers to access one or more virtual visit services.<br><br>Patients must be registered users of a virtual visit service.<br><br>Solutions should enable other clinical users to participate in virtual visits.<br><br>Please see 3.2.8, 3.2.9 and 4.2.3 for related requirements specific to video and secure messaging. |
| 2.1.2 | Will record virtual visit information for clinical documentation purposes | M | Solutions must record any information that is relevant for clinical documentation purposes.<br><br>At a minimum, solutions will record:<br><br>• Encounter summary (e.g. event ID, start and end date and time);<br>• Any messages, files or images that were exchanged during the patient encounter; and<br>• Any clinical documentation or notes.<br><br>Solutions must record sufficient information to associate the virtual visit information with a specific patient record. |
| 2.1.3 | Will transfer virtual visit information to a medical or hospital record[11] . | M | Virtual visit information (as defined in 2.1.2) must be transferable as searchable files to a medical or hospital record for clinical documentation and audit purposes. |
| 2.1.4 | Will make technical support services available to clinical users | M | Vendors offering virtual visit services must provide reasonable technical support to organizations.<br><br>Organizations offering virtual visit services must ensure reasonable technical support services are available to patients.<br><br>Contact information for technical support should be easily accessible by patients. |
| 2.1.5 | Will be able to extract data for reporting purposes | M | Solutions must make virtual visit data available to support organizational reporting.<br>See Section 5 for minimum data elements. |

11 This requirement is not applicable to videoconferencing solutions where no machine-readable patient data is exchanged between systems.

| | | | |
|---|---|---|---|
| 2.1.6 | Will manage patient agreements for virtual visit services | R | Solutions should allow clinical users to send and receive patient agreements and other educational materials relating to virtual visit services. |
| 2.1.7 | Will provide seamless integration with Point of Service systems | R | Stand-alone solutions should demonstrate seamless integration, which should include elements such as:<br>• Single sign-on with PoS login credentials<br>• Receiving patient context (identification) information from PoS systems<br>• Automatically sending clinical information to PoS patient records as discreet data<br>• Sending virtual visit notifications to the PoS |
| 2.1.8 | Will support identification of virtual visits eligible for claims submission | R | Solutions should not automatically trigger claims submission for all completed encounters.<br><br>Solutions can assist clinical users to identify virtual visits that are eligible for claims (e.g. offering a “billable” vs “nonbillable” flag). |
| 2.1.9 | Will provide automated verification of patient's OHIP number | R | Automated OHIP verification can assist clinical users from a claims and medico-legal perspective. It can also make patient registration processes more efficient.<br><br>Solutions should verify that 10-digit number format is valid.<br><br>Solutions can also:<br>• Verify that number is associated with patient<br>• Verify that OHIP number is valid through MOH verification |
| 2.1.10 | Will support distribution of patient surveys | R | Solutions should allow users to trigger survey distribution to registered patients (e.g. at the end of a virtual care encounter) to support quality improvement efforts and patient experience reporting. |
| 2.1.11 | Will provide ability for virtual visit information to be shared with patients and their caregivers | R | Solutions should allow clinical users to share notes with patients after the visit has ended. |

| | | | |
|---|---|---|---|
| 2.1.12 | Will enable verification of provider identity using a provincial identity management service | R | Solutions should integrate with provincial provider identity and access management services and Ontario Identity Access Management (ONEID) using latest standards (e.g. OAuth)<br><br>Once available, solutions should integrate with the provincial patient digital Identity Authentication and Authorization (IAA) services.<br><br>Future versions of the standard will provide further guidance. |

## 2.2 Privacy and Security

***Privacy***

Virtual visits involve the collection, use and disclosure of personal health information (PHI) and personal information (PI). As a result, organizations delivering virtual visits must ensure their operations are compliant with the *Personal Health Information Protection Act* and other relevant legislation.[12]

Virtual visits can entail certain risks not often encountered in-person care. Examples that organizations, clinical users and vendors should consider and plan for, include:

*Video*

- Scheduling confirmation or reminder includes unauthorized PHI access
- Video launches from an unsecure location
- Wrong patient being invited to participate in a video virtual visit
- Wrong patient attending a video virtual visit
- Wrong clinical user invited to or attending a multipoint video virtual visit
- Video virtual visit launched in error after a patient virtual visit is cancelled
- Sharing information (I.e. test results) for the wrong patient during a video virtual visit
- Clinical users or staff given unauthorized access during an encounter or to the videoconferencing system
- A Video virtual visit is recorded without authorization

*Secure Messaging*

- Messages sent to the wrong patient
- Attaching personal health information for the wrong patient to a message
- Unauthorized clinical users reviewing patient requests and messages without their consent
- Unauthorized clinical users copied on a message sent to a patient

Organizations and clinical users can mitigate many of these risks by implementing appropriate privacy and security policies, procedures and practices. Certain risks can also be mitigated by selecting virtual visit solutions that meet a minimum set of privacy and security requirements (outlined in Section 2.2.1). This includes taking reasonable steps to confirm that technologies used by patients permit personal health information to be shared in a private and secure manner[13] .

12 Other statutes that may apply include the Personal Information Protection and Electronic Documents Act (PIPEDA Ontario) for personal information exchange and Canadian Anti-Spam Legislation (CASL) for secure messaging and emailing.

13 See the CPSO's Telemedicine Policy. https://www.cpso.on.ca/Physicians/Policies-Guidance/Policies/Medical-Records (November 2019)

***Information Security***

Health care organizations and clinical users should ensure their virtual visit solution providers will deliver information security services as part of their service obligations. For example, virtual visit solutions must have information security safeguards such as access to information, security incident response, encryption, logging & monitoring, operational procedures and other mechanisms.

Virtual visit information security services will comply with applicable requirements described in the Ontario Health EHR Security Toolkit[14] which is aligned with OntarioMD's EMR Hosting Requirements.

Solution providers will formally describe and commit to delivering information security safeguards to the health care organizations and clinical users implementing their virtual visit solutions.

### 2.2.1 Privacy & Security Requirements

*Priorities: (M)andatory; (R)eccomended*

| # | Requirement | Priority | Notes |
|---|---|---|---|
| 2.2.1.1 | Will provide an audit trail of all virtual visit encounters. | M | Audit records must record and retain information about virtual visit transactions (i.e. event ID, start and end date and time).<br><br>Audit records must include:<br>• Visits that were interrupted or abandoned for technical reasons<br>• Any modification or deletion of personal health information (encounter summaries, messages, file or image attachments) |
| 2.2.1.2 | Will protect all data, whether in transit or at rest, from unauthorized disclosure and/or modification | M | Solutions must use industry standard cryptographic and hashing mechanisms to encrypt and safeguard personal health information. |
| 2.2.1.3 | Will provide an up-to-date Privacy Impact Assessment (PIA) | M | Solution providers will provide an updated privacy impact assessment (PIA) with no major risks outstanding and confirmation that all applicable laws, regulations and policies are met. |
| 2.2.1.4 | Will provide an up-to-date application level Threat Risk Assessment (TRA) | M | Solution providers will provide an updated threat risk assessment (TRA) with all critical/high risks mitigated will be conducted, according to industry standards, by a certified information security professional (i.e. CISSP, CISA), preferably an impartial third-party resource. |

14 https://www.ehealthontario.on.ca/en/support-topics/EHR-security-toolkit/policies-and-standards

| | | | |
|---|---|---|---|
| 2.2.1.5 | Will provide a comprehensive, binding services agreement for the virtual visit solution | M | Solution providers will describe the services and the administrative, technical and physical safeguards relating to the confidentiality and security of patient and other information.<br><br>At minimum, safeguards will include: Access controls; Data retention; Cybersecurity coverage; and Liability terms. |
| 2.2.1.6 | Will ensure all virtual visit data is held by systems located in Canada | M | Virtual visit personal health information must not be accessible from outside of Canada or transferred outside of Canada except with the prior express notification of the appropriate user. |

## 3.0 VIDEOCONFERENCING VISITS

This section lists solution requirements for synchronous videoconferencing virtual visit solutions.

A synchronous video virtual visit involves an encounter between one or more clinicians ("consultant") and a remotely located patient at a specific day and time. Clinicians and patients join video visits using endpoint devices, such as video monitors, laptops, tablets or mobile phones.

A patient may participate in the visit from home or another chosen location using a device they operate independently ("direct-to-patient video visit"). Alternatively, a caregiver or clinician may assist the patient to access care virtually by providing a device, as well as initiating and managing the video visit ("supported video visits").

Other patients may be located at a secure physical environment that provides them with onsite access to technology and, in some cases, clinical support services ("hosted video visit"). Please see section 3.3 for more information about hosted visits.

Video virtual visits can either be point-to-point (2 endpoints) or multipoint (3 or more endpoints). A single video virtual visit may be scheduled for multiple patients ("group video visit").

Videoconferencing may also be used by two or more clinical users to discuss and direct the management of an individual patient's care ("case conferencing")[15].

In addition to video media, a video virtual visit may also involve the exchange of text, documents, images or biometric data through secure messaging, file transfer or screen-sharing tools.

Health care organizations and clinical users should ensure videoconferencing solutions can support a secure, uninterrupted clinical encounter. Unauthorized user access to a video event can be avoided by requiring user authentication to access the video event (e.g. password-protected portal) or other security controls for video visit accessible by URL within emails or calendar entries. In addition to these controls, patient identity can be verified during the video event through manual facial recognition or OHIP card display.

Videoconferencing solutions can also support audio-only encounters (no visual input). In some situations, audio only visits may be an acceptable alternative to video visits, especially if insufficient bandwidth is available.

15 While case conferencing encounters are not virtual visits, they can be supported by videoconferencing solutions that meet the requirements outlined in this document.

## 3.1 Video Visit - Use Cases

| Use Case | Description |
|---|---|
| Direct-to-Patient | A family physician uses their EMR to initiate a scheduled video visit with a patient, who connects using an application on their mobile phone. The physician and patient discuss the patient's response to a new medication and agree to a follow-up visit in two weeks. The physician ends the call, documents directly into their medical record and submits a claim for the visit. |
| Supported Video Visit | A registered nurse from an Integrated Community Care team schedules a video visit with a geriatrician prior to visiting a patient at home. At the appointment time, the Registered Nurse logs into her tablet from the patient's home and initiates the video visit, which the geriatrician joins from their desktop. Once connected, the RN positions the tablet so the geriatrician can interact directly with the patient. When the geriatrician closes the visit, both clinicians document the encounter and the geriatrician submits a claim for the visit. |
| Hosted Video Visit | A surgeon's administrative assistant schedules a follow-up video visit at a community hospital, supported by a telemedicine nurse, near the patient's home in northeastern Ontario. At the appointment time, the surgeon initiates the visit from their HIS calendar and the nurse connects through their room-based video system. The nurse introduces the patient and uses a medical peripheral to facilitate the surgeon's visual inspection of the surgical site. Both the surgeon and nurse document in their client records and the surgeon submits a claim for the visit. |
| Case Conferencing | A multi-disciplinary cancer conference coordinator (MCC) schedules a multipoint rounds meeting between an oncologist and several allied health care professionals based in a hospital and family health team. The MCC initiates the visit from their laptop and the other clinicians use either desktop or laptops to initiate the visit by selecting a URL and entering a security PIN. The MCC leads a discussion of the treatment of several patients. Once the discussion finishes, the MCC ends the call and documents the outcome. |
| Group Video Visit | A psychologist initiates a scheduled group video visit as part of a group cognitive behavioural therapy (CBT). Each patient accesses the video visit by using their mobile phone or laptop to log into the hospital's patient portal and requesting access to the video session. The psychologist authorizes each patient to join the call based on their first name. The first names of the nine patients who join the group visit are displayed to help the psychologist facilitate the group discussion. At the end of the session, the psychologist ends the session and documents the group visit. |

## 3.2 Video Visit - Solution Requirements

*Priorities: (M)andatory; (R)eccomended*

| # | Requirement | Priority | Notes |
|---|---|---|---|
| 3.2.1 | Will enable unique video visits | M | Solutions must assign a unique event ID to each video visit. |
| 3.2.2 | Will enable scheduled video visits | M | Solutions must allow clinical users to schedule a video visit for a future date and time. |
| 3.2.3 | Will enable unscheduled video visits | M | Solutions must allow clinical users to immediately initiate video visits. |
| 3.2.4 | Will enable point-to-point video visits | M | Solutions must support video visits between a clinical user and another user endpoint. |
| 3.2.5 | Will enable multipoint video visits | M | Solutions must support video visits between a clinical user and two or more user endpoints. |
| 3.2.6 | Will deliver a high level of video experience via commonly available network bandwidths | M | Solutions should support high resolution and high framerate content sharing.<br><br>Min Content Resolution: 1024x768<br>Min Content Framerate: 5 fps<br><br>At a minimum, video solutions must support:<br><br>Minimum Resolution: 448p<br>Minimum Framerate: 15fps |
| 3.2.7 | Will enable clinical users to manage a video visit | M | Solutions must provide clinical users with configurable options for managing the video visit.<br><br>These could include:<br>• Initiating visits (virtual waiting room)<br>• Managing participant access<br>• Ending the visit |
| 3.2.8 | Will enable clinical users to invite a guest user to a video event | M | Solutions must offer a mechanism for guest users such as caregivers or care team members to join a video visit. |
| 3.2.9 | Will prevent unauthorized entry to an ongoing virtual visit event. | M | Access controls include restricting access to authenticated users or providing a PIN to unauthenticated users. |
| 3.2.10 | Will enable users to share files or documents | M | Solutions must support content sharing relating to the encounter. Possible options include screen-sharing or secure file transfer. |
| 3.2.11 | Will support industry standard encryption for real-time communications | M | Recommended encryption standards for real-time communication protocols include:<br><br>• **H323:** (H.235 for H.323 media encryption, AES)<br>• **SIP:** (DTLS SRTP, TLS 1.2 or higher)<br>• **WebRTC:** (DTLS SRTP) |

| | | | |
|---|---|---|---|
| 3.2.12 | Will enable clinical users to export a secure calendar entry and URL for scheduled video visits | R | Solutions should enable scheduled video visits to be integrated in external calendaring systems of other clinical users (e.g. HIS, EMR, Outlook). |
| 3.2.13 | Will provide a visual indicator of poor call quality to all participants in an ongoing video virtual visit event. | R | None |
| 3.2.14 | Will provide an audio-only option | R | An audio visit may be an acceptable alternative if insufficient bandwidth is available to support a video visit. |
| 3.2.15 | Will provide the ability to switch audio and/or video inputs (USB peripherals) during an active video visit event. | R | Solutions should allow different audio and video sources to be used during an event. For example, the clinical user could use a standard webcam and a hand-held exam camera in the same event. |
| 3.2.16 | Will provide additional data for operational statistics and information.<br><br>This data could include:<br>• Negotiated media codecs<br>• Role of each participant (host, guest) in the event.<br>• Performance data such as packet loss, jitter. | R | Operational data is used to identify technical issues and support requirements for end-user support.<br><br>A common issue that would require investigation is degraded video and audio during an eVisit. |
| 3.2.17 | Will enable a videoconferencing endpoint to be added to a video virtual visit event using a dialing alias | R | Dial String Format:<br>H.323 ID, E.164 or SIP URI |

## 3.3 Hosted Video Visits - Solution Requirements

This section lists additional requirements for hosted video visits.

A hosted videoconferencing visit is a point-to-point or multipoint videoconferencing encounter where the patient is physically located at a regulated health care facility or equivalent organization (“host site”). In Ontario, patients currently receive care at over 1,500 host sites. Many of these sites are located in Northern and rural communities and provide patients with access to nursing supports and peripheral technologies.

Hospital and specialist providers purchasing non-OTN videoconferencing solutions must ensure they can continue to schedule, initiate and manage hosted video visits. For some patients, a hosted video visit may be more appropriate than a direct-to-patient video visit.
Some examples include:

- The patient requires support accessing appropriate videoconferencing equipment or internet connection
- The patient is receiving intensive or residential care at the host site
- The consulting clinician has a clinical protocol requiring the videoconferencing event to take place at a secure, supportive physical environment
- The consulting clinician requires a clinical assessment be performed on the patient by a telemedicine nurse, which may involve the use of peripheral device such as an electronic stethoscope or ENT scope

Support for hosted video visits involves coordinated scheduling with host site organizations who support events initiated by multiple consulting providers. To maximize stability and the patient/provider experience, OTN Video (via Pexip) is currently the only video solution that supports visits at host sites. OTN will be working with partners to pilot flexible mechanisms for connecting to the host site network.

Hospital and specialist providers are advised to select video solutions that can support the requirements below. The standard will be updated once host site connectivity specifications are confirmed.

*Priorities: (M)andatory; (R)eccomended*

| # | Requirement | Priority | Notes |
|---|---|---|---|
| 3.3.1 | Will enable clinical users to import and launch a video event from a secured iCalendar data source | R | Enables health care organizations and clinical users to launch a secure video event, |
| 3.3.2 | Will enable clinical users to support interoperable video visits with sites using codec-based videoconferencing systems and peripheral devices | R | Supported Interoperability Protocols:<br>H.323, SIP, WebRTC<br><br>Audio Protocols:<br>G.711(a/μ), G.719, G.722, G.722.1, G.722.1 Annex C, Siren7™, Siren14™, G.729, G.729A, G.729B, Opus, MPEG-4 AAC-LD, Speex, SILK, AAC-LC<br><br>Video Codecs:<br>H.261, H.263, H.263++, H.264 (Constrained Baseline Profile, Baseline Profile and High Profile), H.264 SVC (UCIF Profiles 0, 1)<br>VP8, VP9<br><br>Content Sharing:<br>H.239 (for H.323)<br>BFCP (for SIP)<br>VP8, VP9 (for WebRTC high framerate)<br><br>Firewall Traversal:<br>H323 – H.460.17, H.460.18, H.460.19<br>SIP/WebRTC: STUN, TURN, ICE |

## 4.0 SECURE MESSAGING VIRTUAL VISITS

This section lists requirements for secure messaging virtual visit solutions.

A secure messaging virtual visit is a clinical encounter in which a patient and clinician exchange secure messages about a particular medical issue. It does not include videoconferencing between the patient and clinician as this would be classified as a virtual video visit instead.

A secure messaging virtual visit can be initiated by a patient (“patient-initiated visit”) or by a clinician (“clinician-initiated visit”). The exchange of messages can be "synchronous” or “asynchronous”. With synchronous messaging, the patient and clinician are connected at the same time and exchange messages back and forth during the session. With asynchronous messaging, when a message is sent, the receiver is notified and responds at a later time. Each secure messaging virtual visit typically involves one or more messages sent by both the clinician and patient.

A virtual visit solution must support patient-initiated virtual visits. Pilot evaluation results also strongly support clinician-initiated visits. Solutions must support bidirectional communication between patients and one or more clinicians, including follow-up questions and responses.

Virtual visits performed using secure messaging involve the collection, use and disclosure of personal health information. Unlike videoconferencing events, where patient identity can be confirmed during the encounter, health care organizations and clinicians must select a solution that offers mechanisms to both register and authenticate patients and their caregivers.

A secure messaging solution can be used to interact with patients regarding both clinical and administrative matters. In the eVisit Primary Care pilot, qualified solutions enable their users to identify whether a set of messages is “billable” or “non-billable” for physician reimbursement purposes within the pilot. Solutions that are intended to support the communication of medical assessments and advice should provide their clinical users with a similar mechanism to ensure appropriate claims submissions. Please see the Ontario Virtual Care Program billing manual and recent INFOBulletins for up-to-date information about virtual care services which are eligible for reimbursement and any associated requirements.

The following patient-facing digital tools offer value but the functionality that they provide does not meet the minimum requirements of a virtual visit:

- Online appointment scheduling services
- Portals that provide online access to health records
- Solutions that support completion of documentation by patients
- One-way clinician-initiated communication (I.e. notifications)

Online messages can be complex to secure adequately, particularly where messaging occurs between disparate solutions. It is recommended that digital planners consider solutions that achieve requisite levels of security in simple ways including, for example, software-as-a-service (cloud-based) solutions, provincial (Digital Health Service Catalogue) solutions or portal-based solutions.

## 4.1 Secure Messaging Virtual Visit - Use Cases

| Use Case | Description |
|---|---|
| Patient Initiated Virtual Visit | A patient experiencing chills, fatigue and congestion opens an application on their phone and initiates a visit by sending a message to their physician. The patient is prompted to enter their symptoms, which are shared with the physician. The physician reviews the symptoms and sends a response with additional questions. The patient responds with information and an attached image of their temperature reading. The physician provides medical advice to the patient. The physician closes the visit and saves the encounter summary in the patient's record. |
| Clinician Initiated Virtual Visit | A family physician receives a blood test result showing low thyroid levels for a patient on thyroid medication. The physician uses their EMR to send the patient a message advising them of the result and requesting the patient respond with information about missed doses or low thyroid symptoms. The patient responds the following day, reporting fatigue and constipation and asking a question about when the medication should be taken. The physician answers the question and advises the patient to fill a new prescription at an increased dose. The physician closes the visit. The message thread is automatically saved in the patient's record. |

## 4.2 Secure Messaging Virtual Visit – Solution Requirements

*Priorities: (M)andatory; (R)eccomended*

| # | Requirement | Priority | Notes |
|---|---|---|---|
| 4.2.1 | Will protect messages exchanged between clinician users and patients | M | Solutions must protect messages by means of secure infrastructure or equivalent cloud services |
| 4.2.2 | Will enable unique secure messaging visits | M | Solutions must assign a single unique ID to all secure messaging transactions associated with the visit. |
| 4.2.3 | Will ensure secure messaging services are only accessible by authenticated users | M | Solutions must ensure secure messaging based virtual visit services are only accessible to authenticated patients and caregivers. |
| 4.2.4 | Will enable registered patients and their caregivers to initiate a virtual visit about a health issue or concern | M | Solutions must enable registered patients to send a clinician a message about a health issue or concern. |
| 4.2.5 | Will enable patient notification when virtual visit services are unavailable | M | Solutions must allow health care organizations and clinical users to notify patients when virtual visit services are unavailable.<br><br>Potential scenarios include<br>• After hours / weekends<br>• Vacation / leave<br>• Technical issues |

| | | | |
|---|---|---|---|
| 4.2.6 | Will enable configurable user notifications to alert clinical users and patients | M | Clinical users and patients should be notified when there has been a change in the status of the virtual visit.<br><br>Some examples include:<br>• New visit request<br>• Accepted visit<br>• Cancelled visit<br>• Completed visit |
| 4.2.7 | Will allow patients and their caregivers to attach and send files to a clinician to support their virtual visit | M | Some health issues or concerns require patients to submit supporting documentation or images to support completion of the visit. |
| 4.2.8 | Will allow different user roles to manage patient virtual visit messages | M | Solutions must enable health care organizations and clinical users to configure how patient virtual visit requests are reviewed and managed. This might involve manual or automated triaging of patient requests. |
| 4.2.9 | Will allow clinical users to end a virtual visit | M | Clinical users determine when a virtual visit is complete.<br><br>Solutions must not default to ending a video or secure messaging visit based on elapsed time or number of transactions. |
| 4.2.10 | Will record all messages, files and images associated with each individual virtual visit for clinical documentation and auditing purposes | M | Solutions must logically group multiple message transactions relating to a single visit. Information should be recorded in a chronological format. |
| 4.2.11 | Will enable clinical users to initiate secure messaging virtual visit | M | Solutions should enable clinical users to initiate a virtual visit.<br><br>Solutions must enable patients to send follow-up questions before the visit can be closed (bidirectional). |
| 4.2.12 | Will separate clinical and administrative messages | R | Clinical user experience and efficiency can be improved by creating separate inboxes (groups) for administrative versus clinical messages. |
| 4.2.13 | Will enable multiple clinical users to participate in a secure messaging visit | R | Solutions should allow other care team members to join in a secure messaging visit. This can include reading or creating messages. |
| 4.2.14 | Will allow clinical users to flag patient messages as urgent or requiring attention | R | Physicians participating in the provincial pilot identified the ability to flag patient messages for review as important for triaging and care team collaboration purposes. |
| 4.2.15 | Will provide a read receipt for messages that can be filtered | R | Physicians participating in the provincial pilot identified this feature as important in order to confirm that medical advice has been received before a visit can be completed. |

# 5.0 VIRTUAL VISITS – DATA REQUIREMENTS

The following minimum data specification has been developed to support consistent reporting of virtual visit activity by health service providers, including OHTs, and vendors in Ontario.

OTN has developed a data dictionary, with field definitions and sample values, to support implementation of the specification.

## 5.1 Minimum Virtual Visit Data Elements

| Data Requirement | Mandatory | Recommended |
|---|---|---|
| Event ID | Unique identifier for each transaction | None |
| Organization ID | Organization which provisioned the account | Ministry-assigned MNS Facility Number |
| Product ID | Ability to identify the platform that supported the event transaction | |
| Event Details | Event Start Date<br>Event Start Time<br>Event End Date<br>Event End Time<br>Event Type | Therapeutic Area of Care |
| Provider Information | MRP First Name<br>MRP Last Name<br>Regulatory College of MRP<br>Professional Registration Number | None |
| Provider Location | Postal Code | IP Address |
| Participant Location | Postal Code | IP Address |
| Modality User | Primary modality | None |
| Event Outcome | None | Event outcome |

# APPENDIX

## i. Disclaimer

This document relates to but is not specific to the provincial services of OTN, Ontario Health or other provincial health organizations. The standard detailed in this document is a non-normalized standard and therefore errors, omissions and revisions may occur. This document is not intended to be nor should be deemed legal advice. OTN encourages legal counsel be engaged as required.

## ii. All rights reserved



## iii.Trademarks