



**Ontario  
Health**

# Virtual Visits Solution Requirements

Version 3.0

July 14, 2025

# TABLE OF CONTENTS

- i. Acknowledgements
- ii. Disclaimer
- iii. Change Highlights in This Version

## **1. Introduction**

- 1.1. Definitions
- 1.2. Key Audiences
- 1.3. Scope
- 1.4. Out of Scope
- 1.5. Terms and Abbreviations

## **2. General Virtual Visit Requirements**

- 2.1. General Solution Requirements
- 2.2. Privacy and Security
- 2.3. Privacy and Security Requirements

## **3. Videoconferencing Visits**

- 3.1. Video Visit – Use Cases
- 3.2. Video Visit – Solution Requirements
- 3.3. Hosted Video Visit Solution Requirements

## **4. Secure Messaging Virtual Visits**

- 4.1. Secure Messaging – Use Cases
- 4.2. Secure Messaging – Solution Requirements

## **5. Virtual Visits – Data Requirements**

- 5.1. Mandatory Virtual Visit Data Elements
- 5.2. Recommended Virtual Visit Data Elements

## **Appendix**

- i. All Rights Reserved
- ii. Trademarks

## i. Acknowledgements

The requirements listed in this document are informed by several provincial initiatives, including the Virtual Visits Verification Program, and have been reviewed by numerous health service providers 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 your legal counsel be engaged as required.

### iii. Change Highlights

For traceability, the following significant changes were made:

In version 3.0

- Section 1.1 - Addition to clarify that SMS (Short Messaging Service) is not considered secure messaging under “Use Cases”
- Requirement 2.1.3 – Addition to notes that recorded events are also considered PHI
- Requirement 2.1.10 – Addition to the notes around accessibility reports being made available
- Section 2.2 – Addition of more information around Privacy Management and Information Security Programs
- Requirement 2.3.2 – Clarified notes around contact for privacy issues
- Requirement 2.3.4 – Clarification around audit logs
- Requirement 2.3.7 – Substantial changes to the notes around what is required in the PIA and submitted as part of the PIA summary. Added Certified Information Privacy Professional (CIPP/US) to list of accepted credentials
- Requirement 2.3.8 – TRA requirement removed. And only the noted certificates will meet this requirement. Clarification that it must be clear that video and/or secure messaging were in scope for the assessment. Removal of CHI certification.
- Requirement 2.3.11 – This requirement now refers to the mandatory software supplier questionnaire
- Section 4.0 – Added clarity that SMS does not meet the standard
- Section 5.0 – Added clarity that Ontario Health does not collect this Virtual Visit usage data
- Section 5.1 - Physician Flag, Event Type was moved from mandatory to recommended (Section 5.2), Organization ID has been removed
- Section 5.2 – requirement 5.2.4, 5.2.5, 5.2.6 have been removed
- Section 5.3 – merged into section 5.2

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
- 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 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 service providers 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.

A list of Solution Providers that have attested to meeting all mandatory requirements in the provincial standard and have successfully completed Verification and Validation is published by Ontario Health. Health Service Providers 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 and the legislative landscape changes. 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](#), [College of Physician and Surgeons of Ontario’s published policies on telemedicine](#), [medical record-keeping](#), [Ontario Hospital Association guidance](#), and the [Hospital Act](#).

The Information and Privacy Commissioner of Ontario has issued Guidelines for The Health Sector, Privacy and Security Considerations for Virtual Health Care Visits.

### 1.1 Definitions

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

Solution Providers are providers of virtual care solutions that are required to meet all Mandatory Requirements for patient-to-provider video and/or secure messaging, as applicable and as specified in these Virtual Visits Solution Requirements. Solution Providers may be solution vendors, Health Service Provider Innovators (HSP Innovators), or Local Solution Providers.

Health Service Providers (HSP) 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. The *Personal Health Information Protection Act, 2004* (PHIPA) refers to this role as a Health Information Custodian (s. 3).

Health Service Provider Innovator (HSP Innovator) is an HSP who has developed, procured and/or implemented a non-commercial virtual care solution, independently or in partnership with other Health Service Providers and/or Solution Providers.

Local Solution Provider is a Solution Provider that has deployed and self-hosts a unique instance of a solution vendor's software.

### **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.

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.

PHIPA applies to virtual care as it does to in-person care. Health Information Custodians must comply with the provisions of PHIPA; in addition to “all” other applicable laws and regulations, as well as guidance issued by relevant professional regulators.

<b>Use Case</b>	<b>Description</b>
<b>Video Visit</b>	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.
<b>Secure Message</b>	A patient logs into an Electronic Medical Record (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

Use Case	Description
	<p>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.</p> <p>NOTE: Short Message Service (SMS) or texting is not considered a secure means of communication and cannot be used to transmit sensitive information and data.</p>
<p><b>Multiple Digital Transactions</b></p>	<p>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 discusses 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.</p>

*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. 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.
- Collection of biometric data by a remote monitoring device.

## *Virtual Visit Solutions*

Some Point of Service (“PoS”) systems, such as Electronic Medical Records (“EMR”) or Hospital Information Systems (“HIS”), 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 Service Providers and clinicians are encouraged to consider solutions that can support other uses beyond virtual visits. For example, a secure messaging service can also support administrative functions and provider-to-provider collaboration.

## 1.2 Key Audiences

Key audiences for this document include:

- Solution Providers
- Health Service Providers
- Health Service Provider Innovators
- Local Solution Providers
- 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 used by Health Service Providers (e.g., primary care, specialists, hospitals, community service providers, etc.).

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 without patient interaction
- 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 this document.

### 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 solutions, patient safety, privacy, and security requirements that apply to all virtual visit solutions.

When selecting a virtual visit solution, Health Service Providers and clinicians should consider several factors including clinical suitability, workflow, and patient preferences, in addition to relevant professional, regulatory and industry standards.

Professional standards, for example, the [CPSO's Telemedicine Policy](#), that should be considered when selecting a virtual visit solution and delivering virtual care include the ability for Health Service Providers and clinicians to:

- Identify patients accurately
- Manage patient informed consent to receive care virtually
- Ensure patient information obtained virtually is 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 Service Providers 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. 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 Service Providers 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 the Digital Health Consumer Access Program (DHCAP).

## 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	<p>Solutions must provide a secure mechanism to access virtual visit services.</p> <p>Solutions should enable other clinicians to participate in virtual visits.</p> <p>See 3.2.6, 3.2.7 and 4.2.2 for applicable requirements.</p>
2.1.2	Allow clinicians to end a virtual visit	M	<p>Clinicians determine when a virtual visit is complete.</p> <p>Solutions must not default to ending a video or secure messaging encounter based on elapsed time or number of interactions.</p> <p>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.</p>
2.1.3	Capture information about a virtual visit to meet record keeping or reporting obligations	M	<p>Solutions must record information that is relevant for the virtual visit.</p> <p>At a minimum, solutions must capture:</p> <ul style="list-style-type: none"> <li>• Event details as identified in section 5.1</li> <li>• A recording of any messages, files or images</li> </ul>

#	Requirement	Priority	Notes
			<p>that were exchanged during the patient encounter</p> <p>Solutions must record sufficient identifying information to associate the virtual visit information with a specific patient record.</p> <p>Recorded audio and video events and secure messages are considered PHI and should be retained, transferred and disposed of in accordance with PHIPA and other applicable legislation or guidance from regulatory colleges.</p>
2.1.4	Enable the electronic transfer of virtual visit information to a medical or hospital record	M	<p>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.</p> <p>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.</p> <p>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.</p>
2.1.5	Make technical support services available to Health Service Providers	M	Virtual visit Solution Providers must provide technical support

#	Requirement	Priority	Notes
			<p>to Health Service Providers and clinicians as part of their Service Level Agreement (SLA). Health Service Providers offering virtual visit services must ensure that reasonable technical support services are available to patients and if not that they are provided directly by the clinical organization. Contact information for technical support should be easily accessible by patients.</p>
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 for the minimum data elements.
2.1.7	Enable patient notification when virtual visit services are unavailable	M	<p>Solutions must allow Health Service Providers and clinicians to notify patients when virtual visit services are unavailable.</p> <p>Potential scenarios include:</p> <ul style="list-style-type: none"> <li>• After hours / weekends</li> <li>• Vacation / leave</li> <li>• Technical issues</li> </ul> <p>Solutions should indicate to patient if messages were received or failed during transmission.</p>
2.1.8	Enable configurable user notifications to alert clinicians and patients	M	<p>Clinicians and patients must be notified when there has been a change in the status of a virtual visit.</p> <p>Some examples include:</p> <ul style="list-style-type: none"> <li>• New visit request</li> </ul>

#	Requirement	Priority	Notes
			<ul style="list-style-type: none"> <li>• Accepted visit</li> <li>• Cancelled visit</li> <li>• Completed visit</li> </ul>
2.1.9	Manage patient agreements for virtual visit services	R	Solutions should allow clinicians to send and receive patient agreements and educational materials relating to virtual visit services.
2.1.10	Meets Web Content Accessibility Guidelines (WCAG) 2.0 Level AA requirements or higher	R	<p>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).</p> <p>Solution providers should make available upon request or publish a notice of the web accessibility level the solution provider reaches relevant to its solution. At a minimum the solution provider must be able to provide an Accessibility Conformance Report (ACR) or Voluntary Product Accessibility Template (VPAT).</p>
2.1.11	Provide seamless integration with Point of Service (PoS) systems	R	<p>Stand-alone solutions should demonstrate seamless integration, which should include elements such as:</p> <ul style="list-style-type: none"> <li>• Single sign-on with PoS login credentials</li> <li>• Receiving patient context (identification) information from PoS systems</li> <li>• Automatically sending clinical information to PoS patient records as discreet data</li> </ul>

#	Requirement	Priority	Notes
			<ul style="list-style-type: none"> <li>• Sending virtual visit notifications to the PoS</li> <li>• Calendar information</li> </ul>
2.1.12	Support identification of virtual visits eligible for claims submission	R	<p>Solutions should not automatically trigger claims submission for all completed virtual visits.</p> <p>Solutions can assist clinicians to identify virtual visits that are eligible for claims (e.g., offering a “billable” vs “nonbillable” flag).</p>
2.1.13	Provide automated verification of patient's Ontario Health Insurance Plan (OHIP) number	R	<p>Automated OHIP verification can assist clinicians from a claims and medico-legal perspective. It can also make patient registration processes more efficient.</p> <p>Solutions should verify that the OHIP number format is valid.</p> <p>Solutions can also:</p> <ul style="list-style-type: none"> <li>• Verify that number is associated with the patient by matching with registration details</li> <li>• Verify that the patient’s OHIP number is valid through MOHLTC Health Card Validation (HCV)</li> </ul>
2.1.14	Support distribution of patient surveys	R	<p>Virtual visit solutions will allow providers to send surveys to patients to:</p> <ul style="list-style-type: none"> <li>• Administer certain types of clinical questionnaires prior to and after an encounter (e.g., relating to mental</li> </ul>

#	Requirement	Priority	Notes
			<p>health, child development, post-operative care, etc.)</p> <ul style="list-style-type: none"> <li>• Support quality improvement efforts and patient experience reporting (e.g., at the end of a virtual care encounter)</li> </ul>
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.
2.1.16	Enable verification of provider identity using a provincial identity management service	R	<p>Solutions should integrate with provincial provider identity and access management services and Ontario Identity Access Management (ONEID) using latest standards (e.g., OAuth).</p> <p>Once available, solutions should integrate with the provincial patient digital Identity Authentication and Authorization (IAA) services.</p> <p>Future versions of the standard will provide further guidance.</p>
2.1.17	Will support Canadian English and Canadian French languages	R	<p>Solutions will support Canada's official languages of English and French.</p> <p>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.</p>

#	Requirement	Priority	Notes
2.1.18	Enable verification of clinician identity using multi-factor authentication	R	<p>Clinicians should authenticate using more than one piece of evidence to access the solution (2FA).</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>• FOB + PIN</li> <li>• Password + Security question</li> <li>• Password + Authentication app</li> <li>• Authenticator + SMS/Phone call</li> </ul>

## 2.2 Privacy and Information Security

### *Privacy*

Virtual visits involve the collection, use, disclosure, retention, and/or transmission of personal health information (PHI) and personal information (PI). In addition, access, transfer and disposal, when required, of PHI/PI are fundamental to the solution capabilities. The purpose of this program is to support Solution Providers, healthcare organizations and clinicians to develop and use privacy and security enhanced solutions and services in accordance with applicable laws, regulations, regulatory bodies, and industry standards. These include but are not limited to the *Personal Health Information Protection Act, 2004*, the *Freedom of Information and Protection of Privacy Act*, and other relevant legislation. Other Legislation that may apply to service providers include the Personal Information Protection and Electronic Documents Act (PIPEDA) and Canadian Anti-Spam Legislation (CASL).

Maintaining privacy while delivering care using virtual visit solutions involves unique challenges that can lead to unintended breaches. Below are examples of 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/PI
- 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/PI sent to the wrong patient
- Attaching PHI for the wrong patient to a message
- Unauthorized individuals reviewing patient requests and messages without their consent
- Unauthorized individuals 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 selecting virtual visit solutions that meet a minimum set of privacy and security requirements as outlined in Section 2.2. Mitigation includes taking reasonable steps to confirm that technologies used by patients enable PHI/PI to be shared in a private and secure manner, as described in the [CPSO Telemedicine Policy](#).

Solution Providers must have a Privacy Management Program in place. A Privacy Management Program ensures an organization has a governance and accountability framework in place so that privacy is built into all initiatives, programs or services and assists in meeting their legislative privacy obligations, protect individual rights and meet the expectations of their business partners or clients. The program should include an implementation roadmap that provides the structure (documented privacy policies and procedures), provide transparency and guide the development, operation, and management of all programs, processes, solutions, and technologies involving PHI/PI.

The Privacy Management Program should be aligned with the organizations' Information Security, data governance and technology infrastructure. The goal is to create a comprehensive plan to effectively operationalize an organization's privacy compliance programs including but not limited to:

- Data breach incident response policy and procedure
- Privacy and cybersecurity training
- Data classification and management
- Data retention
- Solution provider due diligence and contract negotiations

## 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 (administrative, physical, and technical) such as access to information, security incident response, encryption, audit 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](#) which is aligned with [OntarioMD's EMR Hosting Requirements](#).

Solution Providers must have an information security program that consists of activities, projects, and initiatives supporting their organization's information technology framework. These initiatives help organizations accomplish all related business objectives and meet corresponding benchmarks.

An information security program practices allow solution providers to safeguard key business processes, IT assets, and employee data from potentially prying eyes. It also identifies individuals or technological assets that may impact the security or confidentiality of those assets. A well-developed information security program enables an organization to take an inclusive approach to protecting data such as personal health information (PHI), personally identifiable information (PII).

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*

#	Requirement	Priority	Notes
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 manages (uses, discloses) PI and PHI, including a general description of safeguards in relation to that information– this should include the practices that apply to the services the Solution Provider provides to patients, health care organizations and clinicians, how

#	Requirement	Priority	Notes
			to reach the contact person, how to obtain access to or request correction of information and how to make a complaint.
2.3.2	Have a designated employee responsible for privacy	M	The name or title and contact information for the person who is accountable for the organization's privacy program. Solution Provider's privacy policies and practices must be publicly and easily accessible on the solution provider's website. Note: Generic email address (privacy@abc.com) is acceptable; the email must be directed to the employee responsible for privacy and/or the Solution Provider's Privacy Office.
2.3.3	Have a privacy and security program that includes policies and procedures	M	At a minimum, Solution Provider 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, business continuity and disaster recovery, access, correction and complaint practices
2.3.4	Provide an electronic audit log of all virtual visit encounters including a log of all accesses and transfers of PHI	M	The electronic audit log must include: <ul style="list-style-type: none"> <li>• the type of PHI viewed, handled, modified, or dealt with</li> <li>• the date and time the information was viewed, handled, modified, or dealt with</li> <li>• the identity of all persons who viewed, handled, modified, or dealt with the PHI</li> </ul>

#	Requirement	Priority	Notes
2.3.5	Provide audit security controls to maintain audit integrity	M	<ul style="list-style-type: none"> <li>the identity of the individual to whom the PHI relates</li> </ul> <p>Audit trail will include all login attempts whether successful or failed.</p> <p>Must log traffic that indicates unauthorized activity encountered at the application server.</p> <p>The log must include:</p> <ul style="list-style-type: none"> <li>Timestamp, user ID/application ID, originating IP address, port accessed or computer name</li> <li>External ODBC connections used to execute SQL or data layer queries</li> <li>Application data stored external to the database such as attachments</li> <li>All data files used to meet other local requirements (e.g., reporting requirements)</li> <li>System time must be synchronized with a trusted source to maintain audit trail integrity</li> <li>Be protected to ensure audit integrity and from unauthorized access, modification, and destruction</li> </ul>
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 (i.e., at-rest and in-transit data encryption) using current industry standard

#	Requirement	Priority	Notes
			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	<p>OH requires Solution Providers to conduct PIAs on their Solution and to provide to OH the PIA Summary. OH does NOT require a copy of the full PIA. The initial PIA must have been completed within two years of the VVV program initial submission date and subsequently refreshed every 3 years (or prior if there has been a change in the solution, policy, or business operations of the Solution Provider or changes in applicable legislation such as PHIPA that may have an impact to the privacy of health information or to privacy rights). The PIA must be based on the IPC PIA Guide for PHIPA and/or the content of the template contained herein. The PIA summary must include:</p> <ul style="list-style-type: none"> <li>• Table of contents from the PIA;</li> <li>• Detailed description of product/service specifically revolving around the video/secure messaging and related services such as</li> </ul>

#	Requirement	Priority	Notes
			<p>authentication, email and SMS notifications, and appointment booking;</p> <ul style="list-style-type: none"> <li>• A list of third parties assisting in delivering solution with whom the Solution Provider should have agreement(s) in place;</li> <li>• Identification of PHIPA role (s) and rational as to why the authority applies</li> <li>• A legislative analysis for the Ontario healthcare context (PHIPA), based on Fair Information Principles from Canadian Standards Association;</li> <li>• The mandatory and any of the recommended requirements implemented specifically for their software that includes a review of the video and secure messaging solution;</li> <li>• An assessment of all mandatory privacy requirements listed in this Standard;</li> <li>• A reference that an information security assessment (refer to 2.3.11) was also completed;</li> <li>• A confirmation that all PHI is accessed from and hosted within Canada (refer to 2.3.14);</li> <li>• A statement from the Chief Privacy Officer (CPO) or executive responsible for privacy that the PIA reflects the latest solution design</li> </ul>

#	Requirement	Priority	Notes
			<p>and technical architecture with no significant changes to the solution, services, or privacy program since completion of the PIA;</p> <ul style="list-style-type: none"> <li>• A statement of approval from Chief Privacy Officer (CPO) or executive responsible for privacy that the summary reflects the PIA;</li> <li>• 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</li> <li>• A risk table and mitigation plan (for each risk findings) and provide a status on any outstanding risks as of the date of PIA report: <ul style="list-style-type: none"> <li>○ The risk table must state whether a risk has been identified</li> </ul> </li> </ul>

#	Requirement	Priority	Notes
2.3.8	Meet security controls assurance requirements	M	<p>as high, medium or low;</p> <ul style="list-style-type: none"> <li>○ Any risks identified as high must be mitigated prior to VVV submission;</li> <li>○ Risks identified as medium must have a clear mitigation plan with timelines for closure within six months of the date the PIA was submitted. OH may ask for confirmation that risk mitigation has been completed;</li> <li>○ Low risks should be identified and have a mitigation plan for 12 months from the date the PIA was submitted. OH will not track for completion;</li> </ul> <p>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.</p> <p>Provide a current copy of one of the following certifications: SOC 2 Type 2 Audit Report, ISO 27001 certification, HITRUST r2 certification or alternatively, inform Ontario Health that your solution is an OntarioMD Certified EMR listed on OntarioMD’s website.</p>

#	Requirement	Priority	Notes
---	-------------	----------	-------

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

**If SOC 2 Type 2 report is submitted:**

The SOC 2 Type 2 Audit Report must satisfy the following requirements, as applicable:

- The SOC 2 Type 2 Audit must have been completed within the last year, being relevant to the virtual visit solution submitted with no significant changes to the

#	Requirement	Priority	Notes
			<p data-bbox="1047 279 1372 646">solution and clearly indicate that the video and/or secure messaging functionality were in scope for the assessment, services, or security program since the completion of the SOC 2 Type 2 Audit.</p> <ul style="list-style-type: none"> <li data-bbox="998 657 1372 1024">• The SOC 2 Type 2 Audit was performed by a qualified assessor: <ul style="list-style-type: none"> <li data-bbox="1096 783 1372 1024">○ This requires that the audit was performed by an AICPA certified third-party organization</li> </ul> </li> <li data-bbox="998 1098 1372 1717">• 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:</li> </ul> <p data-bbox="950 1749 1356 1890">Trust Services Criteria: Security Control Environment (CC1.1, CC1.2, CC1.3, CC1.4, CC1.5)</p>

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

- 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

#	Requirement	Priority	Notes
---	-------------	----------	-------

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).

When entering the program, Ontario Health will accept a SOC 2 Type 1 report provisionally. The Solution Provider is required to provide a SOC 2 Type 2 report within 6 months of the date its SOC 2 Type 1 is performed.

**If HITRUST r2 certification is submitted:**

Where Solution Providers elect to submit HITRUST certification, the following requirements apply:

- Copy of the validated assessment report, including the scope of the services (video and/or secure messaging) being offered, prepared by a certified HITRUST auditor
  - i1 Certification is accepted on a provisional basis for up to 12 months

#	Requirement	Priority	Notes
---	-------------	----------	-------

- r2 Certification is required no later than 12 months from the date a Solution Provider earns its i1 Certification
- Copy of the HITRUST certificate
- HITRUST certification must be refreshed every 2 years

**If ISO 27001 certification is submitted:**

Where Solution Provider's elect to submit ISO 27001 certification, the following documents must be provided:

- Copy of the Statement of Applicability report including the scope of the services (video and/or secure messaging) being offered.
- Copy of the ISO 27001 certificate
- Annual Surveillance report if ISO certification was received in more than a year from the date of submission.
- ISO certification must be refreshed every 3 years.
- ISO Annual Surveillance Report must be

#	Requirement	Priority	Notes
			submitted for Ontario Health review every year
			<p><b>Local Solution Providers can meet this requirement by submitting a Threat Risk Assessment (TRA) report and attesting to Security Operational Controls:</b></p>
			<p><u>TRA Report Requirements:</u></p>
			<ul style="list-style-type: none"> <li>• The TRA must have been completed within the last two years, being relevant to the virtual visit solution submitted with no significant changes to the solution and clearly indicate that the video and/or secure messaging functionality were in scope for the assessment, services, or security program since the completion of the TRA.</li> <li>• The TRA was performed by a qualified assessor who has at least five years of direct full-time security experience that includes conducting TRAs or managing security risks and is in possession of at least one of the following industry recognized security certifications (CISSP,</li> </ul>

#	Requirement	Priority	Notes
			<p>CISM, CISA, CRISC) that is in good standing</p> <ul style="list-style-type: none"> <li>• The TRA must have been completed with a security analysis based on an industry-standard risk assessment methodology (e.g., HTRA, NIST, OCTAVE, etc.)</li> <li>• The TRA report must include a detailed scope (people, processes and technology), standard/ methodology used, list of identified risks, current status of the risks and a risk treatment plan for the open risks.</li> <li>• Latest vulnerability scan results are to be submitted with the TRA report.</li> <li>• Latest penetration test results are to be submitted with the TRA report. Penetration tests must include the application and application infrastructure.</li> <li>• A refreshed TRA must be conducted every 3 years or whenever there is a significant change in the design of the solution, or applicable business operations/processes</li> </ul>

#	Requirement	Priority	Notes
			that may impact the security posture of the solution. TRA reports shall be submitted to Ontario Health for review.
2.3.9	Perform regular vulnerability assessment scans	M	<p>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.</p> <p>Vulnerability scans must include the application and application infrastructure. For hosted environments, the hosting provider may need to submit their own VA scan results.</p> <p>Evidence of the quarterly scans or a summary of the results may be requested</p>
2.3.10	Perform regular penetration tests	M	<p>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.</p> <p>Penetration tests must include the application and application infrastructure. For hosted environments, the hosting</p>

#	Requirement	Priority	Notes
			<p>provider may need to submit their own penetration test results.</p> <p>Evidence of the annual scans or a summary of the results may be requested.</p>
2.3.11	Security compliance of software suppliers	M	<p>The Solution Provider must provide responses to the Secure Supply Chain Questionnaire for compliance.</p> <p>The Solution Provider should provide YES/NO answers to the questionnaire.</p> <p>In case of a “NO” answer to any of the questions, details of compensating controls, if any, must be provided.</p>
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	<p>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(s) retained comply with applicable legislation including but not limited to those listed above.</p> <p>The third-party provider agreement should include the extent of access to PHI and breach management practices.</p>
2.3.13	Support healthcare organizational or clinician retention obligations and policies	M	<p>Solutions must facilitate or enable the collection and retention of PI and PHI.</p> <p>Solutions must retain PI and PHI in accordance with record</p>

#	Requirement	Priority	Notes
			<p>keeping and retention obligations and policies.</p> <p>It is recommended that clinicians follow applicable regulatory and/or professional standards such as the College of Physicians and Surgeons of Ontario (CPSO) data retention and destruction guidance within the medical records management policy.</p>
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 VIDEO VISITS

This section lists solution requirements for synchronous video 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”). While case conferencing encounters are not virtual visits, they can be supported by videoconferencing solutions that meet the requirements outlined in this document.

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 Service Providers 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
<b>Direct-to-Patient</b>	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.
<b>Supported Video Visit</b>	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 the patient. When the geriatrician closes the visit, both clinicians document the encounter.
<b>Hosted Video Visit</b>	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.
<b>Case Conferencing</b>	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.
<b>Group Video Visit</b>	A psychologist initiates a scheduled group video visit as part of a group cognitive behavioral therapy (CBT) session. Each patient

Use Case	Description
	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.
3.2.2	Enable point-to-point video visit	M	<p>Solutions must support a video visit between a clinician and another user endpoint.</p> <p>This must apply to at least one of the following:</p> <ul style="list-style-type: none"> <li>• Video visit scheduled for a future date and time</li> <li>• Unscheduled or real-time video visit</li> <li>• Video visit triggered from a patient or clinical alert</li> </ul>

#	Requirement	Priority	Notes
3.2.3	Enable group video visit	M	<p>Solutions must support video visits between clinician and two or more user endpoints such as:</p> <ul style="list-style-type: none"> <li>• Clinician to multiple patients</li> <li>• Clinician to patient and Caregiver(s)</li> <li>• Multiple clinicians to patient</li> </ul>
3.2.4	Deliver a high level of video experience via commonly available network bandwidths	M	<p>Solutions must support high resolution and high framerate content sharing.</p> <p>Min Video Resolution: 1024x768 Min Video Framerate: 5 fps</p> <p>At a minimum, video solutions must support:</p> <p>Minimum Resolution: 448p Minimum Framerate: 15fps</p>
3.2.5	Enable clinicians to manage a video visit	M	<p>Solutions must provide clinicians with configurable options for managing the video visit.</p> <p>This must include:</p>

#	Requirement	Priority	Notes
			<ul style="list-style-type: none"> <li>• Initiating visits</li> <li>• Managing participant access</li> <li>• Disabling features such as video recording, transcripts, and file transfer</li> <li>• Ending the visit (clinician host will determine end session)</li> </ul>
3.2.6	Enable clinicians to invite a guest user to a video event	M	<p>Solutions must offer a mechanism for guest users such as caregivers or care team members to join a video visit.</p> <p>For guest users, additional security and privacy controls are required.</p> <p>These must include:</p> <ul style="list-style-type: none"> <li>• Invites and invite URLs are encoded and unique (e.g., they cannot be easily reversed engineered, and are not reusable)</li> <li>• Virtual visits must have the option to be protected with a password or PIN</li> </ul> <p>Alternatively, the clinician can enable a waiting room where the guest user's</p>

#	Requirement	Priority	Notes
			<p>identity can be confirmed before allowing them to join the visit.</p> <p>Additional recommended controls include:</p> <ul style="list-style-type: none"> <li>• The invite URLs expire within a given time frame or become invalid if the session does not take place within a scheduled period</li> <li>• If there are multiple participants, the invite URLs can only be used by the invited participant</li> <li>• Virtual visits passwords should not be shared through non-secured channels (e.g., unencrypted e-mail)</li> </ul>
3.2.7	Prevent unauthorized entry to an ongoing virtual visit event	M	<p>Access controls include restricting access to authenticated users or providing a PIN, password, or secured token to unauthenticated users.</p> <p>Solutions should display participant</p>

#	Requirement	Priority	Notes
			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: <ul style="list-style-type: none"> <li>• H323: (H.235 for H.323 media encryption, AES)</li> <li>• SIP: (DTLS SRTP, TLS 1.2 or higher)</li> <li>• WebRTC: (DTLS SRTP)</li> </ul>
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 calendaring systems of other

#	Requirement	Priority	Notes
			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: <ul style="list-style-type: none"> <li>Negotiated media codecs</li> </ul>

#	Requirement	Priority	Notes
			<ul style="list-style-type: none"> <li>• Role of each participant (host, guest) in the event.</li> <li>• Performance data such as packet loss, jitter.</li> </ul> <p>A common issue that would require investigation is degraded video and audio during a video visit.</p>
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.
3.2.17	Provide equipment and connectivity testing	R	Solutions should 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

#	Requirement	Priority	Notes
			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 in northern and rural communities and provide patients with access to nursing supports and peripheral technologies.

Health Service Providers and clinicians developing, procuring and/or implementing 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.

Health Service 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 Service Providers and clinicians to launch a secure video visit.
3.3.2	Enable clinicians to support an interoperable video visit with sites using codec-based	R	Supported Interoperability Protocols: H.323, SIP, WebRTC  Audio Protocols:

#	Requirement	Priority	Notes
	videoconferencing systems and peripheral devices		<p>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</p> <p>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</p> <p>Content Sharing: H.239 (for H.323) BFCP (for SIP) VP8, VP9 (for WebRTC high framerate)</p> <p>Firewall Traversal: H323 – H.460.17, H.460.18, H.460.19 SIP/WebRTC: STUN, TURN, ICE</p>

## 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 later. 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. 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 PHI. Unlike videoconferencing events, where patient identity can be confirmed during the encounter, Health Service Providers 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. 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.

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)

Additionally, Short Message Service (SMS) or texting is not considered a secure means of communication and should not be used to transmit sensitive information and data. SMS would not meet the minimum requirements of a secure message visit.

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
<b>Patient Initiated Virtual Visit</b>	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.
<b>Clinician Initiated Virtual Visit</b>	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

#	Requirement	Priority	Notes
			infrastructure or equivalent cloud services.
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.

#	Requirement	Priority	Notes
4.2.8	Enable clinicians to initiate secure messaging virtual visits	M	Messaging must be bi-directional between clinicians and patients.
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	Solutions should allow clinicians 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	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. **Ontario Health does not collect Virtual Visit usage data. These requirements are intended to support Health Information Custodians and to provide guidance to fulfill their PHIPA audit requirements.**

The minimal requirement is an event summary that provides information about the organization, solution, modality of each unique virtual visit, unique event ID and the date 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](#) for further details.

Please note that audit logs must record and retain information about virtual visit transactions; what follows are data elements that can guide a service provider on what an audit capability should be able to retrieve.

### 5.1 Mandatory Virtual Visit Data Elements

#	Data	Requirement
5.1.1	Event ID	Unique identifier for each virtual visit
5.1.2	Solution ID	If solution provider has two or more products it must identify which product facilitated the visit. If there is only one solution this is optional
5.1.3	Event Details	<ul style="list-style-type: none"><li>• Event Start Date</li><li>• Event Start Time</li><li>• Event End Date</li><li>• Event End Time</li></ul>
5.1.4	Clinician Information (Event Host)	<ul style="list-style-type: none"><li>• First Name</li><li>• Last Name</li></ul>
5.1.5	Clinician Location (Event Host)	Postal Code or IP Address
5.1.6	Participant Location (patient)	Postal Code or IP Address

#	Data	Requirement
5.1.7	Modality Used	Video or Secure Messaging

## 5.2 Recommended Virtual Visit Data Elements

#	Data	Requirement
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	Participant Identification (patient)	Participant's name, date of birth, gender, and unique identifier i.e., Health Card Number
5.2.5	Event Outcome	Event Outcome
5.2.6	Physician Flag	Physician Flag
5.2.7	Event Type	Event Type
5.2.8	Create Date	Date the Event was created
5.2.9	Last Modified date	Date the event record was last modified
5.2.10	Event Actor	Author of the event creation or last modification

## APPENDIX

### i. All rights reserved.

This document is protected by copyright laws and treaty provisions in Canada and elsewhere. Any unauthorized copying, redistribution, reproduction, or modification (in whole or in part) of the content by any person may be a violation of copyright laws in one or more countries and could subject such person to legal action. Use of this document must comply with all copyright laws worldwide, including all measurements taken to prevent any unauthorized copying of the content contained within this document. Prior written consent of Ontario Health is required prior to the use, disclosure, or reproduction of any content in this document in any form.

### ii. Trademarks

Certain names, graphics, logos, icons, designs, words, titles, and phrases in this document constitute trademarks, trade names, domain names, trade dress or other intellectual property of Ontario Health that is protected in Canada and elsewhere.

Other trademarks, trade names, trade dress and associated products and services mentioned in this document may be the trademarks of their respective owners.

The display of trademarks, trade names, trade dress and associated products and services does not convey or create any license or other rights in trademarks or trade names. Any unauthorized use of them is strictly prohibited.