Online Appointment Booking

Service Standard Final Version 1

March 2021

TABLE OF CONTENTS

Appendix

i. Acknowledgements

The requirements listed in this document are informed by other provincial standards, including the Virtual Visits Solution Requirements https://otn.ca/verification/ and have been reviewed by many health care organizations, clinician leaders, regional leaders, and internal experts.

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

Dr. Neil Naik, West Region
Dr. Paul Gill, West Region
Dr. David Daien, Central Region
Rodney Burns, CIO Alliance for Healthier Communities
Dr. Yoel Abells, Toronto Region
Kevin Chung, Project Director, Sunnybrook Health Sciences Centre
Justin Saindon, Senior Project Manager, Digital Health, Southlake Regional Health Centre
Julie Swedak, Director of Quality & Knowledge Management, Gateway Community Health Centre
Bruce Pye, Shared Regional CIO / IT Advisor
John Brunetti, RN, Primary Care Manager, Espanola Regional Hospital and Health Centre
Donald Stokes, Regional and IT specialist
Dave Speedy, Senior Director IT, Digital Health & Transformation, West Region
John McKenna, Patient Representative

Canada Health Infoway
Online Appointment Booking Vendors

Ontario Health would like to thank Ontario MD, as a significant partner in the development of the standard.

ii. Disclaimer

This document relates to, but is not specific to, the provincial services of Ontario Health or other provincial health organizations. The standard detailed in this document is a non-normalized standard and therefore errors, omissions and revisions may occur. This document is provided purely as a guide, and not intended to be, nor should it be deemed: (i) a replacement for due diligence; (ii) an alternative to procurement in accordance with any legislation and regulations by which you are governed; or, (iii) legal advice. Ontario Health encourages you to conduct your own due diligence and engage your own advisors and legal counsel as you deem appropriate. Ontario Health assumes no legal liability for your election to use this document in any way.

1.0 Introduction

Booking a healthcare appointment online is less common in Ontario than it should be. In 2014 Canada Health Infoway conducted an in-depth analysis, and, at that time, results indicated fewer than 10 percent of Canadian Physicians offered OAB while over 90 percent of Canadians said they would book a medical appointment online if the option were available. [1]

In 2019, the Ministry of Health launched a new Digital First for Health Strategy for Ontario to modernize the patient experience and help end hallway health care. There are five pillars of the strategy—and online appointment booking is one of them.[2] OAB is an "option" available to patients, and the goal is not to discontinue telephone appointments.

Offering OAB to book health care appointments may decrease providers' no-show rates, amount of time administrative staff(s) is on the phone and improve office efficiency.[3] OAB can improve the experience of the patients and caregivers by helping them view available times from which they can select an appointment that is most convenient to their schedule, spend less time back and forth with office assistants, and receive timely confirmation and reminders prior to the appointment –all of which reduce no-shows.

The purpose of this standard is to facilitate the selection and implementation of digital OAB solutions. This service standard describes mandatory and recommended general functional and non-functional requirements for digital solutions used by health care organizations and clinicians to support patient-initiated OAB. These requirements define minimum requirements for secure, patient-centric solutions; and do not attempt to define requirements for every possible function of OAB solutions.

Health care organizations, including OHTs seeking to implement an OAB application for primary and community-based specialty care, can refer to this document to support their education and decision-making prior to procuring and implementing an OAB service. Organizations selecting an OAB solution should consider impacts to administrative and clinical workflows, patient experience, privacy and security, and analytics and reporting—all of which this document will cover.

Intended audiences for this document include: OHTs, health care organizations, primary care physicians, OAB vendors, Point-of-Service (PoS) application providers, and non-clinical users.

For information regarding Virtual Visit standards for video and secure messaging please refer to the Virtual Visits Solution Requirements Version 1.1.1 at https://dw9n3hga5m4wq.cloudfront.net/wp-content/uploads/2020/03/virtual-visits-solution-standard1-1-1-1.pdf. A standard is being developed for patient portal and once it is published a link will be provided here.

[1] Canada Health Infoway, 'Exploring the value, benefits common concerns of e-booking White Paper Full Report', *Canada Health Infoway,* 2014, page 4, https://www.infoway-inforoute.ca/en/component/edocman/supporting-documents/1832-exploring-the-value-benefits-and-common-concerns-of-e-booking?Itemid=101 (assessed 2 March 2021).

[2] Ministry of Health, 'Connected Care Update', *Ministry of Health*, 2019, http://www.health.gov.on.ca/en/news/connectedcare/2019/CC_20191115.aspx (assessed 2 March 2021).

[3] Cassandra Fraser, Canada Health Infoway, Keith Chung, Magenta Health, Dr. Boris So, Patient Health Networks, 'Patient E-Booking Practice perspectives on the benefits, challenges and lessons learned', *Canada Health Infoway,* 2015, slide 11, https://www.infoway-inforoute.ca/en/component/edocman/resources/2717-patient-e-booking-practice-perspectives-on-the-benefits-challenges-and-lessons-learned?Itemid=101 (assessed 2 March 2021).

2.0 Definitions

1. Online Appointment Booking

Online appointment booking (OAB) solutions allow patients and caregivers to book an in-person, video, or telephone appointment electronically, by choosing a date and time and receive an automated appointment confirmation, with limited to no interaction with another person. Appointment reminders are automated either by email, text message, app notification or voice recordings.

Email addresses and online enquiry forms are not OAB solutions, as they require human interaction to confirm appointment availability.

2. Point of Service

A Point of Service (PoS) application is software used by clinicians and their administrative staff for the administration and provision of patient care. Primary care and community care Electronic Medical Records (EMRs), Hospital Information Systems (HIS), and Clinical Information Systems (CIS) are all examples of PoS solutions. A growing number of PoS software vendors are offering integrated OAB solutions. The OAB solutions are only available to their existing customer base (i.e., not sold as a standalone product), and are sometimes integrated into the patient portal solutions provided by the PoS vendor.

3. Standalone Solutions

Standalone OAB solutions are cloud-based software designed specifically for patient-initiated OAB. These solutions may offer integration with PoS applications used by physicians in Ontario.

4. Mandatory

Mandatory (M) refers to an OAB requirement that must be met.

5. Recommended

Recommended (R) refers to an OAB requirement that would be optional but that is recommended.

6. Roster

Rostered patients are individuals the provider or clinic considers to be its patients.

7. Enrollment

Enrollment refers to individuals that have been formally registered by the provider with the Ministry of Health as part of a specific primary care payment model (e.g., capitation, enhanced fee-for-service, etc.)
http://www.health.gov.on.ca/en/pro/programs/pcpm/

3.0 Use Cases

The following use cases provide example scenarios illustrating the use of OAB software by different types of users. These examples are not exhaustive and do not represent all possible use-case scenarios.

Patient

1. *A patient and/or caregiver needs to book an appointment for their dependent today. The patient uses her mobile device to log into the booking system, chooses an available time quickly and easily with the provider. The patient could not find the exact reason for visit but was able to type in the concern. She receives a confirmation of appointment and a reminder notification prior to the appointment.*

2. *A patient would like to book a follow-up appointment to discuss the x-rays from last week. While using his work computer, he accesses his medical clinic's website and chooses from the available dates and times for an appointment next week. Unfortunately, the patient's work schedule has changed, and he must cancel his follow-up appointment and find a new time. He easily cancels his appointment from the confirmation text and has the option to pick a new time that meets his needs.*

Primary Care Provider

1. *The provider's EMR schedule is integrated with the OAB solution, which enables flexibility for both the provider and administrative staff. The provider can easily customize dates, times, length of visit, patient access, and reason for visit, as well as embed rules to support equal access to appointments. The provider can customize each available time slot to be in-person, video, or a phone appointment.*

Administrative Office Assistant

1. *The office assistant receives the clinic's new schedule for all the providers. She makes the changes quickly in the EMR to reflect all the providers' changes. These changes are automatically reflected in the OAB solution.*

2. *The office assistant receives an internal message from the physician in their EMR to book an appointment for a patient. The office assistant contacts the patient and books an appointment directly in the EMR. This appointment time will automatically be blocked off in the OAB solution and not be available for other patients.*

4.0 Online Appointment Booking Requirements

The following sections contain tables of requirements that use the following column headings:

- # - the unique requirement ID
- Requirement – a statement describing a need that OAB solutions will have to satisfy.
- Priority – indicates the importance of the requirement where "M" = mandatory or "R" = recommended
- Notes – additional information or guidance to help interpret the requirement.

4.1 Usability

#	Requirement	Priority	Notes
4.1.1	Enable patients and/or caregivers to select an appointment for a specific day and time.	M	The available appointments displayed to patients must be updated on a near real-time basis based on each clinician's availability
4.1.2	Enable patients to view in-person or virtual appointment options.	M	Solutions must be capable of displaying appointment options (in-person, video, or telephone) offered by the clinical user to patients prior to their appointment selection.
4.1.3	Send an automatic appointment confirmation to the patient.	M	Solutions must be able to automatically notify patients that the appointment they selected has been confirmed within the clinician's schedule.
4.1.4	Meets AODA Level AA compliance.	M	This level of compliance is mandatory by June 30, 2021. For example: Support patients with vision impairments

#	Requirement	Priority	Notes
4.1.5	Enable a mobile and web interface that is device agnostic.	M	Designed to be displayed clearly in mobile device browsers or provides a mobile app.
4.1.6	Ability to track online booking statistics	M	Solutions should be able to report, for example: • Number of unique online appointment bookings. • Number of unique patients who booked an online appointment. • Number of patients who registered for OAB. • Percentage of total appointments that were booked online based on total available for booking online. • Number cancelled/rescheduled by patient or provider.
4.1.7	Enable patients to download the confirmed appointment to a calendar.	R	The patient should be able to "add to calendar" from a link within the confirmation email or screen.
4.1.8	Provide a user interface in either English or French for patients.	R	Both English and French are official languages of Ontario.
4.1.9	Enable a multilingual patient interface.	R	Supports languages other than English and French.

4.2 Booking Rules

#	Requirement	Priority	Notes
4.2.1	Enable patients and caregivers to view appointment types when selecting an appointment.	M	Solutions must be capable of displaying sufficient information to patients to enable them to make an appropriate appointment.

#	Requirement	Priority	Notes
			Examples of appointment types: - New Onset Issue - Blood Pressure Check - Diabetic Counselling - Follow Up - Well Child Check
4.2.2	Enable patients and/or caregivers to view appointment duration when selecting an appointment.	M	Solutions must be capable to display different appointment durations. For example: 10 min. appointment 15 min. appointment 20 min. appointment
4.2.3	Enable patients and/or caregivers to schedule, modify or cancel appointments from the OAB solution.	M	For example: a parent can book an appointment for their child or a caregiver (child) can book an appointment for their parent.
4.2.4	Enable clinical users to customize the appointment types, durations, and modalities that are available for online booking.	M	Robust appointment type/reason selection avoids needing to follow up with a patient due to booking an incorrect appointment type with a duration or modality (e.g., in-person, virtual, etc.) that is not appropriate for the patient's needs.
4.2.5	Enable physicians to open specific appointment times in the calendar for online bookings.	M	This allows providers to easily provide periods of appointment times.
4.2.6	Ability to allow for recurring day and time blocks for online booking.	M	For example: Mon, Wed, Fri mornings are available for OAB.
4.2.7	Enable a clinical and/or non-clinical users to approve or decline appointments before they are confirmed.	M	While a goal of OAB solutions is automatic scheduling of requested appointments in a provider's schedule, there are use cases where it is in the patient's best interest to allow clinical and non-clinical users to review the appointment request prior to confirmation.

#	Requirement	Priority	Notes
4.2.8	Enable appointment booking options to be configurable based on patient enrolment status.	M	Enrollment means patients enrolled by a provider to the MOH as part of a primary care payment model (e.g., capitation, enhanced FFS). *A provider should be able to restrict walk-in appointments*
4.2.9	Enable clinical and non-clinical users to reflect changes in the schedule like vacation coverage, after-hours clinics, specialty clinics (e.g., flu shot clinic).	R	Enable the solution to display clearly to patients/caregivers when times and/or blocks of time are available.
4.2.10	Enable mass cancellations of appointments from an OAB solution and/or from the EMR	R	The OAB can either allow users to do mass cancelations from within the OAB or the OAB can receive mass cancelations from the EMR and trigger the appropriate cancelation notifications.
4.2.11	Enable clinical users to customize booking rules.	R	For example: frequency of appointments.

4.3 Notifications

#	Requirement	Priority	Notes
4.3.1	Enable automatic sending of reminders using one or more of the following notification channels of SMS, email, and voice for upcoming appointments to patients	M	The solution can send out appointment reminders automatically, without the need for intervention by clinic users.
4.3.2	Enable patients to choose their preferred notification channels.	M	If the solution supports multiple notification channels, the patient can select the best modality to receive notification.
4.3.3	Enable patients to cancel appointments from a reminder notification.	M	The patient-facing component of the solution enables patients to easily cancel an appointment with little to no instructions from the reminder.

#	Requirement	Priority	Notes
4.3.4	Enable any cancellation rules to be configurable and clearly displayed to the patient.	M	Patients to be informed of any specific instructions up-front prior to cancellation. Example: fees for late cancellations
4.3.5	Ensure email and SMS notifications do not provide any personal health information (PHI) about the appointment. Information included in emails and SMS must be limited to minimum information to advise the patient of an appointment.	M	Electronic notifications can only provide general information about the appointment (i.e., date and time). The end-patient should be made aware that limited PI/PHI may be sent through the Canadian Anti-spam Legislation (CASL) consent and adding to patient-facing FAQs.
4.3.6	Enable clinical and non-clinical users to modify an existing appointment.	R	This can include an office assistant.
4.3.7	Allow patients and caregivers to attach and send files to allow clinicians to prepare in advance of the appointment	R	Solutions capable of allowing attachments of documents for both the clinic and patient and caregiver. For example: forms, communications, questionnaires.
4.3.8	Enable customization of content for all types of notifications.	R	Allows instructions to be communicated to the patient and enables patients to differentiate between multiple notifications. Can include embedding links in email and SMS notifications.
4.3.9	Enable the sender to customize the information in a notification the patient will receive and see.	R	Configuring how the patient sees the information will help patients differentiate notifications from unwanted communications (e.g., spam). Voice: The solution should be able to configure the call display name. SMS and email: The solution should be able to configure the sender number or email address

4.4 Interoperability

At the time of publication of the Online Appointment Booking Service Standard V1, an interoperability standard for OAB for Ontario is not available. However, Ontario's direction is to base provincial standards on the HL7 FHIR standard for appointments.

Future work to address interoperability standards development activities to formally define and publish the health information exchange specifications will enable interoperability between OAB solutions and other applications. Vendors and health service providers will be advised of future updates.

Organizations pursuing an Online Appointment Booking solution should consider the current interoperability capabilities and roadmap when evaluating a vendor solution. Online Appointment Booking sits in a broader context of EMRs, HIS systems, other Point-of-Service applications, and Patient Portals. Meaningful integration of an OAB solution into this broader context will be necessary to maximize productivity and optimize the patient experience.

#	Requirement	Priority	Notes
4.4.1	Enable an OAB solution to integrate with a PoS for appointment booking for the two-way exchange of data in near real time.	M	For example: providers' calendars in their EMR are updated as patients book appointments, and patients see available time slots as providers make changes to their calendar
4.4.2	Enable patients to view confirmed appointments in the OAB solution.	R	For example: a list, a calendar
4.4.3	Enable a provider to have access to multiple PoS using one OAB solution	R	A care provider who works at multiple clinics with potentially different EMRs and at different locations

5.0 Privacy and Security Requirements

Privacy

Online Appointment Bookings involve the collection, use and disclosure of personal health information (PHI) and personal information (PI). As a result, organizations and clinical users delivering bookings must ensure their operations are compliant with the *Personal Health Information Protection Act, Freedom of Information and Protection of Privacy Act* and other relevant legislation.[4]

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

Booking

- Scheduling confirmation or reminder includes unauthorized PHI access
- Wrong patient being invited to participate in an appointment
- Sharing information for the wrong patient during a booking
- Messages sent to the wrong patient
- Unauthorized clinical users reviewing patient requests and messages without their consent
- Unauthorized clinical users copied on a message sent to a patient

Organizations and clinical users can mitigate many of these risks by implementing appropriate privacy and security policies, procedures, and practices. Certain risks can also be mitigated by selecting OAB solutions that meet a minimum set of privacy and security requirements outlined in this section. This includes taking reasonable steps to confirm that technologies used by patients permit PHI to be shared in a private and secure manner[5].

Information Security

Health care organizations and clinical users should ensure their OAB solution providers will deliver information security services as part of their service obligations. For example, solutions must have information security safeguards, such as access to controls, security incident response procedures, encryption, logging and monitoring, secure operational procedures, and other mechanisms to protect the confidentiality, integrity, and availability of data.

.

Online Appointment Booking providers' information security services will comply with applicable requirements described in the Ontario Health EHR Security Toolkit[6] which is aligned with OntarioMD's EMR Hosting Requirements.

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

#	Requirement	Priority	Notes
5.1	Publish a notice of its information practices relevant to its virtual OAB solution and services.	M	At a minimum, the notice must describe how the vendor handles and protects personal health information and the rights of patients

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

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

[6] (https://www.ehealthontario.on.ca/en/support-topics/EHR-security-toolkit/policies-and-standards)

			and caregivers in the context of all applicable legislations (e.g., PHIPA, CASL, etc.).
5.2	Enable the collection of patients and/or caregiver consent as required to meet applicable legislation.	M	OAB solutions will need to capture consent from patients and/or caregivers depending on OAB solution functionality and design. Examples may include: • Consent to receive email/text notifications (Canadian Anti-Spam Legislation) • Consent to exchange PHI (e.g., submitting an OHIP number would require consent under *PHIPA*) • Consent to use de-identified PHI (e.g., Under *PHIPA*, the creation of deidentified information is considered use of PHI. This use must be communicated to patients (through consent) and HCPs (Terms of Use) for permission. *PHIPA* does not specify what vendors can do with deidentified information; PHIPA does require that the ability to reidentify the individual is mitigated). • Vendors should have policies and procedures that reference deidentification/aggregation of data, including method, use, and sharing; the procedures should specify how they prevent re-identification.
5.3	Have a designated employee responsible for privacy.	M	Contact information for the designated privacy official must be publicly accessible on the vendor's website.
5.4	Have a privacy and security program that includes policies and procedures.	M	At a minimum, vendors must have a privacy policy that outlines rules governing the collection, use, disclosure, retention, accuracy, security and disposal of PHI/PI, breach management, information security, business continuity and disaster recovery, access, correction, and complaint practices.

5.5	Provide an electronic audit trail of all encounters, including a log of all accesses and transfers of personal health information.	M	Audit records must record and retain information about transactions (i.e., event ID, start and end date and time). Solutions that retain encounter summary records must maintain an audit log that includes: • Type of information viewed, handled, modified, or otherwise dealt with; • Date and time, it was viewed, handled, modified, or otherwise dealt with; • Identity of all persons who viewed, handled, modified, or otherwise dealt with the personal health information; and • Identity of the individual to whom the personal health information relates. Data in the audit log must not be altered, removed, or deleted, just marked as altered, removed, or deleted.
5.6	Provide an electronic audit trail of access to the solution trail.	M	Audit trail will include all login attempts, whether successful or failed. Must log traffic that indicates unauthorized activity encountered at the application server. The log must include: • Timestamp, user ID/application ID, originating IP address, port accessed or computer name; • External ODBC connections used to execute SQL or data layer queries. • Application data stored external to the database such as attachments; • All data files used to meet other local requirements (e.g., reporting requirements); • System time must be synchronized with a trusted source to maintain audit trail integrity; and

			• Be protected to ensure audit integrity and from unauthorized access, modification, and destruction.
5.7	Put in place reasonable safeguards and controls to protect all data, endpoints, and traffic, whether in transit or at rest.	M	Solutions must use current industry standard cryptographic and hashing mechanisms to encrypt and safeguard personal health information and/or personal information. Recommended cryptographic standards include: NIST SP 800-22 Revision 1a - A Statistical Test Suite for Random and Pseudorandom Number, FIPS 140-2 - Security Requirements for Cryptographic Modules.
5.8	Provide an up-to-date Privacy Impact Assessment (PIA) summary.	M	PIA assurances and requirements must include: • PIA must have been completed within the last two years. • PIA must have been completed by a certified professional with any of the following credentials: obtained through the International Aion of Privacy Professionals (IAPP): Certified Information Privacy Professional (CIPP/C); Certified Information Privacy Manager (CIPM); Certified Information Privacy Technologist (CIPT) or with a minimum of two years of experience conducting privacy impact assessments in Ontario and/or Canada. • The PIA methodology must include a legislative analysis relevant to Ontario and its health care context and at a minimum have been mapped to the 10 Fair Information Principles as published by the Canadian Standards Association (CSA) Model Code for the Protection of Personal Information and in accordance with the PIA guidelines issued by the Information and Privacy Commission of Ontario[7] with respect to health care. • The PIA and PIA summary must include a table of content, a summary of risk findings, including a likelihood and impact table or risk heat map, a mitigation plan, and the

			status of any outstanding risks, as well as the name and contact information of the individual(s) and/or organization who conducted the PIA. Any risks identified as high must be mitigated prior to a vendor being listed as a verified vendor. Risks assessed as medium must have a clear mitigation plan with timelines for closure within six months of risk being identified. Low risks must have a mitigation plan in place within 12 months of date of PIA. • PIA and risk mitigation plan must be approved by the solution vendor's authorized representative of the organization or Chief Privacy Officer, and summary shared with and reviewed by Ontario Health. • Must be based on the latest solution design and technical architecture for the virtual visit solution with no significant changes to the solution, services, or privacy program since the completion of the PIA. • PIAs must be refreshed every three (3) years or when there has been a change in the solution, legislation, policy, or business operations of the solution provider(s) that may have an impact on the privacy of health information or on privacy rights.
5.9	Provide an up-to-date application-level Threat Risk Assessment (TRA)	M	TRA assurances and requirements must include: • TRA must have been completed within the last two years being relevant to online appointment booking, with no significant changes to the solution, services, or security program since the completion of the TRA. • Confirmation that the TRA was performed by a qualified assessor with a minimum of five years of direct full-time security experience and in possession of a CISSP certification in good standing. • The TRA must have been completed with a security analysis based on an industry-standard threat risk assessment methodology (e.g., HTRA, NIST, OCTAVE).

			• The TRA and summary must include a summary of risk tables and a status of the risks. Any risks identified as very high or high must be mitigated prior to a vendor being listed as being verified. Medium risks will show clear mitigation plans for closure within six (6) months of these risks being identified. It is recommended that low risks be identified, monitored, and closed where practical and a summary shared with and reviewed by Ontario Health; every 12 months an annual confirmation of changes is required. • The TRA must refreshed every three (3) years or when there is a change in the solution, legislation, policy, or business operations of the solution provider(s) that may have an impact on the privacy and/or security of health information or on privacy rights. • The TRA must include the results of a vulnerability scan and penetration test.
5.10	Ensure the OAB solution vendor has a policy that describes when or how frequently it performs periodic vulnerability assessment scans.	M	Vulnerability scans must include the application and application infrastructure. For hosted environments, the hosting provider may need to submit their own VA scan results.
5.11	Ensure the OAB solution vendor has a policy that describes when or how frequently it performs periodic penetration tests.	M	Penetration tests should be done, at a minimum, on an annual basis, or when there has been a major software release, change in architecture or infrastructure. Penetration tests must include the application and application infrastructure where possible. For hosted environments, the hosting provider may need to submit their own penetration test results.
5.12	Meets security and privacy controls.	M	Solution provider must follow general security guidance based on ISO 27002 control objectives. Please refer to Ontario Health's Security Toolkit and OntarioMD's Hosting Requirements for requirements related to application security,

			infrastructure, business operations and business continuity. Other security certifications such as SOC2, Hitrust, OntarioMD, or Canada Health Infoway can assist in meeting this requirement. Control Objectives: • Network and Operations • Physical Security • Acceptable Use of Information and Information Technology • Access to Control and Identity Management for System-Level Access • Information Asset Management • Information Security Incident Management • Threat Risk Management • Business Continuity • Security Logging and Monitoring • Electronic Service Provider • Disaster Recovery • Cryptography
5.13	Provide input validation and data sanitization controls to ensure that user-entered data is valid.	M	The solution will check the entered input data to ensure that it meets the expected format, and reject or replace any illegal characters (e.g., single quotes, escape characters, angle brackets, backslashes, etc.) that are typically used in injection attacks (e.g., SQL Injection, Cross Site Scripting).
5.14	Provide a comprehensive agreement framework related services including for any third party it retains to assist in providing these services. The vendor is responsible to notify any providers of any new third-party vendors.	M	Solution and third-party provider agreements will at minimum include privacy and security language that describes the services and the administrative, technical, and physical safeguards relating to the confidentiality and security of PHI and PI and how the vendor and any third-party vendor retained comply with applicable legislation, including but not limited to those listed above.
5.15	Support healthcare organizational or clinician retention obligations and policies.	M	Solution facilitates or enables the collection and retention of PI and PHI; the solution must retain the PI and PHI in accordance with record-keeping and retention obligations and policies. The solution must retain data in accordance with applicable laws or standards. In the absence of an existing retention policy, it is recommended that clinicians follow applicable

			regulatory and/or professional standards, such as the CPSO data retention and destruction guidance within the medical records management policy.
5.16	Ensure all PHI is held and accessed by systems located in Canada.	M	Solution must be hosted and managed within a Canadian data center including all solution data and backups.
5.17	Provide protection against SPAM data generated by bots and automated scripts.	R	Publicly accessible forms (e.g., registration page, help page, etc.) should have controls in place to ensure that the input is coming from a “real” human user and not a robot. Examples include: • CAPTCHA • reCAPTCHA • Honeypot Challenge Question

i. All Rights Reserved

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

ii. Trademarks

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

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

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