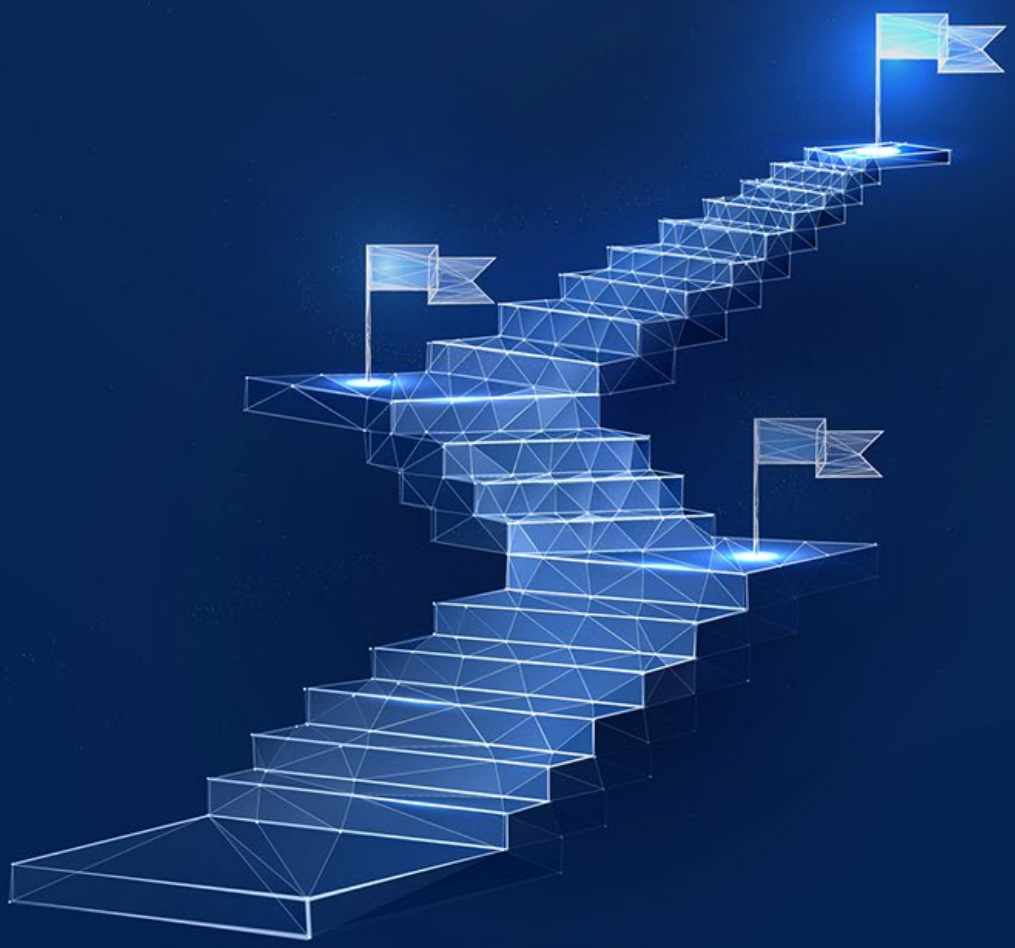


Digital Health Solutions Procurement Toolkit

March 2022 (Version 1.0)

Canada Health Infoway

Table of Contents

Disclaimer

This document represents solely the views of Canada Health Infoway (Infoway). It is based on Infoway's research and analysis as well as information from various sources. Infoway's views are based on information and analysis which Infoway believes is sound and reliable, as of the publication date of this document. Infoway's views contained in this document may be amended or updated at any time by Infoway, without notice.

This document is informative only and cannot be interpreted as providing any indication of Infoway's present or future strategies or investment criteria.

This document is provided as is. No representation or warranty of any kind whatsoever is made by Infoway as to the accuracy, infringement of third party intellectual property, completeness, fitness for any reader's purpose, or correctness of any information or other contents contained in the document, and Infoway assumes no responsibility or liability if there is any inaccuracy, infringement of third party intellectual property, incompleteness, failure to meet any reader's purpose or incorrectness with respect to any of the information or other contents contained in the document.

Infoway does not assume any responsibility or liability related directly or indirectly to the document, including without limitation with respect to any person who seeks to implement or implements or relies or complies with any part or all of the ideas, recommendations or suggestions set forth in the document.

This document does not constitute legal advice in one form or another. Organizations and individuals should seek legal counsel before determining how or whether a given law or regulation affects the implementation or operation of their solution selection process.

Infoway does not implicitly or explicitly endorse any particular technology or solution of any vendor or any other person, it does not guarantee the reliability, or any proposed results related to the use of such technology or solution and this notwithstanding that reference may be made directly or indirectly to any such technology or solution in the document.

Infoway does not make any implicit or explicit commitment of any kind or nature whatsoever to make any investment in any particular technology or solution, and this notwithstanding that reference may be made directly or indirectly to any such technology or solution in the document.

Anyone using the enclosed material should rely on his/her/their own judgment as appropriate and seek the advice of competent professionals and experts.

Executive Summary

This toolkit presents consolidated requirements that can be used for the procurement of virtual visit and remote patient monitoring solutions. These requirements were identified through consultations with executives and subject matter experts from the provinces, territories and other stakeholder groups, and represent a consolidation and expansion of existing work and artefacts developed across various organizations and jurisdictions.

In line with clinical guidelines, digital health requirements are geared towards the provision of non-emergent and non-urgent care that can be safely delivered remotely.

Acknowledgements

Canada Health Infoway would like to acknowledge all the provinces, territories, stakeholders and organizations that contributed materials to inform this document, with a special thanks to British Columbia, the Northwest Territories, Alberta, Saskatchewan, Manitoba, Ontario, New Brunswick, and Newfoundland and Labrador.

Section 1

Introduction

Section 1: Introduction

1.1 Context and Background

Since the onset of the COVID-19 pandemic, health care providers and organizations have been increasingly relying on digital health solutions to deliver care to patients. With the accelerated adoption of digital health, there is a need for guidance on vendor selection processes, including considerations for technical and non-technical business requirements.

In July 2020, Canada Health Infoway (Infoway) received the mandate from the Conference of Deputy Ministers of Health to undertake an analysis of the state of virtual visits and remote patient monitoring within jurisdictions, assessing need and opportunity for pan-Canadian procurements of new innovations.

Extensive engagement and consultation through 2020 and early 2021 resulted in the establishment of core requirements for virtual visit and remote patient monitoring solutions. To ensure a balanced perspective, these requirements were based on input from a variety of Canadian stakeholders, including leading industry experts and organizations, as well as health care administrators from across the jurisdictions.

The requirements developed through these engagements led to Infoway issuing Requests for Pre-Qualification for virtual visit and remote patient monitoring solutions on behalf of the jurisdictions, resulting in established pools of pre-qualified vendors for the jurisdictions to leverage during their individual second-stage procurement processes.

1.2 About This Toolkit

Definitions

- **Bidder** – a vendor of a solution submitting a bid in response to an RFx.
- **Evaluator** – a subject matter expert representing the Purchaser, who is participating in the evaluation of Bidders' submissions in response to an RFx.
- Handling personal information:
  - **Collection of personal information** – to gather, acquire, receive or obtain the information by any means from any source.
  - **Disclosure of personal information** – to make the information available or to release it to another person or organization.
  - **Use of personal information** – to handle or deal with the information, including accessing information for viewing purposes only.
- **Personal Health Information (PHI)** – personal information that meets the definition of "personal health information" in applicable privacy laws.
- **Personal Information (PI)** – information that either on its own or combined with other pieces of data can identify an individual, and that meets the definition of "personal information" in applicable privacy laws.

- **Purchaser** – a health care organization, agency or provider seeking to procure a digital health solution.
- **RFx** – this acronym captures all references to Request for Proposal (RFP), Request for Pre-Qualifications (RFPQ), Request for Quote (RFQ), and Request for Bid (RFB).

Intended Audiences

This toolkit has been created to support those involved in the procurement process of virtual visit and RPM solutions in understanding requirements that should be included in an RFx. Potential toolkit users may include Purchasers of virtual visit and remote patient monitoring solutions, as well as stakeholders responsible for developing requirements for an RFx and for the subsequent evaluations of Bidders' responses to these requirements.

All stakeholders involved in the procurement process should be aware of the requirements and considerations for these solutions and may find the guidance in this document useful. Bidders may also wish to use this toolkit to assist in preparing their responses to an RFx. In addition, the requirements and guidance in this document may prove useful to clinicians and other health professionals wishing to integrate new virtual visit and/or remote patient monitoring solutions into their clinical practice.

Toolkit Content

This document contains consolidated requirements for virtual visit and remote patient monitoring solutions, developed and validated with provincial and territorial representatives in 2020-2021. Users of this toolkit might wish to consider other requirements depending on their jurisdiction and the specific technology they wish to acquire for their digital health purposes.

This toolkit focuses on requirements in the following stages of the vendor selection process as part of an RFx (e.g., RFPQ and/or RFP):

1. **Mandatory requirements evaluations**
2. **Rated requirements evaluations**

For certain mandatory and priority privacy and security requirements, additional guidance has been provided for Evaluators and Bidders: i.e., guidance for those evaluating RFx submissions on how to assess Bidders' responses to the proposed requirements; or, for those who are bidding, guidance on responding to the proposed requirements. Health care organizations and/or providers may also use these Evaluator Guidance sections to inform their considerations when asking prospective Bidders to demonstrate their privacy and security compliance.

The following modules are not intended to be representative of all possible requirements, but to serve as an initial set. Specific solutions may require only a subset of requirements and/or the addition of fit-for-purpose complementary criteria to this baseline. The scope of this toolkit does not include guidance on pricing considerations for the procurement of the digital health solutions.

1.3 How to Use This Toolkit

Toolkit Sections

This toolkit is comprised of four sections:

- **Section 1:** Introduction
- **Section 2:** Virtual Visit Solutions
- **Section 3:** Remote Patient Monitoring Solutions
- **Section 4:** Privacy and Security Requirements Common to Virtual Visits and Remote Patient Monitoring Solutions

Each section contains an overview of the solution type, mandatory requirements as validated by participating jurisdictions during Infoway's previous procurement initiatives and rated requirements that may be used to further refine a Purchaser's RFx.

All users should consult ***Section 4:*** *Privacy and Security Requirements Common to Virtual Visits and Remote Patient Monitoring Solutions* in conjunction with the solution-specific sections, as the privacy and security requirements contained therein are relevant to both virtual visits and RPM solutions.

Requirement Types

Mandatory requirements include non-negotiable required functionality and/or features a Purchaser expects in a solution. Mandatory requirements must result in yes/no answers, because meeting such requirements only partially is not an option. There is no grading scale or priority rating for mandatory requirements, as Bidders can only fully pass or fail these requirements. A Bidder must provide sufficient details to demonstrate that the Bidder meets or exceeds these requirements. Bidders would not be able to move to the next stage (i.e., rated requirements evaluations) of the procurement process if they fail any of the mandatory requirements.

Rated requirements include features that are desirable but not critical for the solution. These requirements cannot be formulated as a yes/no question as they require more details to evaluate the degree of a Bidder's capabilities. Bidders should provide sufficient details to demonstrate that they meet or exceed these desirable requirements. Even though these requirements are not mandatory, they can be of high priority for Purchasers, and a Bidder can still fail the rated requirements evaluation stage if their responses do not meet the Purchaser's expectations and needs.

Requirements can include solution functionality, customization, or policies and procedures. Regardless of how capabilities are described, a Bidder should demonstrate sufficient evidence in support of their response.

Toolkit Tips

Look for this icon to quickly identify high priority rated requirements.

Requirements deemed “high priority” received strong agreement across consulted stakeholders that the requirement is foundational and essential to support minimal user needs related to a virtual visit or remote patient monitoring solution. Bidders are expected to demonstrate that their solutions support such requirements.

Look for this icon to identify requirements that cover similar topics.

Considering related requirements in conjunction with each other may help guide your RFx process.

Look for this icon to identify guidance for Evaluators.

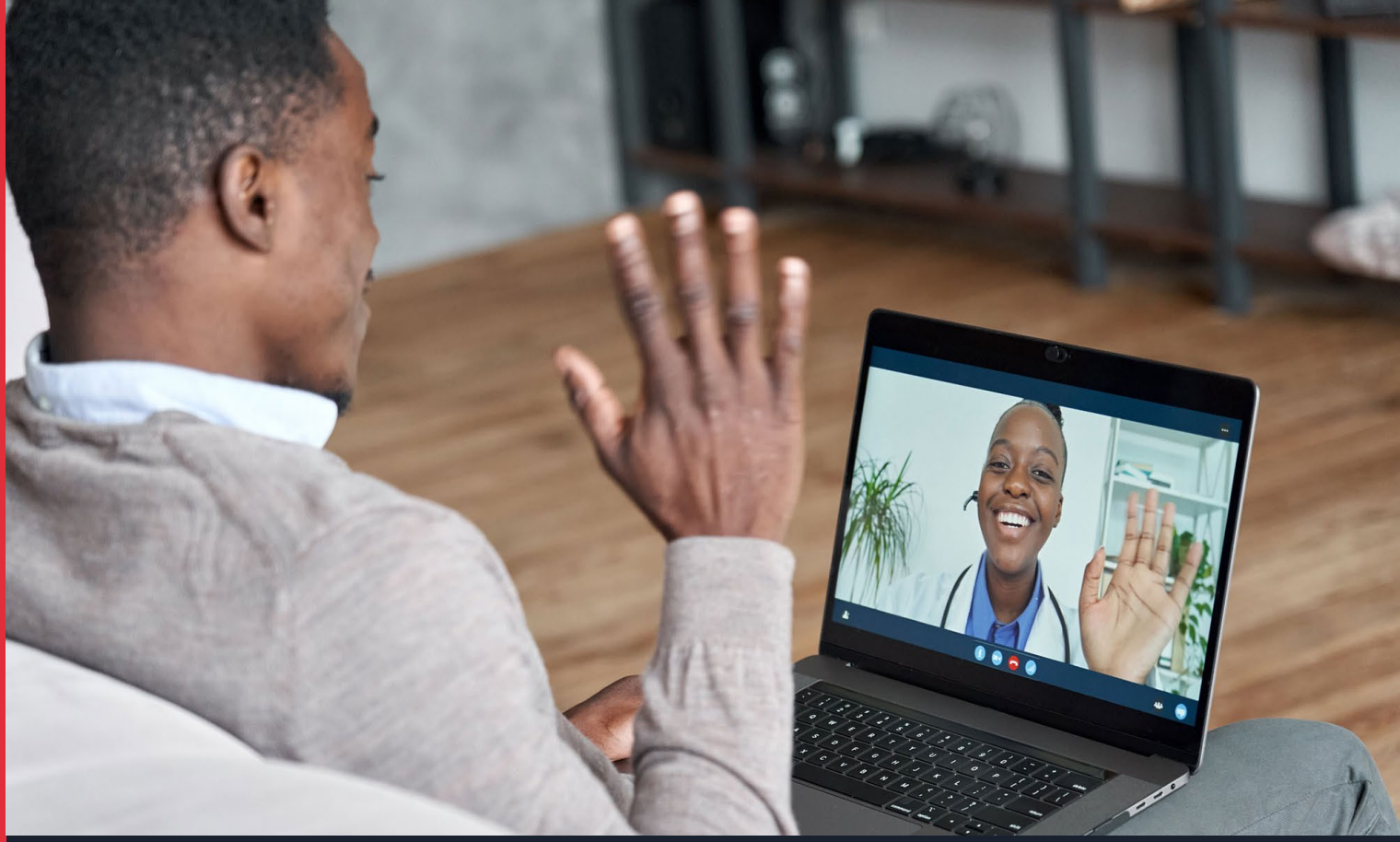
Evaluator Guidance provides additional information about how to assess a Bidder’s response to certain high priority privacy and security requirements.

Look for this icon to identify guidance for Bidders.

Bidder Guidance provides additional information for Bidders about how to respond to certain high priority security requirements.

Look for this icon to identify helpful reminders.

Reminders about key terms and concepts will help you move through the toolkit efficiently.



Section 2

Virtual Visit Solutions (Synchronous and Asynchronous)

Section 2: Virtual Visit Solutions (Synchronous and Asynchronous)

2.1 Overview

In addition to consultations by phone, providers can conduct remote clinical encounters with patients from their computers and/or mobile devices, via solutions enhanced to support synchronous or asynchronous communications.

While virtual visits can be conducted by telephone, that modality of care is not the focus of this toolkit.

Definitions

1. Virtual Visits
Clinical encounters between patients and care providers, occurring remotely, using various forms of electronic communication, such as audio, videoconferencing, secure messaging, or file exchange, with the aim of securely facilitating and maximizing the quality, efficiency and effectiveness of patient care.

Synchronous Visits	Asynchronous Visits
Involves real-time communication between clinician(s) and a patient. The patient can be at home, at another chosen location, or at a host site that may be supported by a health care professional.	Involves intermittent communication between clinician(s) and a patient, instead of real-time. Asynchronous visits are enabled by secure messaging and secure file exchange capabilities, which provide security safeguards that are not available with regular email and other unsecure forms of communications.

Synchronous virtual visits

Synchronous virtual visits are remote clinical encounters in which patients and clinicians communicate in real-time via a combination of voice and/or video and/or secure instant messaging. Synchronous virtual visits can be initiated by a patient or by a clinician and can be scheduled or ad hoc.

Types of Solutions	Description
Direct-to-Patient	A patient may participate in the visit from home or from another chosen location using a device they operate independently. Example: *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 documents the visit in their EMR.*
Supported Video Visit	A caregiver or clinician may assist the patient to access care virtually by providing a device, as well as initiating and managing the video visit. Example: *A Personal Support Worker (PSW) from a clinic schedules a video visit with a physician prior to visiting a patient at home. At the appointment time, the PSW logs into their tablet from the patient's home and initiates the video visit, which the physician joins from their desktop. Once connected, the PSW positions the tablet so the physician can interact directly with the patient. When the physician closes the visit, both clinicians document the encounter in their clinical documentation solutions.*
Hosted Video Visit	A patient goes to a secure physical environment that provides them with onsite access to technology and, in some cases, clinical support services. Such solutions support specialized peripherals to enable remote evaluation. Example: *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 a rural region. At the appointment time, the surgeon initiates the visit from their HIS calendar and the nurse connects through their room-based video system. The nurse introduces the patient and uses a medical peripheral to facilitate the surgeon's visual inspection of the surgical site. Both the surgeon and nurse document the encounter in their clinical documentation solutions.*
Group Video Visit	Video virtual visits can either be point-to-point (two endpoints) or multipoint (three or more endpoints). A single video virtual visit may be scheduled for multiple patients. Example: *A psychologist initiates a scheduled group visit as part of group cognitive behavioral therapy (CBT). Each patient logs into the hospital's patient portal and requests access to the video session. The psychologist authorizes each patient to join the session. The psychologist facilitates the group discussion. At the end of the session, the psychologist ends the session and documents the group visit in their clinical tool.*

Asynchronous virtual visits

Asynchronous virtual visits are remote encounters in which patients and clinicians exchange secure messages about a medical issue.

Types of Solutions	Description
Patient Initiated Virtual Visit	A virtual visit in which a patient initiates the request for care. Example: *A patient experiencing chills, fatigue and congestion opens an application on their mobile phone and initiates a visit by sending a message to their clinician. The patient is prompted to enter their symptoms, which are shared with the clinician. Later, the clinician reviews the symptoms and sends a response asking the patient how long they have been experiencing symptoms and what their temperature is. The patient responds with their temperature reading. The clinician advises the patient to stay home, rest and drink fluids and to schedule a follow-up visit in a week if symptoms remain. The clinician closes the visit and documents the encounter in the patient's record, including the message thread.*
Clinician Initiated Virtual Visit	A virtual visit in which a clinician initiates by sending the patient a request. Example: *A family physician receives a blood test result showing abnormal thyroid function for a patient on thyroid medication. Clinic staff use their EMR to send the patient a message advising them of the result and requesting the patient respond with information about missed doses or underactive thyroid symptoms. The patient responds the following day, reporting fatigue and constipation and asks a question about when the medication should be taken. Clinic staff engage the physician for a response. Clinic staff acts on the physician's direction to advise the patient that the physician will write a new prescription at an increased dose and that the patient can go directly to their pharmacy to fill it. The physician sends a new electronic prescription with the increased dose to the patient's pharmacy using their EMR. The physician closes the visit and documents the encounter in the patient's record, including the message thread.*

2.2: All Virtual Visit Solutions (Synchronous and Asynchronous)

2.2.1 Technical Requirements for All Virtual Visit Solutions (Synchronous and Asynchronous)

Mandatory Technical Requirements: All Virtual Visit Solutions

Requirement VV-1: Will enable service agreements for virtual visit services.

Solutions will allow providers to send and receive service agreements, instructions and other supporting materials related to registration for virtual visit services to the patient and or caregivers.

Requirement VV-2: Will support patient consent for virtual visit services.

Solutions will allow clinicians to obtain written consent or record informed patient consent to use virtual visit services to communicate medical information in the patient's medical record.

See Related Requirement PS-14: Ability/Mechanism to Record Consent.

Requirement VV-3: Will allow provider and patient to end a virtual visit.

Solutions must allow providers to determine when a virtual visit is complete. That is, solutions must not default to ending a video or secure messaging visit based on elapsed time or number of transactions.

Note that patients and/or caregivers must also be allowed to end a virtual visit; however, it will not be formally documented as a completed visit in the virtual visit solution unless the provider does so.

Rated Technical Requirements: All Virtual Visit Solutions

Requirement VV-4 Will enable patient notification when virtual visit services are unavailable.

Solutions will allow health care organizations and providers to notify patients (email or phone call) when virtual visit services are unavailable.

Potential scenarios include:

- After hours/weekends
- Vacation/leave of absence
- Technical issues
- Scheduled service updates

Requirement VV-5: Will allow provider access to visit histories and documents related to the visit.

Solutions should allow providers access to their patients' visit histories with them, along with related visit documents, such as prescriptions, requisition forms, etc.

Requirement VV-6: Will enable patient registration for virtual visit services.

Solutions should allow providers to send invitations for patients to register and will validate that invitations are received by the intended recipients. Solutions should allow patient self-registrations and the creation of user profiles.

Requirement VV-7: Will allow caregivers to manage the patient's user profile.

Solutions will allow caregivers to manage and edit a patient's user profile with the consent of the patient, or, if it has been verified, they are an authorized representative with the appropriate legal authority to do so.

Solutions will notify the patient when changes have been made to their user profile by the caregiver(s).

Requirement VV-8: Will allow caregivers to change patient's account password and authentication information.

Solutions will allow caregivers to set and change the password and authentication information of the patient's user account with the consent of the patient, or if it has been verified, they are an authorized representative with the appropriate legal authority to do so.

Solutions will notify the patient when the password or authentication information has been changed by the caregiver(s).

Requirement VV-9: Will enable end-user to share files or documentations to support the virtual visit.

Solutions will support secure content sharing relating to the encounter through screen-sharing or secure file transfers.

Requirement VV-10: Will allow patient access to visit history and documents related to the visit.

Solutions will allow patients and their caregivers access to the patients' visit histories and documents related to the visit, such as previous virtual visits with their providers.

Requirement VV-11: Will support distribution of patient surveys.

Solutions will allow providers to trigger survey distribution to registered patients 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 (i.e., at the end of a virtual visit encounter)

Requirement VV-12: Will enable patients to be accompanied by their caregivers during a virtual visit.

Solutions will enable patients to be accompanied by their caregiver(s) during a virtual visit. Bidder to describe how the solution will enable patients, caregivers and providers to participate in virtual visits, including offering a mechanism for caregivers or family members authorized by the patients to join a virtual visit.

Additional Requirements: Service Level Requirements

Requirement VV-13: Reliability

Bidder to describe service levels related to unplanned outages/service interruptions in a month and how this is maintained.

Requirement VV-14: Availability

Bidder to provide standard up time/availability to users except approved maintenance windows/planned outage and how this is maintained.

Requirement VV-15: Monitoring and Reporting

Bidder to describe health check, service monitoring and operational report generation capabilities.

Requirement VV-16: Incident Resolution Time

Bidder to describe issue resolution time SLA for high priority incidents and how this is maintained.

Requirement VV-17: Support Responsiveness

Bidder to describe how Help Desk functions, including Responsiveness SLA to customer reported issues.

Additional Requirements: Visit Documentation and Health Information Management:

Some virtual visit solutions only offer communication features and documentation of the encounter occurs in another solution such as an electronic medical record (EMR) or other clinical system.

The following requirements only apply to virtual visit solutions that offer built-in functionality for the purposes of encounter documentation and actively manage PHI linked to a specific patient record. This section also covers links between such solutions and external clinical systems to share encounter documentation or to consult health information.

Requirement VV-18: Will ensure unique identification of patients and providers.

Solutions will provide mechanisms to ensure unique identification of patients and providers in support of accurate encounter documentation.

Support provider logging into the appropriate context (e.g., providers part of more than one team).

Requirement VV-19: Will link the virtual visit to a patient record

Solutions will record sufficient information to associate the virtual visit information with a specific patient record.

A virtual visit must be linked to a patient record.

A virtual visit can only be linked to one patient record.

Requirement VV-20: Will support minimum data requirements.

Solutions will meet minimum data requirements.

Solutions may capture additional data attributes during the visit (notes or other supplemental attributes).

Requirement VV-21: Will record all messages, files exchanged with each individual virtual visit.

Solutions will record all messages and files exchanged during each virtual visit with sufficient context to meet jurisdictional auditing requirements.

Requirement VV-22: Will prevent deletion or changes to content.

Solutions will preserve all data captured, message and files exchanged during each visit.

Solutions will allow and track corrections and amendments.

Requirement VV-23: Will transfer virtual visit information to a medical or hospital record.

Virtual visit information will be transferable to a legal medical record for clinical documentation and audit purposes. Solution must support Canadian interoperability standards for this purpose.

Requirement VV-24: Will support identification of virtual visits eligible for claims submission.

Solutions will not automatically trigger claims submission for all completed encounters.

Solutions can assist clinical users to identify virtual visits that are eligible for claims (e.g., offering a "billable" vs "nonbillable" flag).

2.2.2 Privacy Requirements: All Virtual Visit Solutions

 Please see **Section 4: Privacy and Security Requirements Common to Virtual Visits and Remote Patient Monitoring Solutions.**

2.2.3 Security Requirements: All Virtual Visit Solutions

 Please see **Section 4: Privacy and Security Requirements Common to Virtual Visits and Remote Patient Monitoring Solutions** in conjunction with the requirements below.

Mandatory Security Requirements: All Virtual Visit Solutions

Requirement VV-25: Will generate a unique access code/identifier for each event.

Each session booked must be provided with a unique access code that is randomized (i.e., non-sequentially guessable).

 *Evaluator Guidance:*

The Bidder must describe how they ensure that every session is given a unique and random-access code. For example, a Bidder with a large user base would be expected to have long codes using both letters and numbers.

 *Bidder Guidance:*

The Bidder should be able to describe how they ensure that every session is given a unique and random-access code. For example, a Bidder with a large user base would be expected to have long codes using both letters and numbers.

Requirement VV-26: Will authenticate registered users prior to permitting them to join a session.

The solution must provide an authentication mechanism for registered users that is enforced prior to joining a session.

 *Evaluator Guidance:*

The solution must ensure every person has signed into the service. This helps to ensure that only invited attendees can join the session. Best responses require an account is set up with the service and enforce this feature automatically; second best responses set this configuration by default. Least preferred, but still acceptable, responses will have this as a feature that is configurable by the administrator.

Bidder Guidance:

Describe how the solution ensures that all attendees authenticate to the service before they can join a session hosted by the provider. At a minimum the solution must give the administrator a configuration option that forces all registered users to authenticate before joining a session.

Requirement VV-27: Will provide the ability for administrators to block sharing features such as chat and file sharing.

Administrators must be able to control whether chat and file sharing features are available to providers to use, as aligned with organizational expectations.

Evaluator Guidance:

The Bidder must provide the option to enforce policies related to sharing features and be able to change these policies in the future as the organizational needs change. Controls described by the Bidder must be granular such that certain types of sharing features can be permitted while others are blocked.

Bidder Guidance:

Describe how the solution provides granular controls to administrators to enable/disable sharing features within the virtual visit solution. Clearly identify if there are additional permissions granted to hosts to allow/disallow functions and if hosts can override any of the settings of the administrator.

Requirement VV-28: Will provide the ability for administrators to block content recording and processing features.

Administrators must be able to control whether content recording features are available to providers to use, as aligned with organizational expectations. Content recording and processing features include but are not limited to full audio/video recording, audio recording, session transcription, language translation, closed captioning and session chat recording.

Note that this is separate from security and privacy logging features which must be enabled (refer to respective security and privacy logging requirements).

See Related Requirement PS-25: Will generate security logs.

Evaluator Guidance:

Evaluation teams must determine first if session recording will be permitted.

The Bidder must provide the option to enforce policies related to content recording and processing features, with the ability to change these policies in the future as the organizational needs change. Controls should be granular such that certain types of content recording and processing features can be permitted while others are blocked.

Bidder Guidance:

If content recording and content processing features are available as part of the solution, provide explicit detail regarding how the solution provides granular controls to administrators to enable/disable these types of features. Clearly identify if there are additional permissions granted to hosts to allow/disallow functions and if hosts can override any of the settings of the administrator.

Requirement VV-29: Security patches and updates are provided.

Solution providers must have a mechanism that allows for notification of security updates. The solution must identify if updates are security related (or "mandatory").

Rated Security Requirements: All Virtual Visit Solutions

Requirement VV-30: Will generate additional event authentication in addition to the access code (e.g., meeting password).

To protect against unauthorized persons from joining the session, the solution should require an additional event authentication factor to enter the session (e.g., a password/passcode for the session).

Section 2.3. Synchronous Virtual Visit Solutions

Remember: Synchronous virtual visits involve real-time communication between clinician(s) and a patient. The patient can be at home, at another chosen location, or at a host site that may be supported by a health care professional.

2.3.1 Technical Requirements for Synchronous Virtual Visit Solutions

Mandatory Technical Requirements: Synchronous Virtual Visit Solutions

Requirement VV-31: Will enable synchronous virtual visits.

Solutions must allow providers to immediately initiate a synchronous virtual visit.

Requirement VV-32: Will enable multipoint synchronous virtual visits.

Solutions must support synchronous virtual visits between two or more endpoints. Endpoints may be providers, the patient or other authorized participants.

Requirement VV-33: Will provide an audio-only option.

Solution must support an audio-only option for the virtual visit. An audio visit may be an acceptable alternative if insufficient bandwidth is available to support a video visit.

Requirement VV-34: Will enable switching between video and non-video settings.

Solutions must provide the ability to toggle between video "on" and video "off" settings.

Rated Technical Requirements: Synchronous Virtual Visit Solutions

Requirement VV-35: Will provide a waiting room function for providers to screen patients/ attendees before adding them to the session.

The solution should include a waiting room or similar concept, allowing the provider (i.e., the host) to screen attendees before admitting them to the session. This is to block any unauthorized attendance and allow the clinician to control when participant(s) join the synchronous virtual visit.

Requirement VV-36: Will support one video session at a time.

Solutions will support one video session at a time. Bidder should describe how the solution only allows the provider to start a video session with a patient and/or caregiver(s) when the provider's previous video session with another patient is marked as complete and/or with explicit invitation to join the session.

Requirement VV-37: Will enable scheduled synchronous virtual visits.

Solutions will enable scheduled synchronous virtual visits. Bidder to describe how solution will allow providers to schedule a synchronous virtual visit.

Additional: Solutions will allow providers to import a scheduled event from a secured iCalendar data source.

Requirement VV-38: Will show calendar of virtual visit appointments.

Solutions will show a calendar of virtual visit appointments. Bidder to describe how solution will show providers a calendar of all virtual visit appointments:

- Participants
- Date, time, duration
- Type of virtual visit
- Reason for visit

Solutions will show patients and caregivers calendar views of previous and upcoming virtual visits:

- Providers that are/were participants
- Date and time
- Reason for visit

Requirement VV-39: Will enable configurable user notifications to alert provider, patient and caregiver.

Providers and patients will have the option to be notified when there has been a change in the status of the virtual visit. For example:

- New visit request:
  - Accepted
  - Cancelled
  - Completed
- Change in appointment time

Requirement VV-40: Will show dashboard of the virtual waiting room.

Solutions will show providers the queue of patients (anonymized) in the virtual waiting room, scheduled appointment time and wait times.

Solutions will notify providers when patients enter the virtual waiting room.

Solutions will notify patients with the estimated wait time to see their providers.

Requirement VV-41: Will support waiting room check-in.

Solutions will allow patients/caregivers to check in when they arrive in the virtual waiting room.

Requirement VV-42: Will support waiting room management.

Solutions will allow clinic administrators to perform administrative tasks such as:

- Check and validate patient's provincial health insurance plan number, address, etc.
- Verify patient's reason for visit
- Verify that relevant files and reports for the appointment has been received
- Verify that patient has passed equipment and connectivity test prior to virtual visit

Requirement VV-43: Will provide equipment and connectivity testing.

Solutions will allow patients and caregivers to perform equipment (e.g., audio and/or visual) and connectivity tests (e.g., Wi-Fi) and send reports to clinics prior to virtual appointments.

Requirement VV-44: Will provide status of action items.

Solution will allow patients, caregivers, and providers to view status of action items. Example:

- Calendar invitation has been sent
- Calendar invitation has been accepted by the patient and/or caregiver(s)
- Relevant files or data has been sent and received

Requirement VV-45: Will enable scheduled synchronous virtual visits.

Solutions will allow providers to schedule a synchronous virtual visit.

Or:

Solutions will allow providers to import a scheduled event from a secured iCalendar data source.

Requirement VV-46: Will enable bi-directional integration with provider's calendaring systems.

Solutions will enable integration with providers' calendaring systems using iCalendar (e.g., providers' calendar managed within the HIS, EMR, Outlook).

Solution will support Canadian interoperability standards for this purpose.

Requirement VV-47: Will enable patients to save a virtual visit calendar entry and URL to their virtual calendar application.

Solutions will enable patients to import a scheduled event into their calendaring systems (e.g., Google calendar, Yahoo calendar, Hotmail calendar, Outlook).

Solutions will enable patients to forward a scheduled event to caregivers to participate in the event.

Requirement VV-48: Will provide training video URL for new users.

Solutions will provide a URL to a training video for new users prior to their first visit to ensure patients and caregivers understand how to use the system.

Requirement VV-49: Will provide ability for provider to schedule a virtual follow-up visit with the patient.

Solutions will have the ability to schedule a virtual follow-up visit while in a virtual visit with a patient, or after the visit.

Requirement VV-50: Will provide adjustable video quality.

Solutions should provide users with the option to adjust the video quality setting (especially in low bandwidth environments).

Requirement VV-51: Will enable provider to initiate call or end the visit within a specified time frame.

Solutions should allow providers or delegates with configurable options for managing the virtual visit.

These could include:

- Initiating visits
- Managing participant access
- Ending the visit

Solutions should allow providers or delegates with configurable options for initiating the virtual visit and managing participant access, whether before, at, or after the scheduled appointment time.

Requirement VV-52: Will support secure file exchanges.

Solutions should support the secure bi-directional exchange of files among providers and patients and caregivers before, during, and after a video session.

Requirement VV-53: Will support screen sharing.

Solutions should be able to support bi-directional screen sharing capabilities during a video session.

Requirement VV-54: Will support remote mouse control.

Solutions will support bi-directional remote mouse control to enable and enhance interactions and therapy between patients, caregivers, and providers.

2.3.2 Privacy Requirements: Synchronous Virtual Visit Solutions

Please see **Section 4: Privacy and Security Requirements Common to Virtual Visits and Remote Patient Monitoring Solutions**.

2.3.3 Security Requirements: Synchronous Virtual Visit Solutions

Please see *Security Requirements for All Virtual Visit Solutions (Synchronous and Asynchronous)* for additional requirements.

Please consult **Section 4: Privacy and Security Requirements Common to Virtual Visits and Remote Patient Monitoring Solutions** in conjunction with the solution-specific requirements below.

Mandatory Security Requirements: Synchronous Virtual Visit Solutions

Requirement VV-55: Will provide hosts with the ability to mute, disable video and/or remove attendees.

The solution should give the host control to disable audio and video of attendees (via mute and disabling video) and to remove attendees. Removing audio, video, or overall participation of attendees gives the hosts control over unwanted disruptions/distractions. Removing unwanted individuals from a session gives hosts control over who can continue to participate in confidential conversations if multiple participants are present.

Evaluator Guidance:

The Bidder must describe how the solution allows users to control attendee presence. Controls must be intuitive for users to find when responding to a disruption/intrusion.

Bidder Guidance:

Describe how the solution supports hosts to a) manage disruptions to the session by stopping session input (audio, video, screen/file sharing) of attendees, and b) maintain confidentiality by removing attendees from a session. Clarify how the solution works and whether only hosts or both hosts and participants can use these functions.

Rated Security Requirements: Synchronous Virtual Visit Solutions

Requirement VV-56: Will provide the ability to lock the session once all expected attendees have joined.

The solution should provide functionality to block additional/unexpected people from joining or interrupting the session once it has started.

2.4 Asynchronous Virtual Visit Solutions

Remember: Asynchronous virtual visits involve intermittent communication between clinician(s) and a patient, instead of real-time. Asynchronous visits are enabled by secure messaging and secure file exchange capabilities, which provide security safeguards that are not available with regular email and other unsecure forms of communications.

Considerations for Asynchronous Virtual Visit Solutions

While providers can use general purpose encrypted messaging tools to communicate with patients, such solutions typically do not meet privacy and security requirements for the exchange of health information and entail additional work by providers for documentation and management of communications. Health care solutions must support basic messaging requirements such as the ability to compose, reply and include attachments, but other considerations come into effect:

- The flow of messages is restricted between the patient, their caregivers and specific providers.
- Ideally, asynchronous virtual visits should have a clear start and an end. The scope of the encounter is defined by a thread of messages between the clinicians and the patient.
- Providers need the ability to accept a visit request and to close the visit for documentation and/or remuneration purposes.
- Unlike general purpose encrypted messaging, the message thread must be easily ingested into the patient's legal medical record within the clinician's EMR/EHR for documentation purposes.

There are also important distinctions between the requirements for provider-to-provider secure messaging and provider-to-patient messaging (i.e., asynchronous virtual visits), but some solutions can be configured to support specific requirements for each use case.

The following requirements are specific to solutions supporting message-based virtual visits.

2.4.1 Technical Requirements for Asynchronous Virtual Visit Solutions

Mandatory Technical Requirements: Asynchronous Virtual Visit Solutions

Requirement VV-57: Will enable provider to initiate virtual visit conversation.

Solutions must enable providers to initiate a virtual visit conversation.

Requirement VV-58: Will enable patient to initiate a virtual visit conversation.

Solutions must enable registered patients to send providers a message request about a health issue or concern.

Requirement VV-59: Will enable provider to accept or decline a virtual visit request.

Solutions must enable providers or delegates to accept or decline a patient's request for a visit. Acceptance triggers the start of a visit.

Rated Technical Requirements: Asynchronous Virtual Visit Solutions

Requirement VV-60: Will support bi-directional exchanges.

Solutions will support bi-directional exchanges. Bidder to describe how solution enables patients/caregivers to send follow-up questions before the visit can be closed.

Requirement VV-61: Will allow providers to flag and filter "high importance" messages.

Solutions will allow providers to flag and filter "high importance" messages. Bidder to describe how solution has the ability to flag and filter "high importance" messages to or from patients.

Requirement VV-62: Will support read receipt before a visit can be completed.

Solutions will support read receipt before a visit can be completed. Bidder to describe how solution will confirm that medical advice has been read by the recipient before a visit can be completed by providing a read receipt.

Requirement VV-63: Will export message thread for documentation in the patient's medical record.

Solutions will export message thread for documentation in the patient's medical record. Bidder to describe how the message thread including attachments is transferable to a legal medical record for clinical documentation and audit purposes. This includes supporting Canadian interoperability standards for this purpose.

Requirement VV-64: Will allow different user roles to triage or manage patient messages.

Solution allows different user roles to triage or manage messages from patients. Bidder to describe how solution will enable health care organizations and providers to configure how patient messages are reviewed and managed. This might involve manual or automated triaging of patient requests.

Bidder to describe how solution will allow role-based access or to receive, triage, respond, forward messages, archive messages and add providers or teams to a conversation.

Requirement VV-65: Will enable capture of key information in advance of a virtual visit conversation.

Solutions will enable providers to capture information about the visit request, or send patients and caregivers standardized forms for input of key information, such as the reason for the request and complementary information.

Requirement VV-66: Will enable multiple providers to participate in a visit.

Solutions will allow other care team members to be invited to participate at any time during a visit. This can include reading or creating messages, as well as being added into a conversation or dropping out of it.

Multiple providers or delegates may be authorized to communicate with a patient (after identifying themselves) during a visit and have access to the complete message thread of communication.

Requirement VV-67: Will validate message threads being exported to the patient's medical record.

For transferring messages and attachments between non-integrated messaging platforms, solutions will validate that the content is being transferred to the correct patient medical records between the different platforms.

Requirement VV-68: Will provide "virtual front desk" capability for management of asynchronous virtual visits.

Solutions will allow providers to configure a "virtual front desk" for incoming or outgoing virtual visit messages.

Solutions will allow a provider to sign out of their account and redirect to the "virtual front desk" or delegate to an appropriate delegate.

Patient messages may be directed at a virtual clinic or service, and responses may also be sent back from the virtual clinic.

Example: a patient should be able to message an outpatient clinic (e.g., diabetes management) in which their request goes to virtual front desk for triaging before being assigned to the appropriate provider

Requirement VV-69: Will allow individual providers to designate "delegates roles."

Solutions will allow providers to designate delegate roles with various levels of permissions, such as ability to read, forward, reply, compose, end visits, export messages for documentation, archive messages, and manage mailboxes for front desk/virtual teams. The person responding to patient messages will also be identifiable by the patient.

2.4.2 Privacy Requirements: Asynchronous Virtual Visit Solutions

Please see **Section 4: Privacy and Security Requirements Common to Virtual Visits and Remote Patient Monitoring Solutions.**

2.4.3 Security Requirements: Asynchronous Virtual Visit Solutions

Please see *Security Requirements for All Virtual Visit Solutions (Synchronous and Asynchronous).*

Please see **Section 4: Privacy and Security Requirements Common to Virtual Visits and Remote Patient Monitoring Solutions**.

Section 3

Remote Patient Monitoring Solutions

Section 3: Remote Patient Monitoring Solutions

3.1 Overview

Remote patient monitoring (RPM), also known as telehomecare or home health monitoring, enables monitoring of patients outside of conventional clinical settings, such as in the home or in a remote area, to increase access to care, develop self-management skills and optimize health care delivery costs. Technology enables patients in their home to be connected to providers, and for health information (vitals, self-assessment reports, etc.) to be electronically transmitted so that providers can monitor, review, coach or modify care plans.

Such populations may include patients from a range of settings with varying health needs:

- Aging at home
- Palliative care
- Cancer care
- Long term care
- Mental health
- Perioperative monitoring

Definitions

Patients have the ability to collect their health information via peripheral devices. These peripherals may include wearables and implants, as well as external devices such as pulse oximeters, thermometers, blood pressure monitor, weight scales and glucose meters. Peripherals may fall into several categories:

- Analogue (not connected, requires manual data entry; i.e., inputting readings from an analogue weight scale)
- Digital
    - Unconnected (e.g., a digital thermometer)
    - Connected wirelessly (e.g., Wi-Fi, Bluetooth)
    - Connected by wire (e.g., USB)

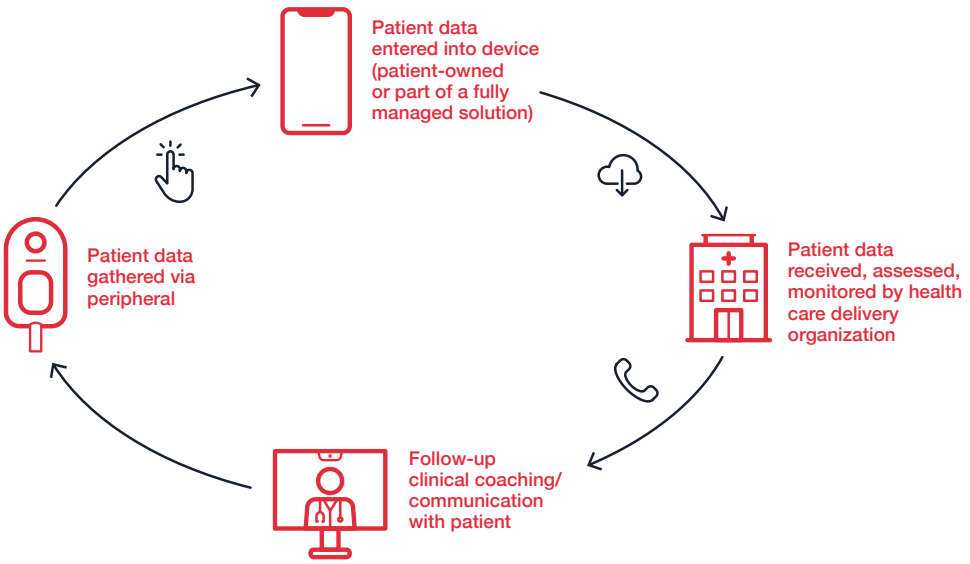
Once collected, health information is transmitted to a care provider or care team through a device which may be a fully managed aspect of the RPM solution itself, or an application installed on the patient's own device, as illustrated below:

Fully Managed Solution		Patient-Owned Device
A custom-built solution supplied, managed and maintained by a health care delivery organization and delivered to the patient. Such solutions may include:		*A "bring your own device" (BYOD) approach, using the patient's own device:*
A dedicated electronic device that communicates directly with peripherals and prompts the patient to enter symptoms through guided questionnaires.	Purpose-built tablets with custom applications to support interaction with peripherals; these tablets are typically restricted to the applications and functions necessary for the RPM program.	Applications that support interaction with peripherals are installed on a patient's device of choice (e.g., a smartphone, tablet or personal computer).

Peripheral readings and responses collected via devices may be transmitted to the clinical destination via dedicated cellular connections, the internet or phone lines. On the receiving end, the health care delivery organization can present the patient's data in their own system dashboards. Clinical care follow-up may occur through both automated and manual communication channels, including:

- Text messaging
- Email
- Phone calls
- Virtual visits (videoconferencing visits)

The RPM workflow is illustrated in the diagram below:



Use Cases

Solutions incorporating fully managed or patient-owned devices may have varying levels of suitability depending on the specific use case. For example, a patient-owned device may be appropriate for short term post-operative or COVID-19 monitoring, while a fully managed device may be preferred for longer-term chronic disease management programs.

Solutions for different use cases are stated below, but can vary across jurisdictions. Some examples include:

Types of Solutions	Description
Chronic Disease Management	A patient may record their vital statistics at home and electronically send the results to health professionals in another location. The care team regularly monitors the data and contacts patients to assess health status and progress towards health goals. Example: *A patient with diabetes monitors their vital statistics at home with a blood pressure monitor and glucometer. They regularly send their results via touch-screen tablet to a registered nurse, who provides coaching, education and support.*
Post-Operative Monitoring	A patient is discharged home following surgery and reports symptoms, vital signs and specific post-operative concerns to their care team in another location. If remote assessments are consistent with absence of infection and return to baseline activities, the patient may be discharged from follow-up. Example: *Following an appendectomy, a patient returns home. They send images of their post-operative wound to their clinician via smartphone and submit questionnaires about their recovery. They do not experience post-operative complications and complete their convalescence at home.*
Light Touch/COVID-19 Monitoring	A patient with COVID-19 records their vital signs and symptoms at home, and electronically sends the results to health professionals in another location. The care team regularly monitors the data and contacts patients to assess health status and determine treatment options. Example: *A patient is confirmed positive for COVID-19 and enters self-isolation at home. Several times each day, they measure their vital signs with a blood pressure monitor, thermometer and pulse oximeter; these measurements are sent to their care team through a dedicated app on their personal device. The health care team may also conduct telephone/virtual visits to determine if the patient is experiencing symptoms such as shortness of breath or cognitive difficulties.*

3.2 Technical Requirements for Remote Patient Monitoring Solutions

Mandatory Technical Requirements for RPM Solutions

Requirement RPM-1: Will support medical device readings.

The proposed solution(s) must support multiple medical device readings submitted by the user (e.g., blood pressure monitor, weight scale, pulse oximeter, glucometer).

Requirement RPM-2: Will assist in managing alerts.

The proposed solution(s) must rank alert severity for clinicians.

Requirement RPM-3: Will generate patient reports.

The proposed solution(s) must generate patient reports (enrollment, status, progress and discharge) and summary reports.

Rated Technical Requirements for RPM Solutions

Enrolling and Assessing New Patients

Requirement RPM-4: Will support patient self-registration.

The solution should enable patients to self-register to respond to interviews/clinical pathway and enter biometric data.

Requirement RPM-5: Will support the configuration of mandatory fields.

The solution should enable the customization/configuration of mandatory fields in various forms (i.e., patient registration).

Requirement RPM-6: Will support "bring your own device" capabilities.

The solution should have "bring your own device" capabilities with options for integrating peripherals with a person's own personal device.

Requirement RPM-7: Will enable the pairing of peripherals and smart devices.

The solution should enable patients and providers to pair peripherals, including those not supplied by the Bidder, with their own smart device to capture biometric readings.

Requirement RPM-8: Will support the capture of new referral information.

The solution should allow health care providers to capture and discretely store key information associated with a new referral for patient monitoring.

Requirement RPM-9: Will support a pre-defined workflow to onboard new patients.

The solution should help providers follow a pre-defined workflow to onboard new patients, ensuring a standardized process is followed and appropriate data is captured at each point in the process.

Requirement RPM-10: Will support the hand-off of tasks between providers within a workflow.

The solution should assist with the hand-off of tasks between providers as part of the standardized workflow (for example, the first steps in the process are handled by an administrative user, and subsequent steps are handled by a clinical user).

Requirement RPM-11: Will support assessment of patient capacities, capability and eligibility.

The solution should provide tools to help assess and document a prospective patient's clinical acuity, functional and cognitive capacity, capability and eligibility to participate in the program.

Requirement RPM-12: Will support wait list management.

The solution should provide a wait list management functionality for patients who have been referred, but cannot participate or be enrolled immediately in the program. The solution should provide various statuses for patients across multiple delivery locations.

Requirement RPM-13: Will assist with equipment management for fully managed solutions.

If the solution incorporates a fully managed (i.e., not patient-owned) device, it should allow a provider to manage device inventory and order equipment to be delivered to, retrieved from, or serviced in a patient home.

Requirement RPM-14: Will support order tracking for fully managed devices.

The solution should provide a way for the health care delivery organization to track the status of pending orders for fully managed devices and be notified at key stages where action is required on their part.

Assigning and Configuring Care Plans

Requirement RPM-15: Will support assigning and configuring care plans.

The solution should assist with the process of assigning and configuring a care plan for enrolled patients.

Requirement RPM-16: Will support alerting logic and thresholds.

The solution should support customizable alerting logic and thresholds. Patient-generated alerts, responses, including absolute thresholds and more complicated algorithms that take patient acuity or data trending into account.

Requirement RPM-17: Will support care plans for multiple comorbidities.

The solution should support assigning care plan to patients with multiple comorbidities to be monitored (for example, if a patient will be monitored for both COPD and CHF, or CHF and diabetes).

Requirement RPM-18: Will enable providers to modify a patient's care plan as needed

The solution should allow providers to modify the patient care plan and changes should be received in near real-time. This includes remote management of all aspects and content of the Monitoring Plan (i.e., patient assessments, questionnaires, educational materials, peripheral device readings and alert thresholds) and the ability to add one-time ad hoc activities (i.e., a question or device reading).

Requirement RPM-19: Will support activity prompts for clinical staff.

Health care staff can be prompted to complete certain activities at designated times or intervals during the patient's time in the program, such as coaching sessions, sending updates to the patient's most responsible provider and/or initiating pre-discharge conversations.

Requirement RPM-20: Will support notifications for offline devices and/or applications.

If a fully managed device or the application on a patient-device is offline, the care team should be notified.

Requirement RPM-21: Will support secure messaging.

The solution should support secure messaging with patients and/or caregivers at home from the clinician interface.

Managing and Tasks and Workload

Requirement RPM-22: Will support assigning clinicians to treatment teams.

The solution should support the assigning of clinicians to one or more treatment teams, so that multiple clinicians can monitor one or more patients.

Requirement RPM-23: Will display and triage patients under a provider's care.

The solution should have a dashboard that shows all the patients that are under a provider's care in a way that automatically triages them.

Requirement RPM-24: Will support workload management.

The solution should assist providers to view and manage their workload and be able to assign patients on an individual and team-based setting.

Requirement RPM-25: Will support access to external databases.

The solution should be able to access clinical providers and patient registries.

Requirement RPM-26: Will support patient medication lists.

The solution should optionally assist providers with creating and managing a list of medications currently in use by the patient or leverage existing databases.

Requirement RPM-27: Will support patient allergy lists.

The solution should optionally assist with creating and managing a patient allergies list or leverage existing databases.

Requirement RPM-28: Will support the creation of treatment teams.

The solution should support the creation of clinician and staff teams (treatment team) so that the patient(s) can be organized with the appropriate monitoring team.

Requirement RPM-29: Will support the grouping and assigning of monitoring interviews.

The solution should enable providers to group one or more monitoring interviews and assign the whole group to a patient.

Patient Monitoring

Requirement RPM-30: Will assist in identifying and managing non-responding patients.

The solution should assist coordinating providers to identify and manage non-responding patients.

Requirement RPM-31: Will support patient assessment auto-reminder.

The solution should send auto-reminders to patients to fill out and submit assessments.

Requirement RPM-32: Will support presentation of biometric data as a trend.

The solution should present biometric data as a trend, including the patient's alert threshold. Trending views of data should be configurable using time parameters and filters, and be available in Canadian values (e.g., Celsius, kgs, mmol/L).

Requirement RPM-33: Will support viewing of data from integrated peripherals.

The solution should enable data from peripherals to be viewable by the monitoring clinician without the patient having to open to send the data (i.e., the patient can use the integrated biometric devices without opening an app or software).

Requirement RPM-34: Will support patient summaries.

The solution should provide an easily accessed patient summary, displaying the key clinical and program information for patients being monitored.

Requirement RPM-35: Will support a patient dashboard.

The solution should have a dashboard for the patient to see a trend and history of their own vitals and responses.

Requirement RPM-36: Will support provider acknowledgement of patient responses.

The solution should enable health providers to acknowledge patients' responses and alerts to scheduled and unscheduled interviews.

Requirement RPM-37: Will support multi-level branching questions.

The solution should have the ability to create multi-level branching questions so that the health provider can dive deeper into the patient's symptoms, and the ability to initiate and branch questions based on the data received from biometric devices.

Requirement RPM-38: Will enable correction of patient readings.

The solution should allow providers to modify a patient's reading in order to fix any incorrect entries, and maintain a record of changes made, by whom and when.

Requirement RPM-39: Will support scheduled synchronous visits.

The solution should allow providers to schedule recurring real-time consults with patients.

See Related Section 2.3: Synchronous Virtual Visit Solutions.

Requirement RPM-40: Will support customizable assessment tools for patient consultations.

The solution should provide assessment tools to guide and document patient consults, helping them to assess the patient's overall health, trends, and issues.

Requirement RPM-41: Will support different types of questions.

The solution should support different types of questions, such as: multiple choice, free text, Likert scale/grid type, checkboxes, dropdown lists, date/time type, viewable text only (e.g., educational messages).

Requirement RPM-42: Will support the management of health improvement goals for chronic disease management.

Solutions intended for chronic disease management should assist providers with helping patients to set health improvement goals such as smoking cessation, weight loss, improved nutrition and increased physical activity; to track how well patients are progressing toward these goals; and to present progress back to patients in a meaningful and encouraging way.

Requirement RPM-43: Will support integration with existing documentation platforms.

The solution should integrate with existing documentation platforms, such as an electronic medical record (EMR).

Notifications and Communications

Requirement RPM-44: Will support customizable alerts.

The solution should provide customizable event-based notifications/alerts that are sent to the patient's circle of care. Providers should be able to select from a variety of notification options: e.g., text, email, secure messaging, etc. Alerts should also be customizable based on a program's needs and thresholds easily established at the patient level.

Requirement RPM-45: Will support multiple languages.

The solution should allow patients to view the monitoring interviews in multiple languages.

Evaluator Guidance:

Language requirements, including bilingual functionality, may differ according to jurisdiction.

Requirement RPM-46: Will support an "offline mode."

The solution should be able to operate in an "offline mode" in case a real-time connection to the network is not available, or in cases of temporary disruption.

Requirement RPM-47: Will support API protocols to extract data.

The solution should have the ability to use an API protocol to extract data from the host solution into another service for reporting purposes, including patient and provider utilization reporting.

Requirement RPM-48: Will support real-time access to patient data.

The solution should allow real-time access to patient data.

Requirement RPM-49: Will support integration with secure web portals.

The solution should provide be able to integrate with secure web portals to provide authorized members of the patient's circle of care (including informal and/or family caregivers) access to patient program and summary health information.

Requirement RPM-50: Will support video visits.

The solution should allow care providers to initiate video calls to the patient's assigned equipment.

Requirement RPM-51: Will support multipoint visits.

The solution should support multipoint messaging and/or calls.

Requirement RPM-52: Will support screen sharing.

The solution should support screen sharing to allow the clinician to share information with the patient and vice versa.

Requirement RPM-53: Will allow in-solution multitasking during video visits.

The solution should allow providers and patients to access other parts of the application while a video conference is occurring.

Requirement RPM-54: Will support options for sessions in low-bandwidth conditions.

The solution should provide the ability to have a video or audio-only session even under low connectivity locations.

Usability and Recovery

Requirement RPM-55: Will meet Health Canada Device requirements.

Provide the Health Canada classification and Medical Licence Number for each device supported by the solution.

Requirement RPM-56: Will implement CSA approved devices, or equivalencies accepted by the Standards Council of Canada.

All systems and individual components proposed that classify as electrical equipment defined by the Canadian Electrical Code must be approved by CSA or a recognized equivalent standard established under the provisions of the Canadian Electrical Code.

Requirement RPM-57: Will be easy to install, configure and use

Describe the level of knowledge required for a patient or health care provider to install and configure a medical device with minimal to no training. Describe the features that makes it easy for a patient to use the device (i.e., take measurements).

Requirement RPM-58: Will be accessible on multiple types of devices and operating systems for patients and clinicians.

The system should be accessible on desktops, laptops, smartphones (Android/Apple etc.).

Requirement RPM-59: Will support quality control by capturing the state of the medical device at the time of the reading. Describe the data elements captured.

Information about the device that records a clinical reading should be captured and associated with the reading. The information captured may include, but is not limited to:

- Device.manufacturer
- Device.manufatureDate
- Device.expirationDate
- Device.deviceName.name
- Device.modelNumber
- Device.serialNumber
- Device.safety.coding.code

Requirement RPM-60: Will implement HL7 FHIR.

The solution should implement HL7 FHIR Resources (Patient, Observation, Device) to achieve system interoperability.

Requirement RPM-61: Will support backups.

All patient data and application configuration information should be backed up. Transaction logs are backed up hourly with full database backups performed daily and weekly.

The Proponent should retain the last:

- Eight copies of daily backups
- Five copies of weekly backups
- 13 copies of monthly backups
- 10 copies of yearly backups

Requirement RPM-62: Will provide a disaster recovery plan.

A disaster recovery plan should be provided to support the RTO and RPO targets and tested at least once per year.

Requirement RPM-63: Will support extracting of reports in different formats.

The solution should allow reports to be extractable in PDF, XLSX and CSV formats.

Requirement RPM-64: Will support 24/7 client support.

The solution should provide 24/7 client support.

Requirement RPM-65: Will support a system uptime of 99.995%.

The solution should have a system uptime of 99.995%

Requirement RPM-66: Will be supported on major web browsers and operating systems.

The solution should be supported on all major web browsers and operating systems.

Requirement RPM-67: Will meet Infection Prevention and Control (IPAC) standards.

Devices and packaging incorporated as part of fully managed solutions will meet Infection Prevention and Control (IPAC) standards.

3.3 Privacy Requirements for Remote Patient Monitoring Solutions

 Please see **Section 4: Privacy and Security Requirements Common to Virtual Visits and Remote Patient Monitoring Solutions.**

3.4 Security Requirements for Remote Patient Monitoring Solutions

 Please consult **Section 4: Privacy and Security Requirements Common to Virtual Visits and Remote Patient Monitoring Solutions** in conjunction with the solution-specific requirements below.

Mandatory Security Requirements for RPM Solutions

Requirement RPM-68: Will generate security logs.

The solution must generate logs for activities of interest for security monitoring of activities in the service, including end-user devices.

 *Evaluator Guidance:*

Security logging must be available at all layers of the solution, including (as applicable) application, database, web server, operating system, etc. Alternately, security-specific solutions may be used to generate logs where equivalent or better than the source system (e.g., EDR may be sufficient to replace operating system logging).

 *Bidder Guidance:*

Describe how security logging is implemented in the solution, including details such as activities that are logged (e.g., logon/logoff, add/change/delete accounts) and layers where logging occurs (e.g., application, database).

Additional Requirements: SaaS/Hosted Solutions

Vendor hosted solutions, or Software-as-a-Service (SaaS) requires that the solution provider has secured the hosting infrastructure, and that the systems are located in secure data centers. These types of Cloud solutions are subject to infrastructure security requirements beyond what is in the general security requirements section.

Requirement RPM-69: Will ensure infrastructure supporting the solution is secured.

The solution infrastructure must be designed, deployed and managed in a secure manner.

Evaluator Guidance:

The Bidder must provide sufficient details regarding the solution such that the evaluation team can understand the various components to assess and rate the solution against security requirements.

Bidder Guidance:

The vendor must provide sufficient details regarding the solution such that the evaluation team can understand the various components to assess and rate the solution against security requirements.

Requirement RPM-70: Will monitor security.

Security logs for the hosting environment must be centrally collected and monitored.

Evaluator Guidance:

The Bidder must describe how the security logs from the backend infrastructure and security solutions are collected, how those logs are used (e.g., alerts based on predefined use cases, anomaly detection, threat hunting), the monitoring service (e.g., 24/7 security operations centre; alert-only monitoring) and how this integrates into incident response procedures.

Bidder Guidance:

Describe how security logs are collected and monitored for timely detection of security events. For example:

- Is there a dedicated SOC team?
- Is there 24x7 monitoring?
- What are the expected response times for alerts of various priorities?
- Is threat hunting conducted?
- Are these logs available to the customer?

Requirement RPM-71: Will ensure secure policies, standards and procedures are followed to secure the solution.

The Bidder, or Solution Hosting Provider, must have a security program, including policies, standards and procedures.

See Related Requirement RPM-81: Will obtain independent evaluation of security controls against frameworks.

Evaluator Guidance:

The Bidder must be able to clearly articulate what security framework they use as a basis for their security program and provide a list of security policies and standards aligned to that framework. Better responses will provide the tables of content of those policies and standards, and best responses will include complete copies of those policies and standards.

Alternate to providing copies of documentation may be to provide an externally audited report of compliance with a recognized framework (e.g., ISO27001, SOC2 Type 1 or Type 2).

Bidder Guidance:

The solution host should make these available for review by the health care provider. The Bidder may have certifications to demonstrate alignment to specific frameworks (e.g. ISO 27001, SOC2) to demonstrate the completeness of their program.

Requirement RPM-72: Will take a whole lifecycle approach to asset security.

The solution must account for security throughout the lifecycle of assets supporting the solution, including secure processes/procedures for initialization, operations, disposal, and lost/stolen devices and peripherals.

Evaluator Guidance:

Physical security of computing equipment managed by the Bidder must be in place to minimize the risk of tampering with assets. Tamper evident measures (e.g., seals) should be used on new equipment to make detection of tampering possible. The Bidder should have clear procedures for securely initializing new assets into their environment, securely operating the environment, securely wiping assets, and securely disposing of assets at end of life (e.g., secure disposal service with certificate of destruction). The Bidder should also have clear procedures for handling lost/stolen assets.

Bidder Guidance:

Describe how physical security and asset management are implemented in the environment to ensure the security of assets throughout their lifecycle. Include a description of procedures such as:

- Receiving devices and inspection for tampering
- Initialization of devices on the network
- Secure operation during use
- Secure wipe and disposal at end of life
- Lost/stolen equipment

Requirement RPM-73: Will secure privileged access.

The Bidder must have controls over administrator access, which should include privileged access management, multi-factor authentication, and strong password settings.

Provide strong password settings, and a description of multi-factor authentication approach, and if this requires third-party integrations or is native to the proposed solution(s).

Evaluator Guidance:

The Bidder must articulate how provider and patient data are protected from unauthorized access by administrators. Additionally, the Bidder must articulate how administrator access is restricted to only personnel with appropriate authorization and training, how that access is protected against unauthorized use, and how access privileges are initially granted, periodically reviewed, and revoked. Best responses will include multiple layers of additional security (e.g., multi-factor authentication, privileged access management solutions, restricted network access controls, dedicated administrator accounts, dedicated administrator access points).

Bidder Guidance:

Describe the access controls in place to prevent unauthorized access by the vendor's employees and contractors to the customer's data. Include details such as technical controls, especially regarding administrator access to the environment, and procedural controls (such as how accounts and privileges are authorized, periodically reviewed, and revoked throughout their lifecycle).

Additional Requirement: Fully Managed Solutions

The following mandatory requirement applies when the Bidder's solution includes managed devices as part of the home monitoring solutions.

Remember: A fully managed device is a custom-built solution supplied, managed and maintained by a health care delivery organization and delivered to the patient.

Requirement RPM-74: Will take a whole lifecycle approach to managed device security.

The solution must account for security throughout the asset lifecycle, including secure processes/procedures for the storage of devices pre-deployment, distribution of devices, initialization, operations, device return, data wipe/destruction, device disposal, and lost/stolen devices.

Evaluator Guidance:

Physical security of any peripherals and devices managed by the Bidder must be in place to minimize the risk of tampering with assets before and after deployment to the user. Tamper evident measures (e.g., seals) should be used on new equipment to make detection of tampering possible. Devices should have location tracking features available for the purposes of finding a lost/stolen device.

Procedures should be clearly articulated to users for a) the return of devices/peripherals, and b) reporting lost or stolen devices/peripherals. The Bidder should have clear procedures for a) handling cases of lost/stolen assets, b) to securely wipe assets (including between users and at end of life), and c) to securely dispose of assets at end of life (e.g., secure disposal service with certificate of destruction).

Bidder Guidance:

List and describe the processes/ procedures in place to ensure devices are kept physically secure through various asset lifecycle stages, for example:

- Initial delivery for setup/configuration
- Holding in storage before deployment to a patient
- Delivery to the patient
- Support for patients to provide physical security of the device (e.g., device tracing, device wipe)
- Return of device to provider
- Readying device before redeployment or disposal (e.g., secure wipe)
- Disposal/end of life

Rated Security Requirements for RPM Solutions

Requirement RPM-75: Will incorporate security testing and controls in SDLC.

The secure SDLC may be waterfall or agile methodology, and should include static code analysis, dynamic code analysis, threat risk assessment, penetration testing, secure code repository, and secure code deployment channels.

If applicable, web application testing includes OWASP Top 10.

Requirement RPM-76: Will protect patient information against loss.

Provide a description of data leakage / data loss detection and prevention tools or techniques are used to protect patient information.

Requirement RPM-77: Will ensure all people who use the solution are aware of their privacy and security responsibilities.

Training or similar guidance should be provided for administrators, users and patients/caregivers on the secure setup and operation of the platform.

Topics for patients could include secure setup of the patient account (e.g., strong password, ensuring passwords are not shared), securely connecting peripherals, and protecting the patient's device (if unmanaged). Topics for administrators should include secure configuration of the platform (e.g. enforcing password policies, setting data retention, administering user access), best practices for handling information, and administrative procedures that support security.

See Related Requirement RPM-83: Will have endpoint security controls, suitable for the managed device type.

Requirement RPM-78: Will support multi-factor authentication

Proposed solution(s) should provide the ability for users to set up multi-factor authentication as part of their profile.

Provide a description of multi-factor authentication approach, and if this requires third-party integrations or is native to the solution.

Requirement RPM-79: Will support certified peripherals.

Peripherals permitted to connect to the solution should comply with recognized standards for personal health devices (e.g., IEEE standards).

Evaluator Guidance:

The Bidder should describe how the app or web application will attempt to limit the service to only allow peripherals that are approved medical devices. This may depend on the peripheral vendor(s) and the specific checks possible for the peripheral. Note that this requirement may not be applicable if the service only collects manual input from the patient, or if it is designed to be highly open to accept any device type.

Bidder Guidance:

Describe how the solution restricts usage to permitted devices, where applicable. Provide details on what types of devices are permitted to connect by default and whether there are options for administrators to configure allowed devices and/or software can be customized to only allow specific devices.

Additional Requirements: Software as a Service (SaaS)/Hosted Solutions

Vendor hosted solutions, or Software-as-a-Service (SaaS) requires that the solution provider has secured the hosting infrastructure, and that the systems are located in secure data centers. These types of Cloud solutions are subject to infrastructure security requirements beyond what is in the general security requirements section.

Requirement RPM-80: Will have infrastructure security controls, including testing.

Infrastructure security should include configuration hardening, endpoint security solutions (e.g., anti-malware), vulnerability scanning, penetration testing, secure network architecture, secure cloud architecture, and patch management.

Infrastructure is patched and upgraded in a timely fashion.

Evaluator Guidance:

The response from the Bidder should describe how infrastructure security is implemented for their environment. The best response would include all the following:

- Endpoint security solutions: a combination of controls on the servers/containers to support the detection and prevention of unauthorized activity. This could include anti-malware/anti-virus (AV), application whitelisting, file integrity monitoring (FIM), endpoint detection and response (EDR or XDR).
- Operating system configuration hardening (i.e., to CIS benchmarks).
- For servers hosting standardized services (e.g., databases, web servers, middleware), configuration hardening of those services.

- Network architecture should show zoning based on trust levels; e.g., internal network for users segregated from infrastructure network; internet facing services segregated from non-internet facing services.
- Cloud architecture follows security best practices for that cloud provider (e.g., AWS, Azure, Google Cloud Platform) to segregate services and highly restrict access.
- All hosts are scanned for vulnerabilities at regular intervals, and the findings of these reports are acted on in a timely manner (e.g., monthly scans, with critical internet facing findings remediated within 7 days).
- Infrastructure penetration testing conducted periodically, minimum annually.
- All operating systems and software components are patched regularly.

Bidder Guidance:

Describe the security controls protecting the infrastructure that supports service, for example:

- What configuration hardening standard(s) are followed?
- What endpoint security solutions (e.g., anti-malware) are implemented for what types of devices (e.g., Windows vs Linux servers)?
- What vulnerability scanning is performed, and how frequently?
- What penetration testing is performed at the infrastructure level, and how frequently?
- How are patches deployed to the environment, and at what frequency?
- How are secure network architecture principles followed in the implementation of the network in context of the solution?
- For cloud-based solutions, how are secure cloud architecture principles implemented?

Requirement RPM-81: Will obtain independent evaluation of security controls against frameworks.

The solution host should make these available for review by the health care provider. The solution host may have certifications to demonstrate alignment to specific frameworks (e.g., ISO 27001, SOC2) to demonstrate the completeness of their program.

Evaluator Guidance:

Look for the Bidder to provide an externally audited report of compliance with a recognized framework (e.g. ISO27001, SOC2 Type 1 or Type 2). Note for all types of compliance reports, the evaluating team must review the report, and any open conditions/findings should be discussed with the Bidder to determine if they have an adequate response to concerns and action plan to address them. Review the scope of the report to determine applicability. Many Bidders simply send reports of the cloud service provider (e.g. Google, AWS, or Azure). Consider if the report is an audit of the Bidder's entire solution, or a subset.

Bidder Guidance:

Provide copies of audit reports against any recognized security frameworks (e.g. ISO27001, NIST 800-53, NIST CSF, SOC2 Type 1 or Type 2). Alternately, describe the security program including alignment to frameworks (if any) and a list of policies and standards to support the program.

Requirement RPM-82: Will provide data segregation.

The solution should be able to segregate data for different tenants.

Evaluator Guidance:

The Bidder should be able to describe how data for different customers/tenants is segregated. It is not recommended to accept a solution where no segregation of environments exists between customers, as this creates multiple challenges ensuring data is protected against accidental disclosure, as well as difficulty ensuring customer data is properly destroyed at end of use. A good response will describe an environment that has logical segregation built into the infrastructure. The best response will include fully segregated infrastructure from all other customers.

Bidder Guidance:

Describe how data is segregated for different customers, including details of how segregation occurs to ensure there is no unintended cross-over of data between customers.

Additional Requirements: Fully Managed Devices

The following requirements apply when the Bidder's solution includes managed devices as part of the home monitoring solutions.

Remember: A fully managed device is a custom-built solution supplied, managed and maintained by a health care delivery organization and delivered to the patient.

Requirement RPM-83: Will have endpoint security controls, suitable for the managed device type.

Managed devices should include configuration hardening, endpoint security solutions (e.g., anti-malware), penetration testing, patch management and firmware updates suitable for the managed device type.

Please include the Manufacturer Disclosure Statement for Medical Device Security.

Evaluator Guidance:

If the Bidder provides managed devices to patients, they are responsible for the security of the device. This may be accomplished through a) centralized management of security (e.g., using a mobile device management service (MDM)), or b) enforcement of security through periodic checks to ensure security requirements are met before permitting a connection to the central service.

For either option, the best response will include a strong technical policy checking for multiple security features, such as (but not limited to): operating system current and patched; confirmation the device has not been jailbroken/rooted; anti-malware installed, running and up to date; strong authentication

required to unlock the device (e.g., strong password with biometrics enabled, lockout after multiple failed attempts); etc. For Bidders using MDM, capabilities should also include secure wipe if the device is lost or stolen.

Any actions which are the responsibility of the patient (e.g., accepting patches and software updates) should be clearly articulated to the patient. A best answer would include training provided to the patient for any actions for which they are responsible.

Bidder Guidance:

Describe the solution(s) used to manage the security of the endpoint. For example:

- Is an MDM solution used?
- Has a set of security compliance criteria been established? If so, what are the criteria?
- Are periodic checks for compliance conducted? If so, what is the trigger for a compliance check?
- Is there a capability to track and/or wipe the device if it is lost or stolen?
- Is it clear what security activities are the responsibilities of the patient (e.g., accepting patches and updates in a timely fashion)?

Requirement RPM-84: Will generate security logs for managed devices.

The solution should generate security logs for managed devices for the purposes of security monitoring.

Evaluator Guidance:

The Bidder should describe what logs are generated on managed devices for the purposes of monitoring the security of the device. This could include software adds/changes/deletes, anti-malware detection/block/scans, user logins, security setting changes, etc.

Bidder Guidance:

Describe what logs are generated on the device for security tracking. For example, logon/logoff events, security configuration changes, software updates, security alerts, etc.

Section 4

Privacy and Security Requirements Common to Virtual Visits and Remote Patient Monitoring Solutions

Section 4: Privacy and Security Requirements Common to Virtual Visits and Remote Patient Monitoring Solutions

4.1 Context

Given certain inherent similarities in virtual visit and remote patient monitoring solutions, there are Privacy and Security requirements common to both. For ease of use, this section of the toolkit therefore includes common privacy and security requirements in the following section rather than repeating them in the solution-specific sections.

Remember: Please refer to *Section 2: Virtual Visit Solutions* and *Section 3: Remote Patient Monitoring Solutions* for additional privacy and security requirements unique to those solutions.

Privacy and security requirements should be considered in advance when procuring a digital health solution to ensure that a Bidder has adequate policies, processes, functionality and controls in place to be able to protect personal health information (PHI), prevent unauthorized activity and ensure compliance with applicable laws and regulations.

The following section provides tips and guidance on baseline common privacy and security requirements that should be considered in the procurement process of a virtual visit or remote patient monitoring solution (e.g., solutions for synchronous and/or asynchronous virtual visits between patients and care providers, remote patient monitoring and/or home health monitoring solutions).

If you have internal privacy and/or security subject matter experts within your organization, e.g., a privacy and/or security officer, they should be involved and consulted in the determination of the privacy requirements to include in the RFx, as well as further involved in the evaluation of Bidders' responses to these requirements.

4.2 Privacy Requirements Common to Virtual Visit and Remote Patient Monitoring Solutions

Mandatory Privacy Requirements

Requirement PS-1: Data Residency

PHI must be stored in Canada. Please indicate where the data will be stored. Will any PHI be stored outside of Canada?

Evaluator Guidance:

PHI must be held by systems located in Canada (i.e., hosted in Canada).

This requirement stems from Canadian legislation, as certain health information laws prohibit personal information from being disclosed outside of Canada or province(s) in certain circumstances. In some cases (e.g., Ontario) disclosures outside of a province are permitted but requires express consent of the

individual. In addition, public sector privacy laws in some provinces (British Columbia and Nova Scotia) prohibit personal information in the custody or control of public bodies from being stored or accessed outside of Canada, subject to exceptions.

When procuring a solution that processes PHI, a Purchaser should consider making Canadian data residency a mandatory requirement to validate whether or not the service provider complies with the data residency requirements in the applicable jurisdiction.

The Purchaser may wish to expand this requirement and ask Bidders to identify specifically where the data will reside, where it will be processed and accessed for PI/PHI, and who will have access (e.g., proponent, third party, subcontractor).

Requirement PS-2: Data Retention

Solution must have controls in place to retain PHI in accordance with the applicable legislation and policies of health care organizations or networks where the solution is implemented.

The technology must be configurable to adhere to different data retention requirements; i.e., the Bidder must have mechanisms in place to be able to retain PI/PHI in accordance with the applicable record-keeping requirements.

Evaluator Guidance:

Retention requirements may vary depending on the Purchaser's organization's business requirements. Retention schedules should be determined based on applicable legislation and regulations, policies and industry standards.

The solution must be able to accommodate the required retention periods either by standard functionality of the solution or customization. Personal information must only be kept for as long as required to serve the purposes for which it was collected.

If a Bidder cannot demonstrate that the solution can retain data to satisfy an organization's business retention requirements, they should not be considered further in the procurement process.

Requirement PS-3: Audit Trail/Log

The Bidder must demonstrate the solution has auditing functionality for all accesses to personal health information. The system must be able to provide/generate audit reports.

Evaluator Guidance:

Most digital health solutions should have auditing functionality available. The solution must be able to generate audit logs and produce audit reports.

Evaluators/Purchasers should consider including a mandatory requirement for auditing. In addition, it would be prudent to also include specific rated requirements for auditing (see Requirement PS-10: Audit of All Activity Involving PI/PHI). As a reminder, Mandatory Requirements are often posed as a yes/no question, which does not allow requirements to be rated based on a grading scale of not

meeting, partially meeting or exceeding the desired attributes. This differs from a rated requirement where Purchasers can ask Bidders for details about their solution auditing capabilities and how the functionality works.

See Related Requirement PS-10: Audit of All Activity Involving PI/PHI.

Requirement PS-4: Protection of Log Information

Logs must be protected against tampering and unauthorized access, and appropriate safeguards must be in place to protect sensitive information contained within the logs.

Evaluator Guidance:

Organizations have an obligation to maintain audit logs. Audit logs generated within a solution must be protected from tampering and inappropriate access to ensure logs' integrity and validity. This requirement should be a standard component of the solution's functionality.

Rated Privacy Requirements

Requirement PS-5: Compliance with Privacy Legislation and Regulations.

Describe how the Bidder ensures compliance with the Personal Information Protection and Electronic Documents Act (PIPEDA) and/or other privacy legislation applicable to the Bidder (e.g., PHIPA in ON, PHIPAA in NB, PHIA in NS, PHIA in NL, PHIA in MB).

The Bidder should include a description of how its organization demonstrates compliance (e.g., through policies and procedures, agreements in place, training, audits, external or internal assessments, etc.).

Evaluator Guidance:

A digital health solution that processes PHI should satisfy legislative requirements for how PHI should be collected, used, stored, disclosed or otherwise handled. Implementing a solution that is not compliant with applicable laws exposes you to significant privacy risk, which is why this requirement should be assigned a high priority.

Bidders should be able to describe and/or provide documentation demonstrating their compliance. Evidence of conformity may include policies and processes aimed at delivering privacy best practices, internal or external compliance audits, privacy assessments, and agreements in place.

When adding this requirement to your RFx, consider specifying which legislation and/or regulations the Bidder must demonstrate compliance with.

When completing your evaluation, consider whether the Bidder demonstrates understanding of this requirement and provides sufficient evidence of their ability to meet the necessary compliance obligations.

See **Appendix A** for a reference guide of current applicable privacy legislation by jurisdiction in Canada.

Requirement PS-6: Privacy Impact Assessment (PIA)

The Bidder should assess, by means of a Privacy Impact Assessment (PIA), the risks to personal privacy associated with implementation and/or use of the solution/technology and should implement appropriate privacy controls to mitigate identified risks. A PIA report should be up-to-date and with no major risks outstanding and should be made available to the Purchaser upon request.

If a PIA has not been conducted by the Bidder, the Bidder should be able to participate and/or cooperate with the Purchaser and their PIA process and provide all the necessary information to the Purchaser/client (i.e., implementing organization) for them to be able to complete their own PIA.

Evaluator Guidance:

A PIA is a risk management process that helps organizations identify and address potential risks and privacy impacts of programs, initiatives or solutions that collect, use and/or disclose personal health information. A PIA report documents the PIA process, including privacy analysis, identified privacy risks and recommended risk treatment plan.

A PIA is generally required for solutions that may have an impact on the PI/PHI of individuals. It will be important to determine if this requirement applies to the type of the solution or technology you wish to procure. If the solution has access and/or processes or handles PHI, conducting a PIA is an important requirement.

Did the Bidder complete a PIA to identify potential risks to the privacy of individuals whose personal health information is or will be collected, used, retained or disclosed by the solution? Are written copies of the results of the solution PIA for review? Did the Bidder mitigate major/high risks if any were identified? Review the Bidders' description and any supporting documentation provided in response to this requirement to assess if these questions are satisfied.

When determining an evaluation score, consider if the PIA or PIA results provided by the Bidder are up to date. Does the assessment represent the Bidder's current practices and solution design and functionality, and has the privacy analysis been conducted against current legislative requirements?

If relevant and/or in circumstances where PIA results could not be provided or a PIA has not been conducted yet, the Bidder should demonstrate their commitment to conduct a PIA and/or assist the Purchaser or implementing organization with their PIA process by providing all the necessary information about the solution and how they handle PHI.

Requirement PS-7: Privacy Safeguards

The solution should have administrative, technical and physical safeguards in place to prevent theft, loss and unauthorized access, copying, modification, use, disclosure or disposal of data. The Bidder should describe controls, standards and processes currently in place for safeguarding PI/PHI.

Evaluator Guidance:

To achieve a high score, a Bidder should address all aspects of the question and demonstrate that they have reasonable controls in place for all the categories including (1) administrative, (2) technical and (3)

physical safeguards. Assess if the Bidder's response contains a description or documentation of any of the following as evidence that they can meet this requirement:

Administrative Safeguards	Technical Safeguards	Physical Safeguards
► Privacy policies and procedures ► Privacy training and awareness program ► Confidentiality agreements ► Privacy impact assessments ► Internal audits and self-assessments	► Strong authentication and access controls ► Logging, auditing and monitoring ► Strong passwords and encryption ► Maintaining up-to-date software by applying the latest security patches ► Firewalls, hardened servers, intrusion detection and prevention, anti-virus, anti-spam, and/or anti-spyware software ► Threat risk assessments	► Controlled access to locations where PI/PHI is stored ► Locked cabinets ► Access cards and keys ► Identification, screening and supervision of visitors

Table 1: Examples of Administrative, Technical and Physical Safeguards

More in-depth evaluation of technical safeguards and information security controls should be done as part of the security procurement requirements evaluation process, independently from privacy requirements.

Requirement PS-8: Privacy Training and Awareness

The Bidder should require that privacy education and training and regular updates in organizational privacy policies and procedures are required of permanent and temporary employees, including third-party contractors who are registered users of the solution and have access to PI/PHI.

The Bidder should provide a description of their privacy and security awareness program and include specifics on the scope of the training (e.g., employees, third party contractors), the training content and frequency of training.

Evaluator Guidance:

The Bidder's response should include the following:

- Description of the training provided to the staff required to complete the privacy training and the frequency of the training
- Ideally, staff should be required to complete privacy training no less than once each year. Annual training should include updates on changes to Bidder's privacy-related policies and the privacy controls (including the programs and policies related thereto)
- Each new staff member should be required to complete training in accordance with the Bidder's privacy training program prior to performing any services or otherwise accessing any systems and networks in scope of the solution
- The Bidder should have a process in place for tracking and documenting privacy training completion
- Does the Bidder have any additional privacy education and awareness activities apart from mandatory orientation and/or annual privacy training?

Requirement PS-9: Privacy Incident Management Process

The Bidder should describe or provide a copy of privacy incident management process, including, but not limited to, response to reported incident and breaches, a clearly defined escalation path for individuals or reporting parties to follow, breach containment and remediation approach/procedure, and breach notification requirements.

Evaluator Guidance:

A successful Bidder should have a privacy incident/breach management protocol or procedure, which at minimum includes incident response steps such as:

1. **Breach identification and reporting**
2. **Containment**
3. **Investigation**
4. **Notification and remediation**

Requirement PS-10: Audit of All Activity Involving PI/PHI

The Bidder should describe the solution's ability to record every access, modification and disclosure of PI/PHI, together with the time and identity of the accessing user.

Indicate the type of audit reports are available and how they are generated: e.g., describe the system audit tracking and reporting capabilities.

At a minimum, audit logs should capture the following data elements:

- Date and time that PHI is accessed
- The type of data that was viewed, handled or modified in the system
- Date and time records when the user log on and off the system
- Files accessed by user
- Name of the user accessing PHI
- Name of the patient the user accessed including the relevant patient identifiers (e.g., date of birth, address, medical record number)
- Network name or identification of the device through which the connection is made
- Operations or actions that create, amend, delete, retrieve or disclose PHI (including the nature of the operation or action, the date and time of the operation or action, the name of the user that performed the action or operation and the changes to values, if any)

Evaluator Guidance:

A Bidder should describe the type of audit reports available and how they are generated (e.g., a Purchaser can generate audit reports, or the Bidder must provide the report to the Purchaser).

Solutions that actively access, capture or manage PHI must:

a. have a mechanism to record every access, use, copy, modification, disclosure or deletion of PHI

b. have a mechanism to record every access, use, copy, modification, disclosure or deletion of provider and patient data

c. where required by law, have mechanisms to alert the organisation's individual accountable for privacy when it is suspected that PHI has been accessed, used, copied, modified, deleted or disclosed inappropriately

Requirement PS-11: Data Quality and Integrity

The solution should support data quality and data integrity. The Bidder to provide a description of how data quality and integrity is ensured/supported, e.g., does the system/solution detect and have any notification/flagging to indicate to the end user when data is inputted incorrectly?

Evaluator Guidance:

At minimum, a solution should be able to support data quality through data input validation.

Quality control on data input should check for user input errors and for the following aspects of the data:

- If the data format is appropriate for the fields selected
- Completeness of the data
- Data consistency
- Data value distributions and abnormalities

The Bidder could also provide a description of how data integrity is enforced, which would differ depending on a solution. While data quality refers to whether data is reliable and accurate, data integrity means that data should also be complete, accurate, consistent and in context. Data integrity should be reinforced through solution design and architecture.

To preserve data integrity, a solution should have not only input validation, but data validation controls in place (to certify that data processes have not been corrupted). In addition, the solution should maintain access controls, consistent data backup processes, and keep audit trail/log of all activity. A Bidder could also describe their controls to prevent data duplication.

Requirement PS-12: Data Minimization

The Bidder should have mechanisms in place to only collect PI/PHI necessary to fulfill the purposes of the identified solution. Describe how data minimization is ensured.

Does the system/solution have the ability to turn off data fields to ensure limited data collection? (e.g., if a device collects data from patients, can location services be turned off?)

Evaluator Guidance:

The Bidder should minimize data collection to only what is necessary – i.e., the solution should not collect or retain more than what is needed for the specified purposes.

The Bidder should describe their practices to prevent excessive data collection, which could include:

- Clearly define and limit available data input options to prevent users from inputting too much data or data that is not relevant or necessary
- Anonymize or de-identify PHI where possible if relevant for the type and purposes of the solution
- Follow appropriate data retention and destruction schedules and practices

Note that data minimization requirement should also be documented in the contract with the winning Bidder to ensure future compliance. You could include the following statement in your Agreement with the winning Bidder: “The vendor will only use as much PHI as is reasonably necessary to perform its obligations under the Agreement and will make PHI available only to those employees who require access in order to satisfy those obligations.”

Requirement PS-13: Data Return/Destruction

Describe how the data is returned and destroyed when the contract/service is terminated.

Evaluator Guidance:

Bidders should follow data retention and disposal practices in accordance with industry best practices and applicable regulations.

Note that data return or destruction requirements should be covered in contractual obligation with a vendor, but a Purchaser should consider including this as one of the rated requirements during RFP or RFPQ process to assess if a Bidder can meet expectations. Bidders stating that they keep PHI indefinitely raise a concern as such practices are not advisable and expose purchasing organizations to significant privacy risk.

Requirement PS-14: Ability/Mechanism to Record Consent

Health care providers are required to record consent when providing or assisting the provision of care to a patient. Please describe if the solution is able to record patient's consent.

Evaluator Guidance:

A Purchaser may need a digital health solution with the ability to record patient's consent. While obtaining consent is the responsibility of a health care provider, a solution could have a mechanism or functionality in place to support required consent management practices.

A solution functionality that could satisfy this requirement would depend on the type of the solution and the Purchaser's organizational policies and procedures.

See Related Requirement PS-15: Masking/Locking of PHI.

Requirement PS-15: Masking/Locking of PHI

Patients can withdraw or withhold consent for the use or disclosure of their PHI for health care purposes, which is referred to as placing a "lock box" on PHI or "locking" or "masking" PHI (or implementing a patient's "consent directive" or "non-disclosure directive").

Solution providers should have a mechanism that allows "locking" or "masking" patient's PHI, upon patient request.

Solution providers should also have a mechanism to unmask or unlock PHI for health care purposes when access is needed:

- With the patient's consent
- In an emergency situation without the patient's consent

The reason for unmasking data should be recorded.

The Bidder to describe the solution's capabilities for masking PHI. Please describe the granularity of masking/locking PHI, how the mechanism works and who can have access to mask/lock PHI.

Requirement PS-16: User Access to their PHI

If the solution collects PHI, the solution should support patient access to their own PI/PHI that is being collected or captured. Bidder to provide description of how patients will be able to access their information.

Evaluator Guidance:

If applicable, the solution should support user access to their PHI, or assist the implementing health care provider in responding to patients' access requests by means of functionality or established operational processes. The Bidder's response should include details on how patients' right of access can be facilitated.

Requirement PS-17: Privacy Notice

The Bidder should provide a Privacy Notice/Policy for the solution, which should include a description of what kinds of PI/PHI are being collected, purposes for the collection, and how it will be used and disclosed. The Privacy Notice/Policy should also describe the general types of security measures used to protect PI/PHI within the solution.

Evaluator Guidance:

A Bidder should have documented, user-friendly and easily accessible Privacy Notice.

The Privacy Notice is typically required of the custodian to provide notice to the patient or end user accessing the solution. Depending on the solution type/functionality and on the needs and obligations of the Purchaser, a Privacy Notice may have to be developed together with the Purchaser and a solution vendor to make sure all necessary information is documented within the Privacy Notice.

If a Privacy Notice must be customized for the purposes of the Purchaser, the Bidder should demonstrate that their solution allows for customization.

Requirement PS-18: Data Correction Functionality

The Bidder should have mechanisms in place for the custodian to be able to amend PI/PHI in the record when an error is identified in the record or when an individual (i.e., patient) successfully demonstrates the record of PI/PHI is inaccurate or incomplete for the purpose. Bidder to include a description of the mechanisms in place or a description of how a record can be corrected within a solution.

Requirement PS-19: Third-Party Controls

Please describe the contractual means the Bidder has in place to provide a comparable level of privacy protection while using or engaging with a third party, such as a service provider, to process PI/PHI. The description should note if the contractual means/agreements include the following information:

a. The purpose(s) for which PHI is being shared with the third party

b. A listing of the PHI that will be shared with the third party

c. The purposes for which the PHI may be used or disclosed by the third party

d. Obligations of the third party upon termination of the agreement

4.3 Security Requirements Common to Virtual Visit and Remote Patient Monitoring Solutions

Mandatory Security Requirements:

Requirement PS-20: Will provide registered users with secure access credentials.

Solutions must provide registered users that have been authorized by the health care organizations or networks with unique identification logins and passwords.

Requirement PS-21: Will allow registered users to manage their profile.

Solutions must allow users to manage and edit their user profiles and preferences.

Requirement PS-22: Will allow registered user to change account password and authentication information.

Solutions must allow users to set and change their passwords and other authentication information.

Requirement PS-23: Will follow secure SDLC

The solution provider must follow secure software development lifecycle (SDLC) to ensure applications components of the solution are secure.

Evaluator Guidance:

The response from the Bidder should describe their development process in enough detail to understand their approach and methodology, and how security is built into key points in the lifecycle such as including security consideration in the requirements, testing software to find and remediate security vulnerabilities, and securing the code itself against tampering, loss, or destruction through the lifecycle.

Bidder Guidance:

Describe the software development lifecycle used and how security is built into key control points such as requirements and testing. Include a description of how code is managed to avoid tampering, loss or destruction. This response can be at a high level, with further details provided for the requirement "*PS-28 Will incorporate security testing and controls in SDLC.*"

Requirement PS-24: Will encrypt sensitive data throughout the solution.

Confidential and sensitive data, including PI/PHI, must be encrypted in transit and at rest for all components provided by the solution, including connections to the medical devices. This is to protect against unauthorized disclosure.

Evaluator Guidance:

Encryption in transit: The Bidder should be able to describe what encryption is used. For example, connections from devices to the backend service should meet or exceed accepted cryptography standards. If any connections are not encrypted, including within the backend network, this requirement is not met.

Encryption at rest: Every location where sensitive data is stored must have encryption to protect unauthorized access to the data outside the application. For example, backend servers may have full-disk encryption, databases may have full encryption enabled, or sensitive fields may have encryption enabled. Note that physical protection of backend services may be possibly sufficient to meet this need (e.g., highly restricted physical access to servers hosted in a secured location, coupled with strong secure disposal procedures).

NB: Where session content recording is enabled, storage of recordings is also in scope for this requirement.

Bidder Guidance:

The response should describe how security is built into the development process. For example:

- Where and how is code stored and secured?
- How is code promoted to production through a secured channel (i.e., source of code is highly restricted, authentication must occur for the code to be posted, full log of all activity, data in transit is encrypted)?
- What tools/procedures are used to discover and remediate security vulnerabilities throughout the SDLC?
- What approach is taken for code review?

Requirement PS-25: Will generate security logs.

The solution must generate security logs for activities of interest. Activities of interest for security include, at a minimum: user login and logoff; start and stop of critical services; and administrator activities such as adding/ changing permissions/ deleting users, adding/ changing/ deleting logging.

Evaluator Guidance:

Security logging must be available at all layers of the solution, including (as applicable) application, database, web server, operating system, etc. Alternately, security-specific solutions may be used to generate logs that are equivalent or better than the source system (e.g., EDR may be sufficient to replace operating system logging).

Bidder Guidance:

Describe how security logging is implemented in the solution, including details such as activities that are logged (e.g., logon/logoff, add/change/delete accounts) and layers where logging occurs (e.g., application, database).

Requirement PS-26: Will have a security incident response plan.

A security incident response plan must be in place that includes notifying customers in the event of a breach. The Bidder must describe or provide a copy of incident management response process, including, but not limited to, response to reported vulnerabilities, a clearly defined escalation path for customers or reporting parties to follow, and how reporting parties can ensure that vulnerabilities are repaired.

Evaluator Guidance:

The Bidder must articulate the steps in their incident response plan or procedure, including how incidents are classified for severity, expected response times based on severity, the criteria for notifying customers of an incident, and the timeframes for notifying customers of an incident.

Bidder Guidance:

Describe your security incident response plan or procedure, including how incidents are classified, expected response times, integration into communications plans for key stakeholders and customers, and timeframes to deliver notifications.

Requirement PS-27: Will provide role-based access control.

The solution must provide role-based access control (RBAC) with granularity of access such as:

- Read only access
- Read and write access
- No access

Role-based access controls allow permissions to be granted to a user account based on the role they will perform in the system. Examples of roles may include patient, care provider, clinician, office administrator and application administrator. Permissions are granted within the role. For example, a patient may be able to read and write data entries to their profile, while an essential care partner may only be able to read data entries. An office administrator may only be able to view patient billing information, while a clinician can view a patient's PHI.

Evaluator Guidance:

A good solution provides these roles clearly defined for the provider to use. A best solution allows the provider to further customize roles and permissions to tailor fit their setup. NOTE: Where session content video/audio recording is enabled, role-based access control is also required for access to saved content.

Bidder Guidance:

Provide the details of the roles provided within the solution and the permissions granted to each. This may be in the form of an access control matrix or similar document, which describes the roles, the functions they can perform, and the types of data they have access to.

See Related Requirement PS-29: Will provide customizable role-based access control.

Rated Security Requirements

Requirement PS-28: Will incorporate security testing and controls in SDLC

The secure SDLC should include appropriate controls such as static code analysis, dynamic code analysis, threat risk assessment, penetration testing, secure code repository and secure code deployment channels.

Evaluator Guidance:

The best response will include all the following controls:

- All code is saved in a centralized repository.
- The centralized repository has strong security controls (including access management so all changes are traceable to an individual, multi-factor authentication for internet-accessible code repositories, clearly defined process flow for promoting code from development to test to production with appropriate gates).
- Code can only be promoted to production through a secured channel (i.e. source of code is highly restricted, authentication must occur for the code to be posted, full log of all activity, data in transit is encrypted).
- Code review and approval approach is clearly documented and included in the promotion process.
- Static code analysis tools are provided to developers to readily identify security errors early as code is being written.
- Dynamic code analysis tools are used as part of the testing process.
- Periodic penetration testing of the application (minimum annually).
- Results of the latest scans and/or penetration test are reviewed by a security specialist and all issues remediated or formally risk accepted before release.

Bidder Guidance:

The response should describe how security is built into the development process. For example:

- Where and how is code stored and secured?
- How is promotion of code to production through a secured channel (i.e., source of code is highly restricted, authentication must occur for the code to be posted, full log of all activity, data in transit is encrypted)?

- What tools/procedures are used to discover and remediate security vulnerabilities throughout the SDLC?
- What approach is taken for code review?

Requirement PS-29: Will provide customizable role-based access control

The solution should provide granular role-based access control (RBAC) that can be customized by the health care provider.

Evaluator Guidance:

In addition to the "out of the box" roles, review the alignment of these roles to your organization. If custom roles are needed to align to your organization, look for customization features that support the level of granularity you require, with preference given to solutions that an internal administrator can customize.

Bidder Guidance:

Describe the default password policy and any configuration/ customization options available to the administrator. Details should cover all factors of password strength available in the solution such as length, complexity, reset function, history, lockout duration, etc. Indicate if external identity management systems are supported (e.g., can the solution leverage the provider's Microsoft Active Directory or other solution).

Requirement PS-30: Will support Single Sign-On

The solution should support Single Sign-On (SSO) for users and administrators. Single sign-on (SSO) eliminates the need for a separate username and password to be used when accessing the system. There are multiple solutions that support SSO; for example, Microsoft Active Directory Federation Services (ADFS) or Microsoft Azure AD, and Google Authenticator. SSO reduces the risk of password re-use and can provide additional security controls, such as conditional access checks and shorter session timeouts, to secure access to the service. It is also generally more convenient for users as they do not have to remember their username/password and type it in when they access the system.

Evaluator Guidance:

Review the Bidder's approach and support for SSO to ensure that it is compatible with your identity management system.

Bidder Guidance:

Describe how SSO can be leveraged to streamline access to the solution for clinical users and administrators. Include supported services and any technical considerations which must be met for SSO to function. Indicate if the support for SSO is presently available or requires development time.

Requirement PS-31: Will provide customizable password settings

The solution will support password strength and complexity settings in alignment with the provider's security policy.

Requirement PS-32: Will support two-factor authentication

Solutions will support two-factor authentication for all registered users. Bidder to describe how solution provides the ability for users to set-up two factor authentication as part of their profile.

Requirement PS-33: Will support account disabling

The solution should support disabling accounts without deleting them, for example for inactive users.

Requirement PS-34: Will provide vulnerability notifications and security updates for application components in a timely fashion

Notifications and security updates for critical vulnerabilities must be provided promptly for all components, including client software.

Appendices

Appendix A: Canadian Privacy Legislation by Jurisdiction

Jurisdiction	Health Information Legislation	Private Sector Privacy Legislation
Canada Federal		Personal Information Protection and Electronic Documents Act, S.C. 2000, c 5
Alberta	Health Information Act, R.S.A. 2000, c. H-5	Personal Information Protection Act, S.A. 2003, c.P-6.5
British Columbia	E-Health (Personal Health Information Access and Protection of Privacy) Act, SBC 2008, c. 3	Personal Information Protection Act, SBC 2003, c.63
Manitoba	Personal Health Information Act, C.C.S.M., c. P33.5	Personal Information Protection and Identity Theft Protection Act, C.C.S.M., c. P33.7 (Royal Assent received September 13, 2013 – not yet in force)
New Brunswick	Personal Health Information Privacy and Access Act, S.N.B. 2009, c. P-7.05	N/A[2]
Newfoundland and Labrador	Personal Health Information Act, S.N.L. 2008, c. P-7.01	N/A
Northwest Territories	Health Information Act, S.N.W.T. 2014, c.2	N/A
Nova Scotia	Personal Health Information Act, S.N.S. 2010, c. 41	N/A
Nunavut	Public Health Act S.Nu. 2016, c.13 In force January 1, 2020 except s.21,33,50(5)	N/A
Ontario	Personal Health Information Protection Act, 2004, S.O. 2004, c.3, Schedule A	N/A
Prince Edward Island	Health Information Act, R.S.P.E.I. 1988, c. H-1.41	N/A
Quebec	An Act Respecting the Sharing of Certain Health Information SQ 2012, c. 23	An Act Respecting the Protection of Personal Information in the Private Sector, SQ 2012, c. 73
Saskatchewan	Health Information Protection Act, S.S. 1999, c. H-0.021	N/A
Yukon	Health Information Privacy and Management Act, SY 2013, c. 16	N/A

Table 2: Canadian Health Privacy Laws by Jurisdiction*

**Current as of February 2022*

[2] Within this table, whenever N/A (not available) is indicated, it means that the province or territory does not have their own local privacy law for that category and hence the federal privacy law applies there instead – i.e., Personal Information Protection and Electronic Documents Act, S.C. 2000, c 5 (PIPEDA).

Appendix B: Consideration of Privacy Requirements as Contractual Obligations

Upon successful completion of the RFx evaluation process, the Purchaser will enter into an agreement with the winning Bidder(s) henceforth referred to as a Vendor.

A contract between the Purchaser and the Vendor for provisioning, developing or delivering a digital health solution should include an Information Practices or Privacy Schedule with privacy and information protection obligations outlined.

The checklist below includes common contractual privacy terms or obligations that the Purchaser may wish to consider including in their Agreement with the Vendor. Note that this is not an exhaustive list of contractual provisions that should be considered when drafting an Agreement. Both parties should involve their Legal Counsel in negotiating the contractual provisions to ensure that all the terms and obligations are clearly outlined and reasonable.

A Checklist of Contractual Privacy Obligations for Consideration:

Contractual Obligation	Category	Corresponding Privacy Requirement, if applicable	Included in the contract? (Yes/No)
The Vendor will only use as much PHI as is reasonably necessary to perform its obligations under the Agreement and will make PHI available only to those employees who require access in order to satisfy those obligations.	Collection, Use and Disclosure of PHI	PS-12	
The Vendor will only use and disclose any PHI it receives from the Purchaser as is permitted or required under the Agreement or the laws applicable to the Purchaser.	Collection, Use and Disclosure of PHI	PS-5; PS-12; PS-19	
The Vendor will ensure that any of its agents or subcontractors to whom the Vendor provides the Purchaser PHI has agreed in writing to the same restrictions and conditions that apply to the Vendor with respect to PHI.	Collection, Use and Disclosure of PHI	PS-7; PS-12; PS-19	
The Vendor will not disclose PHI, or any information, to any affiliated or unaffiliated third party without the prior written consent of the Purchaser.	Collection, Use and Disclosure of PHI	PS-19	
The Vendor will maintain a log of access and disclosure of PHI by the Vendor and the Vendor's personnel and make such log available to the Purchaser as and when requested.	Collection, Use and Disclosure of PHI	PS-3; PS-4; PS-10	

Contractual Obligation	Category	Corresponding Privacy Requirement, if applicable	Included in the contract? (Yes/No)
The Vendor will employ appropriate safeguards to prevent theft, loss, and unauthorized access, copying, modification, use, disclosure, or disposal of PHI.	Protection of PHI	PS-7	
The Vendor will maintain privacy policies in accordance with Canadian and provincial and/or territorial laws applicable to the Purchaser, and these policies will be made available for inspection on request.	Protection of PHI	PS-5	
The Vendor will educate its employees on applicable privacy laws and policies and take reasonable steps to ensure employee compliance through staff training, confidentiality agreements, and employee sanctions.	Protection of PHI	PS-7; PS-9	
The Vendor will ensure that all employees who have access to PHI from the Purchaser have undergone screening that includes reference checks.	Protection of PHI	PS-7	
The Vendor will ensure that its employees who are fired, resign, or no longer require access to PHI from the Purchaser return all PHI to the Purchaser and can, thereafter, no longer access submissions, hardware, software, network, and facilities belonging to either the Vendor or the Purchaser.	Protection of PHI	PS-7	
The Vendor will revoke any user's access to PHI if privacy and/or security is breached and on the Purchaser's reasonable request.	Protection of PHI	PS-7; PS-9	
At the termination of the Agreement, the Vendor will return or destroy all PHI received from, created, or received by the Vendor on behalf of the Purchaser that the Vendor maintains custody of in any form and will retain no copies of PHI thereafter. The Vendor will certify to the Purchaser that all such PHI has been returned or destroyed, as the case may be. If such return or destruction of PHI is not feasible, the Vendor will notify the Purchaser of this fact, extend the protections of the Agreement to all PHI in your custody and will cease all further uses and disclosures.	Protection of PHI	PS-13	
The Vendor will provide the Purchaser with the name of a contact person at the Vendor's organization responsible for the Vendor's privacy compliance and notify the Purchaser within 24 hours of any changes in the identity of the responsible person.	Notification of and Communication with the Purchaser	PS-5; PS-7	

Contractual Obligation	Category	Corresponding Privacy Requirement, if applicable	Included in the contract? (Yes/No)
The Vendor will report to the Purchaser's Privacy Office at the Vendor's first reasonable opportunity, but in any event no more than 48 hours after the Vendor becomes aware of any loss theft, or unauthorized access to, or use or disclosure of PHI (including being legally compelled) by the Vendor or any of the agents or subcontractors with access to the PHI.	Notification of and Communication with the Purchaser	PS-9	
The Vendor will refer anyone trying to access, correct, or complain about their PHI to the Purchaser's Privacy Office within 48 hours of receiving the complaint or request for access or correction. The Vendor will cooperate with and assist the Purchaser in the management of any such request for access or correction or complaint.	Notification of and Communication with the Purchaser	PS-16	
The Vendor will, upon request, make PHI available to the Purchaser for amendment and incorporate any amendments into the Vendor's records of PHI. During the term of the Agreement, the Vendor may never deny the Purchaser access to its patients' PHI.	Notification of and Communication with the Purchaser	PS-18	
The Purchaser reserves the right to: inspect any goods used or records maintained by the Vendor in connection with the provision of goods or services; question the Vendor's personnel regarding their handling of PHI; and otherwise audit and verify compliance with these practices.	Notification of and Communication with the Purchaser	PS-6; PS-7	
Notwithstanding anything else contained in the Agreement, the Vendor authorizes, acknowledges, and accepts termination without notice of the Agreement by the Purchaser if the Purchaser determines the Vendor has violated any of these practices.	Additional Purchaser Rights		
All of the privacy terms in this Agreement survive the termination of the Agreement.	Additional Purchaser Rights		
The Purchaser reserves the right to go to court to obtain an order stopping or preventing the Vendor from violating the privacy terms in this Agreement. The Vendor acknowledges that any breach of these practices will result in the Purchaser suffering irreparable harm.	Additional Purchaser Rights		

Canada Health Infoway

Get in touch

RFPQtoolkit@infoway-inforoute.ca

www.infoway-inforoute.ca