Ontario Health

Virtual Visits

Solution Requirements

Version 2.0

October 2022

TABLE OF CONTENTS

i. Acknowledgements

The requirements listed in this document are informed by several provincial initiatives, including the Virtual Visits Verification Program, the Partner Video Project and the eVisit Primary Care pilot and have been reviewed by numerous health care organizations and clinician leaders. Ontario Health would like to thank the following individuals and organizations for their extensive contributions to this document.

Individuals:

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

Organizations:

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

ii. Disclaimer

This document relates to, but is not specific to, the provincial services of 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 it be deemed, legal advice. Ontario Health encourages legal counsel be engaged as required.

iii. Change Highlights

For traceability, the following significant changes were made:

In version 2.0:

- Branding changes made to align with Ontario Health brand
- Notification requirement 2.1.8 moved to general section as it applies to all modalities (previously 4.2.5)
- Removed registration context from 2.1.1 to support all models of care
- Removed clinical data context from 2.1.3
- Additional clarity on requirements 2.1.5, 2.1.7, and 3.2.10
- Combined 3.2.2, 3.2.3 and 3.2.4 to be inclusive of all models of care
- Updated 3.2.3 to provide clarity on group visits (multi point visits)
- Added requirement 2.1.18 to support multi factor authentication (Recommended Requirement)
- Added making acceptable use policy available in requirement 2.3.1
- Added end-to-end encryption and FIPS 2/3 as a recommended standard in 2.3.6
- Updated reference 17 for PIA methodology in 2.3.7
- PIA summary must include a brief description of the service and role that the organization plays under PHIPA in 2.3.7
- Low risk items should be mitigated within 12 months, reporting low risk status is not required in 2.3.7
- Experience of privacy personnel performing PIA must be in health care context in 2.3.7
- Clarified that the PIA submission must be recent within the last 2 years and applicable to the current solution/submission in 2.3.7
- Clarified what is required in a PIA summary in 2.3.7
- Updated 2.3.8 to say that TRA Assessor has five years experience or recognized security certification (Changed from “and/or” to “or”)
- TRA summary must include a table of risks and risk status in 2.3.8
- TRA must be refreshed every 3 years instead of 2 years in 2.3.8
- Revised language and clarity on which certifications are accepted in 2.3.11
- Added wording on breach management and third--party access to PHI in 2.3.12
- Revised language around data residency. Added reference to PHIPA section defining PHI in 2.3.14 and 2.3.15
- Added IP address as an option for Host and Patient location for 5.1.8 and 5.1.9

In version 1.2:

- Requirement 2.3.8 has been amended to provide the option of providing SOC 2 Type 2 compliance as an alternative to a Threat Risk Assessment (TRA) Summary Report

In version 1.1.1:

- It is expected that these requirements will be leveraged by the Ontario Virtual Care Program and other ministry programs. (Further information on this, including provider eligibility requirements, will be released by the ministry in coming weeks.)

In version 1.1:

- Document has been amended to include OTN becoming part of Ontario Health
- Section 1 (Introduction) has been amended to include information about Ontario Health's Virtual Visits Verification Program
- Requirement 2.1.9 has been added to reflect AODA Level AA compliance
- Requirement 2.1.7 about notifications of virtual visit availability is now applicable to both video and secure messaging solutions
- Requirement 4.2.8 was moved to the general section
- English and French language support was added as a recommended requirement in the general section
- General privacy program requirements 2.3.1, 2.3.2 and 2.3.3, have been added
- Audit requirements 2.3.4 and 2.3.5 has been amended with new logging requirements
- Requirement 2.3.6 has been amended to reflect recommended cryptographic standards
- Requirements 2.3.7 and 2.3.8 have been amended to include specific PIA and TRA requirements for the verification process
- Requirements 2.3.9 and 2.3.10 have been added for vulnerability assessment scans and penetration testing
- Requirement 2.3.13 has been added to include support for data retention
- Requirements 2.3.14 and 2.3.15 for data residency have been amended
- Video requirement 3.2.3 has been amended to clarify that video solutions must support immediate initiation of video visits
- Video requirement 3.2.7 has been amended to clarify video event management functionality
- Video requirement 3.2.8 has been amended to include additional security controls for guest user access
- Section 5 (Data Requirements) has been amended

1.0 INTRODUCTION

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

This document addresses two types of virtual visit solutions:

- Videoconferencing
- Secure Messaging

This document outlines a framework and mandatory requirements that virtual visit solutions must demonstrate to be verified by Ontario Health's Virtual Visits Verification Program. The purpose of the Virtual Visits Verification Program is to support health service providers to select solutions that are designed to support safe, privacy and security enhanced virtual visits with patients and to advance interoperable health information exchange in alignment with the Digital Health Information Exchange Standard[1].

A list of solutions that have successfully completed the process and attested to meeting the provincial standard for virtual visits will be published by Ontario Health to guide health care organizations and clinicians to select and procure verified virtual visits solutions. Health care organizations and clinicians may have unique obligations not included in this framework and as such should consult with their respective privacy, security and legal office or counsel as they assess their readiness to deploy or use a virtual visits solution.

Provincial standards for virtual care will continue to evolve as solutions mature. Both Solution Providers and health service providers will be advised of future updates to the solution requirements.

This document references several external sources, including the Ministry of Health's *Digital Health Policy Guidance Document*[2], College of Physician and Surgeons of Ontario's published policies on telemedicine[3], medical record-keeping[4], Ontario Hospital Association guidance[5], and the Hospital Act[6].

A companion document – *Adopting and Integrating Virtual Visits into Care: Draft Clinical Guidance* – is also available (Details in section 5) which provides additional guidance to health care providers.

---

[1] https://www.ontariohealth.ca/system-planning/digital-standards/digital-health-information-exchange
[2] 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] https://www.oha.com/news/understanding-your-legal-accountabilities-a-guide-for-ontario-hospitals
[6] https://www.ontario.ca/laws/regulation/900965

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.

Several virtual visit pilots across Ontario have demonstrated how virtual visits can improve clinical outcomes and improve patient satisfaction and convenience[7].

A virtual visit can be supported using one or more modalities, including videoconferencing and secure messaging, and may involve one or more digital transactions. This is demonstrated in the following three use cases. These examples are provided for illustrative purposes and do not address many other virtual care use cases.

Use Case	Description
Video Visit	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.
Secure Message	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(s) are automatically saved in the patient's medical record.

[7] 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.

Use Case	Description
Multiple Digital Transactions	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 Disease (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 test 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 visit before health care services are provided
- Digital interactions between two clinicians concerning a mutual patient[8]
- Collection of biometric data by a remote monitoring device

Virtual Visit Solutions

Some Point of Service ("PoS") systems, such as Electronic Medical Records or Hospital Information Systems, offer virtual visits through embedded videoconferencing or messaging solutions that rely on the Point of Service system's scheduling, patient portal or application and clinical documentation functionalities.

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, and clinical documentation functionalities.

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-to-provider collaboration.

[8] This includes eReferrals, eConsults and case conferencing encounters. Note however that case conferencing encounters can be supported by videoconferencing solutions that meet the requirements outlined in this document.

1.2 Key Audiences

Key audiences for this document include:

- Solution Providers: A Solution Provider may be a Vendor or an HSP Innovator.
- Health Service Provider Innovators have developed a virtual care solution, independently or in partnership with other Health Service Providers and/or Vendors
- Health Service Providers include solo practitioners, clinics, home and community care organizations, hospitals or any other Health Service Provider type that is fully or in part funded by the Ministry of Health
- Ontario Health Teams

1.3 Scope

This document outlines requirements for virtual care solutions that support videoconferencing, secure messaging, or a combination of videoconferencing and secure messaging. It is applicable to virtual visit solutions delivered by health service providers (e.g., primary care, specialists, hospitals, community service providers, etc.).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 sections:

- Section 2 outlines General, Privacy and Security 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 any of the following user types:

- Patients and caregivers
- Clinicians such as physicians, nurses and allied health professionals
- Organizational users (e.g., administrative staff)

1.4 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 such as eConsult and 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).

1.5 Terms and Abbreviations

The following terms and abbreviations are defined and shall be applied to all requirement tables in this document:

All requirements are either denoted as "M" for Mandatory, or "R" for recommended.

Mandatory: Solution Providers ***must*** support these requirements.
Clinicians ***may*** choose to incorporate these requirements into their workflow as they see fit.

Recommended: Solution Providers ***may*** choose to support these requirements, however they are not mandated to do so.
Ontario Health recommends that Solution Providers work towards meeting recommended requirements as they may become Mandatory in a future version of the solution standard.

#: Unique numeric identifier that identifies each requirement within the Requirements Repository.

Conformance Language
The following definitions of the conformance verbs are used in this document:
• Shall/Must: Required/Mandatory
• Should: Best Practice/Recommendation
• May: Acceptable/Permitted/Encouraged

2.0 GENERAL VIRTUAL VISIT REQUIREMENTS

This section outlines general solution, patient safety, 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 and patient preferences, in addition to relevant professional, regulatory and industry standards.

Professional standards[9] that should be considered when selecting a virtual visit solution and delivering virtual care include the ability for healthcare organizations and clinicians to:

- Identify patients accurately
- Manage patient informed consent to receive care virtually
- 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 available and accessible for patient care, 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.

Solution Providers should ensure that virtual visit solutions and services are designed to enable healthcare organizations and clinicians to meet their relevant professional, regulatory and industry standards and obligations to enable patients to receive safe, privacy and security enhanced virtual care and to access their health information.

An important part of the province's vision for virtual care is the meaningful integration of stand-alone solutions into providers' existing PoS systems. The minimum interoperability requirements stated below align with initiatives underway to improve Ontario's digital health infrastructure[10]. Virtual visit solutions that demonstrate more mature levels of integration with PoS 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 Ontario's Digital Identity Program.

[9] For example, the CPSO's Telemedicine Policy. https://www.cpso.on.ca/Physicians/Policies-Guidance/Policies/Telemedicine (November 2019)

[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)ecommended

#	Requirement	Priority	Notes
2.1.1	Provide patients and their caregivers with secure access to virtual visit services	M	Solutions must provide a mechanism to access the virtual visit services. Solutions should enable other clinicians to participate in virtual visits. Please see 3.2.6, 3.2.7 and 4.2.2 for applicable requirements.
2.1.2	Allow clinicians to end a virtual visit	M	Clinicians determine when a virtual visit is complete. Solutions must not default to ending a video or secure messaging encounter based on elapsed time or number of transactions. Patients and/or caregivers must also be able to end a virtual visit; however, it will not be formally documented as a completed visit in the virtual care solution unless the provider does so.
2.1.3	Capture information about a virtual visit to meet record keeping or reporting obligations	M	Solutions must record information that is relevant for the virtual visit. At a minimum, solutions must capture: • Event details as identified in section 5.1 • A record of any messages, files or images that were

#	Requirement	Priority	Notes
			exchanged during the patient encounter Solutions must record sufficient information to associate the virtual visit information with a specific patient record.
2.1.4	Enable the electronic transfer of virtual visit information to a medical or hospital record	M	Virtual visit information (as defined in 2.1.3) must be transferable to a medical record or hospital record for clinical documentation and audit purposes. Solutions may also allow clinicians to select clinically relevant chat messages, file attachments or images that should be transferred to the patient's medical or hospital record. A minimal event log must be retained which describes the event, event participants, timestamp and if any data was deleted as a result of a data exchange.
2.1.5	Make technical support services available to clinicians	M	Virtual visit Solution Providers must provide technical support to health care organizations and clinicians as part of their Service Level Agreement (SLA). Health care organizations offering virtual visit services must ensure reasonable technical support services are available to patients and if not

#	Requirement	Priority	Notes
			that they are provided directly by the clinical organization. Contact information for technical support should be easily accessible by patients.
2.1.6	Enable authorized users to extract data for reporting purposes	M	Solutions must make virtual visit data available to support organizational and system level reporting. See Sections 5.1 and 5.2 for minimum data elements.
2.1.7	Enable patient notification when virtual visit services are unavailable	M	Solutions must allow health care organizations and clinicians to notify patients when virtual visit services are unavailable. Potential scenarios include • After hours / weekends • Vacation / leave • Technical issues Solution should indicate to patient if messages were received or failed during transmission.
2.1.8	Enable configurable user notifications to alert clinicians and patients	M	Clinicians and patients should be notified when there has been a change in the status of a virtual visit. Some examples include: • New visit request • Accepted visit • Cancelled visit • Completed visit
2.1.9	Manage patient agreements for virtual visit services	R	Solutions should allow clinicians to send and receive patient agreements and other

#	Requirement	Priority	Notes
			educational materials relating to virtual visit services.
2.1.10	Meets Web Content Accessibility Guidelines (WCAG) 2.0 Level AA[11] requirements or higher	R	Solutions should have web and user interfaces that provide accessibility to Ontarians with disabilities; and comply with the Accessibility for Ontarians with Disabilities Act (AODA)[12].
2.1.11	Provide seamless integration with Point of Service systems	R	Stand-alone solutions should demonstrate seamless integration, which should include elements such as: • Single sign-on with PoS login credentials • Receiving patient context (identification) information from PoS systems • Automatically sending clinical information to PoS patient records as discreet data • Sending virtual visit notifications to the PoS • Calendar information
2.1.12	Support identification of virtual visits eligible for claims submission	R	Solutions should not automatically trigger claims submission for all completed virtual visits. Solutions can assist clinicians to identify virtual visits that are eligible for claims (e.g., offering a "billable" vs "nonbillable" flag).

[11] https://www.w3.org/WAI/standards-guidelines/wcag/
[12] https://www.ontario.ca/laws/statute/05a11

#	Requirement	Priority	Notes
2.1.13	Provide automated verification of patient's Ontario Health Insurance Plan (OHIP) number	R	Automated OHIP verification can assist clinicians from a claims and medico-legal perspective. It can also make patient registration processes more efficient. Solutions should verify that the 10-digit OHIP number format is valid. Solutions can also: • Verify that number is associated with the patient by matching with registration details • Verify that the patient's OHIP number is valid through MOHLTC Health Card Validation (HCV)
2.1.14	Support distribution of patient surveys	R	Virtual visit solutions will allow providers to send surveys to patients in order to: • Administer certain types of clinical questionnaires prior to an encounter (e.g., relating to mental health, child development, post-operative care) • Support quality improvement efforts and patient experience reporting (e.g., at the end of a virtual care encounter)
2.1.15	Provide ability for virtual visit information to be shared with patients and their caregivers	R	Solutions should allow clinicians to securely share notes with patients after the visit has ended.

#	Requirement	Priority	Notes
2.1.16	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). Once available, solutions should integrate with the provincial patient digital Identity Authentication and Authorization (IAA) services. Future versions of the standard will provide further guidance.
2.1.17	Will support Canadian English and Canadian French languages	R	Solutions will support Canada's official languages of English and French. Clinicians should be able to use (read, write, and edit) information in the chosen language. The Solution Provider's website can also be read in chosen language, including but not limited to training materials and release notes.
2.1.18	Enable verification of clinician identity using multi-factor authentication	R	Clinicians should authenticate using more than one piece of evidence to access the solution (2FA). Examples: • FOB + PIN • Password + Security question • Password + Authentication app • Authenticator + SMS/Phone call

2.2 Privacy and Security

Privacy

Virtual visits involve the collection, use, disclosure, and transmission of personal health information (PHI) and personal information (PI) over the Internet. As a result, Solution Providers and once procured, healthcare organizations and clinicians delivering virtual visits must be able to demonstrate that solutions and services utilized to deliver virtual care are designed to support privacy and security enhanced virtual visits in accordance with applicable laws, regulations, and industry standards. These include but are not limited to the *Personal Health Information Protection Act, the Freedom of Information and Protection of Privacy Act,* and other relevant legislation.[13]

Maintaining privacy while delivering care using virtual visit solutions involves unique challenges that can lead to unintended breaches. Below are examples of unintended breaches that organizations, clinicians, and Solution Providers should be aware of and prevent:

Video

- Scheduling or appointment confirmation, or reminder notification, includes an excessive amount of PHI
- Video launches from a public space
- Wrong patient being invited to participate in a video visit
- Wrong patient attending a video visit
- Wrong clinician invited to or attending a multi point video visit
- Video visit launching in error after a patient's virtual visit is cancelled
- Sharing information, such as test results, with the wrong patient during a video visit
- Clinicians or staff given unauthorized access during an encounter or to the videoconferencing system
- A video virtual visit is recorded without authorization

Secure Messaging

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

Organizations and clinicians can mitigate many of these risks by implementing appropriate privacy and security policies, procedures, and practices. Certain risks can also be mitigated by

[13] Other Legislation that may apply to vendors include the Personal Information Protection and Electronic Documents Act (PIPEDA) and Canadian Anti-Spam Legislation (CASL).

selecting virtual visit solutions that meet a minimum set of privacy and security requirements as outlined in Section 2.2.1. Mitigation includes taking reasonable steps to confirm that technologies used by patients enable PHI to be shared in a private and secure manner[14].

Information Security

Health care organizations and clinicians 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 and monitoring, operational procedures, and other mechanisms.

Virtual visit information security services will comply with applicable requirements described in the Ontario Health EHR Security Toolkit[15] which is aligned with OntarioMD's EMR Hosting Requirements[16].

Solution Providers must formally describe and commit to delivering information security safeguards to the health care organizations and clinicians implementing their virtual visit solutions.

2.3 Privacy and Security Requirements

Priorities: (M)andatory; (R)ecommended

2.3.1	Publish a notice of its information practices relevant to its virtual visit solution and services	M	At a minimum the notice must describe how the Solution Provider handles and protects personal and health information and privacy rights of patients and makes available an acceptable use policy.
2.3.2	Have a designated employee responsible for privacy	M	Contact information for the designated privacy official must be publicly accessible on the Solution Providers website.
2.3.3	Have a privacy and security program that includes policies and procedures	M	At a minimum, Solution Providers must have a privacy policy that outlines rules governing the collection, use, disclosure, retention, accuracy, security and disposal of PHI/PI, breach management, information security,

[14] CPSO's Telemedicine Policy. https://www.cpso.on.ca/Physicians/Policies-Guidance/Policies/Medical-Records (November 2019)
[15] https://www.ehealthontario.on.ca/en/support-topics/EHR-security-toolkit/policies-and-standards
[16] https://www.ontariomd.ca/emr-certification/emr-specification/library

			business continuity and disaster recovery, access, correction, and complaint practices.
2.3.4	Provide an electronic audit trail of all virtual visit encounters including a log of all accesses and transfers of PHI	M	Audit records must record and retain information about virtual visit transactions (e.g., event ID, start and end time and date) as detailed in Sections 5.1, 5.2 and 5.3. Audit records must include visits that were interrupted or abandoned for technical reasons. Solutions that retain encounter summary records must maintain an audit log that includes: • Type of information viewed, handled, modified, or otherwise dealt with • Date and time it was viewed, handled, modified, or otherwise dealt with • Identity of all persons who viewed, handled, modified, or otherwise dealt with PHI and/or PI • Identity of the individual to whom the PHI relates Data in the audit log must not be altered, removed, or deleted, just marked as altered, removed, or deleted.
2.3.5	Provide audit security controls to maintain audit integrity	M	Audit trail will include all login attempts whether successful or failed. Must log traffic that indicates unauthorized activity encountered at the application server. The log must include: • Timestamp, user ID/application ID, originating IP address, port accessed or computer name • External ODBC connections used to execute SQL or data layer queries

			• Application data stored external to the database such as attachments • All data files used to meet other local requirements (e.g., reporting requirements) • System time must be synchronized with a trusted source to maintain audit trail integrity • Be protected to ensure audit integrity and from unauthorized access, modification, and destruction
2.3.6	Put in place reasonable safeguards and controls to protect all data, whether in transit or at rest	M	Solutions must support end-to-end encryption using current industry standard cryptographic and hashing mechanisms to encrypt and safeguard PHI and/or PI. Recommended cryptographic standards include: NIST SP 800-22 Revision 1a - A Statistical Test Suite for Random and Pseudorandom Number, FIPS 140-2/3 - Security Requirements for Cryptographic Modules.

2.3.7	Provide an up-to-date Privacy Impact Assessment (PIA) summary	M	PIA assurances and requirements must include:
			
			• The PIA summary which contains:
			  ○ a table of contents of the full PIA
			  ○ a brief description of the solution
			  ○ a statement reflecting that the PIA is current
			  ○ the role(s) which the organization plays under PHIPA and why they believe that the authority applies
			  ○ a summary of risk findings including a likelihood and impact table or risk heat map
			  ○ a mitigation plan (for risk findings) and approval of the plan
			  ○ a status on any outstanding risks

- the name and contact information of the individual(s) and/or organization(s) who conducted the PIA

- PIA must have been completed within two years of the date the Solution Provider submits to become an Ontario Health verified solution and is still relevant to the current solution/submission

- Any risks identified as high must be mitigated prior to submission. The Solution Providers risks assessed as medium must have a clear mitigation plan with timelines for closure within six months of risk being identified in the PIA. It is recommended that low risks be reflected in the summary and mitigated within twelve months, however Ontario Health will not monitor completion to this recommended timeline

- PIA must have been completed by a certified professional with any of the following credentials obtained through the International Association of Privacy Professionals (IAPP): Certified Information Privacy Professional (CIPP/C); Certified Information Privacy Manager (CIPM); Certified Information Privacy Technologist (CIPT) or a professional with a minimum of two years of experience conducting privacy impact assessments in Ontario and/or Canada and in a health care context based on PHIPA or other provincial health legislation

			• The PIA methodology must include a legislative analysis relevant to Ontario and its healthcare context and at a minimum have been mapped to the ten Fair Information Principles as published by the Canadian Standards Association (CSA) Model Code for the Protection of Personal Information and in accordance with the PIA guidelines issued by the Information and Privacy Commission of Ontario[17] with respect to healthcare • PIA and risk mitigation plan must be approved by the Solution Provider's authorized representative or Chief Privacy Officer. The PIA summary is required to be submitted to Ontario Health • The PIA must be based on the latest solution design and technical architecture with no significant changes to the solution, services, or privacy program since completion of the PIA • The PIA must be refreshed every 3 years or when there has been a change in the solution, legislation, policy, or business operations of the Solution Provider that may have an impact to the privacy of health information or to privacy rights, whichever is first
2.3.8	Provide an up-to-date Threat Risk Assessment (TRA) Summary Report or SOC 2 Type 2 Audit Report	M	This requirement can be met by providing a Threat Risk Assessment (TRA) Summary Report or a SOC 2 Type 2 Audit Report to satisfy the following conditions, as applicable: • The TRA must have been completed within the last two years, while the SOC 2 Type 2 Audit must have been completed

[17] https://www.ipc.on.ca/wp-content/uploads/resources/phipa_pia-e.pdf

within the last year, being relevant to the virtual visit solution submitted with no significant changes to the solution, services, or security program since the completion of the TRA or the SOC 2 Type 2 Audit

- The TRA or SOC 2 Type 2 Audit was performed by a qualified assessor:
    - For the TRA, this means that the assessor has at least five years of direct full-time security experience that includes conducting TRAs or managing security risks and in possession of an industry recognized security certification (e.g., CISSP, CISM, CISA, CRISC) that is in good standing
    - For the SOC 2 Type 2 Audit report, this requires that the audit was performed by an AICPA certified third-party organization

- If a TRA Summary Report is being submitted, the following, additional requirements apply:
    - The TRA must have been completed with a security analysis based on an industry-standard risk assessment methodology (e.g., HTRA, NIST, OCTAVE, etc.)
    - The TRA Summary must include a table of risks, the status of risks, and a risk treatment status
      Note: Any risks identified as high must be mitigated prior to Solution Provider submissions. Medium risks must have clear

mitigation plans for closure within 6 months of the risks being identified. It is recommended that low risks be mitigated within 12 months however the Solution Provider will not be required to report their status to Ontario Health
    - The TRA must be refreshed every two years or whenever there is a significant change in the design of the solution, policy or applicable business operations that may impact the security posture of the solution

- If a SOC 2 Type 2 Audit report is being submitted, the following, additional requirements apply:
    - The proposed Virtual Visits solution/platform was included in the SOC 2 Type 2 Audit scope.
    - The audit was conducted within the last year and the "Period of Examination" covers the period during which the solution/platform was developed
    - The report states that in the auditor's opinion, the examined controls were suitably designed and operated effectively throughout the audit period to provide reasonable assurance that Solution Provider service commitments and system requirements will be achieved under the following Trust Services and Common Criteria: Trust Services Criteria: Security Control Environment

(CC1.1, CC1.2, CC1.3, CC1.4, CC1.5)
Communication and Information (CC2.1, CC2.2, CC2.3)
Risk Assessment (CC3.1, CC3.2, CC3.3, CC3.4)
Monitoring Activities (CC4.1, CC4.2)
Control Activities (CC5.1, CC5.2, CC5.3)
Logical and Physical Access Controls (CC6.1, CC6.2, CC6.3, CC6.4, CC6.5, CC6.6, CC6.7, CC6.8)
System Operations (CC7.1, CC7.2, CC7.3, CC7.4, CC7.5)
Change Management (CC8.1)
Risk Mitigation (CC9.1, CC9.2)
Trust Services Criteria: Availability
Additional Criteria for Availability (A.1, A1.2, A1.3)
Trust Services Criteria: Processing Integrity
Additional Criteria for Processing Integrity (PI1.1, PI1.2, PI1.3, PI1.4, PI1.5)
Trust Services Criteria: Confidentiality Additional Criteria for Confidentiality (C1.1, C1.2)

- The SOC 2 Type 2 Audit must be refreshed every year or whenever there is a significant change in the design of the solution, policy or applicable business operations that may

			impact the security posture of the solution No unreasonable exceptions or deviations, commonly referred to as control failures, were noted under the “Results of Tests” section. In the auditor's opinion, the examined controls were designed and operated effectively (i.e., no significant negative findings reported).
2.3.9	Perform periodic vulnerability assessment scans	M	Vulnerability assessment (“VA”) scans are to be done at a minimum on a quarterly basis or when there has been a major software release, change in architecture or infrastructure. Vulnerability scans must include the application and application infrastructure. For hosted environments, the hosting provider may need to submit their own VA scan results. Latest vulnerability scan results are to be submitted with the TRA. Evidence that quarterly scans have been completed may be requested within the TRA refresh cycle.
2.3.10	Perform periodic penetration tests	M	Penetration tests are to be done, at a minimum, on an annual basis, or when there has been a major software release or change in architecture or infrastructure. Penetration tests must include the application and application infrastructure. For hosted environments, the hosting provider may need to submit their own penetration test results. Latest penetration test results are to be submitted with the TRA. Evidence that annual tests have been completed may be

			requested within the TRA or SOC 2 Type 2 refresh cycle.
2.3.11	Meet security and privacy controls	M	This requirement can only be met by providing a current copy of one of the following certifications: ISO 27001 certification, SOC 2 Type 2 Audit Report, HITRUST certification, OntarioMD certification or Canada Health Infoway certification. Obtaining any one of these certifications will ensure that the following control objectives have been met: • Network and Operations • Physical Security • Acceptable Use of Information and Information Technology • Access to Control and Identity Management for System-Level Access • Information Asset Management • Information Security Incident Management • Threat Risk Management • Business Continuity • Cryptography • Security Logging and Monitoring • Electronic Service Provider
2.3.12	Provide a comprehensive agreement framework for the virtual visit solution and related services including for any third party retained to assist in providing the agreement framework	M	Solution and third-party provider agreements will at minimum include privacy and security language that describes the services and the administrative, technical, and physical safeguards relating to the confidentiality and security of PHI and PI and how the Solution Provider, and any third-party Solution Provider retained, comply with applicable legislation including but not limited to those listed above. The third-party provider agreement should include the extent of access to PHI and breach management practices.

2.3.13	Support healthcare organizational or clinician retention obligations and policies	M	Solutions must facilitate or enable the collection and retention of PI and PHI. Solutions must retain PI and PHI in accordance with record keeping and retention obligations and policies. It is recommended that clinicians follow applicable regulatory and/or professional standards such as the CPSO data retention and destruction guidance within the medical records management policy.
2.3.14	Ensure all PHI data as defined in PHIPA is held by systems located in Canada	M	Solution must be hosted within a Canadian location including all PHI, data and backups.
2.3.15	Inform users including patients if any PHI data as defined in PHIPA flows outside of Canada	M	Access and transient PHI must only flow outside of Canadian borders with prior consent from the 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 and a remotely located patient at a specific day and time. Clinicians and patients join a video visit 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 in accessing care virtually by providing a device, and/or initiating and managing the video visit ("supported video visit").

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 multi point (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 clinicians to discuss and direct the management of an individual patient's care ("case conferencing")[18].

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 clinicians 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 a video visit accessible by a 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 a video visit, especially if insufficient bandwidth is available.

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 and documents directly into their medical record.
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. The geriatrician joins from their desktop. Once connected, the RN positions the tablet so that the geriatrician can interact directly with

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

Use Case	Description
	the patient. When the geriatrician closes the visit, both clinicians document the encounter.
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 patient's family member also joins the call from their residence in Toronto. The nurse introduces the patient and family member 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.
Case Conferencing	A multi-disciplinary cancer conference coordinator (MCC) schedules a multi point 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 behavioral therapy (CBT) session. Each patient accesses the video visit by using their mobile phone or laptop to login to the hospital's patient portal and requests 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)ecommended

#	Requirement	Priority	Notes
3.2.1	Enable unique video visit	M	Solutions must assign a unique event ID to each video visit.

#	Requirement	Priority	Notes
3.2.2	Enable point-to-point video visit	M	Solutions must support a video visit between a clinician and another user endpoint. This must apply to at least one of the following: • Video visit scheduled for a future date and time • Unscheduled or real-time video visit • Video visit triggered from a patient or clinical alert
3.2.3	Enable group video visit	M	Solutions must support video visits between clinician and two or more user endpoints such as: • Clinician to multiple patients • Clinician to patient and Caregiver(s) • Multiple clinicians to patient
3.2.4	Deliver a high level of video experience via commonly available network bandwidths	M	Solutions must support high resolution and high framerate content sharing. **Min Video Resolution:** 1024x768 **Min Video Framerate:** 5 fps At a minimum, video solutions must support: **Minimum Resolution:** 448p **Minimum Framerate:** 15fps
3.2.5	Enable clinicians to manage a video visit	M	Solutions must provide clinicians with configurable options for managing the video visit. This must include:

#	Requirement	Priority	Notes
			• Initiating visits • Managing participant access • Disabling features such as video recording, transcripts, and file transfer • Ending the visit (clinician host will determine end session)
3.2.6	Enable clinicians 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. For guest users, additional security and privacy controls are required. These must include: • Invites and invite URLs are encoded and unique (e.g., they cannot be easily reversed engineered and are not reusable) • Virtual visits should have the option to be protected with a password or PIN Alternatively, the clinician can enable a waiting room where the guest user's identity can be confirmed before allowing them to join the visit. Additional recommended controls include: • The invite URLs expire within a given time frame or become invalid if the session does not take place within a scheduled period • If there are multiple participants, the invite URLs

#	Requirement	Priority	Notes
			can only be used by the invited participant • Virtual visits passwords should not be shared through non-secured channels (e.g., e-mail)
3.2.7	Prevent unauthorized entry to an ongoing virtual visit event	M	Access controls include restricting access to authenticated users or providing a PIN, password, or secured token to unauthenticated users. Solutions should display participant names to the video visit host.
3.2.8	Enable users to share content	M	Solutions must support content sharing relating to the video visit. Possible options include screen-sharing or secure file transfer.
3.2.9	Support industry standard encryption for real-time communications	M	Recommended encryption standards for real-time communication protocols include: • **H323:** (H.235 for H.323 media encryption, AES) • **SIP:**(DTLS SRTP, TLS 1.2 or higher) • **WebRTC**: (DTLS SRTP)
3.2.10	Enable a virtual waiting room	R	Solutions may allow clinicians to enable a waiting room. This allows clinicians to control when participant(s) join the synchronous video event.
3.2.11	Enable clinicians to export a secure calendar entry and URL for a scheduled video visit	R	Solutions should enable a scheduled video visit to be integrated into the external

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

#	Requirement	Priority	Notes
3.2.17	Provide equipment and connectivity testing	R	Solutions will allow patients and caregivers to perform equipment (i.e., audio and/or video) and connectivity tests (i.e., Wi-Fi) and send reports to clinics prior to virtual visits.
3.2.18	Enable patient to save a virtual visit calendar entry and URL to their virtual calendar application	R	Solutions will enable patients to import a scheduled event into their calendaring systems (e.g., Google calendar, iCal, Outlook, etc.). Solutions will enable patients to forward a scheduled event to caregivers to participate in the event.

3.3 Hosted Video Visit - Solution Requirements

This section lists additional requirements for a hosted video visit.

A hosted video visit is a point-to-point or multi point 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 videoconferencing solutions must ensure they can continue to schedule, initiate, and manage a hosted video visit. 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 a peripheral device such as an electronic stethoscope or ENT scope

Support for a hosted video visit involves coordinated scheduling with host site organizations who support events initiated by multiple consulting providers.

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

Priorities: (M)andatory; (R)ecommended

#	Requirement	Priority	Notes
3.3.1	Enable clinicians to import and launch a video visit from a secured iCalendar data source	R	Enables health care organizations and clinicians to launch a secure video visit.
3.3.2	Enable clinicians to support an interoperable video visit with sites using codec-based videoconferencing systems and peripheral devices	R	Supported Interoperability Protocols: H.323, SIP, WebRTC Audio Protocols: 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 Video Codecs: H.261, H.263, H.263++, H.264 (Constrained Baseline Profile, Baseline Profile and High Profile), H.264 SVC (UCIF Profiles 0, 1) VP8, VP9 Content Sharing: H.239 (for H.323) BFCP (for SIP) VP8, VP9 (for WebRTC high framerate) Firewall Traversal: H323 – H.460.17, H.460.18, H.460.19 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 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 clinicians with a similar mechanism to ensure appropriate claims submissions. Please monitor 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 secure 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)ecommended

#	Requirement	Priority	Notes
4.2.1	Protect messages exchanged between clinician users and patients	M	Solutions must protect messages by means of secure infrastructure or equivalent cloud services.

#	Requirement	Priority	Notes
4.2.2	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	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	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 secure message about a health issue or concern. This can be achieved by sending a message to a care team member for review.
4.2.5	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.
4.2.6	Allow different clinician roles to manage patient virtual visit messages	M	Solutions must enable clinicians to configure how patient virtual visit requests are reviewed and managed. This might involve manual or automated triaging of patient requests.
4.2.7	Enable clinicians to record all messages, files and images associated with each individual virtual visit	M	Solutions must logically group multiple message transactions relating to a single visit. Information should be recorded in a chronological format. Solutions may allow clinical users to select which file or image attachments should be recorded in the patient record.
4.2.8	Enable clinicians to initiate secure messaging virtual visits	M	Messaging must be bi-directional between clinicians and patients.

#	Requirement	Priority	Notes
4.2.9	Separate clinical and administrative messages	R	Clinician experience and efficiency can be improved by creating separate inboxes (groups) for administrative versus clinical messages.
4.2.10	Enable multiple authorized clinicians 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.
4.2.11	Allow clinicians 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.
4.2.12	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 requirements have been developed to support consistent health information exchange, reporting and audit of virtual visit activity.

The minimal requirement is an event summary that provides information about the organization, solution, modality of each unique virtual visit and the day and time it occurred.

Some virtual visit solutions may capture additional encounter summary information, including patient identifiers and consultation notes.

Ontario Health has developed data guidance, with field definitions and sample values, to support implementation of these data requirements.

Please refer to the document Virtual Visit Data Guidance[19] for further details.

5.1 Mandatory Virtual Visit Data Elements

#	Data	Requirement
5.1.1	Event ID	Unique identifier for each virtual visit.
5.1.2	Organization ID	Organization that provisioned the account.
5.1.3	Solution ID	Unique identifier for the solution that supported the virtual visit.
5.1.4	Event Details	• Event Start Date • Event Start Time • Event End Date • Event End Time
5.1.5	Event Type	Event Type.
5.1.6	Clinician Information (Event Host)	• First Name • Last Name
5.1.7	Physician Flag	Physician Flag.
5.1.8	Clinician Location (Event Host)	Postal Code or IP Address.

[19] https://www.ontariohealth.ca/sites/ontariohealth/files/2022-02/virtual-visit-data-guidance.pdf

#	Data	Requirement
5.1.9	Participant Location (patient)	Postal Code or IP Address.
5.1.10	Modality Used	Primary Modality.

5.2 Recommended Virtual Visit Data Elements

5.2.1	Therapeutic Area of Care	Area of Practice.
5.2.2	Name of Regulatory College	Name of Regulatory College.
5.2.3	Professional Registration Number	Professional Registration Number.
5.2.4	Clinical Provider Location (Event Host)	IP Address.
5.2.5	Participant Location (participants)	IP Address.
5.2.6	Participant Location (patient)	IP Address.
5.2.7	Participant Identification (patient)	Participant's name, date of birth, gender, and unique identifier i.e., Health card number
5.2.8	Event Outcome	Event Outcome.

5.3 Virtual Visit Data Elements for Audit

#		
5.3.1	Create Date	Date the Event was created.
5.3.2	Last Modified Date	Date the event record was last modified.
5.3.3	Event Actor	Author of the event creation or last modification.

APPENDIX

i. All rights reserved

ii. Trademarks