Online Appointment Booking

Service Standard Version 2.0

Spring 2024

Table of Contents

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.

Change Highlights

- Acknowledgements section removed.
- Section 1.0: Terms and Abbreviations section added.
- Section 2.0: No major changes
- Section 3.0: Use cases updated (added)
- Section 4.0: No major changes
- Section 4.1: Inclusion of 'caregiver' when referring to patient, Updated AODA requirement (to match Virtual Visits Standard)
- Section 4.2: No major changes
- Section 4.3: Removed 4.3.5 requirement (SMS Notifications)
- Section 4.3: Remove 4.3.7 attach and send files.
- Removed 4.3.9 requirement (ability to customize information in a notification to patient)
- Section 4.4: Remove 4.4.2 Patients can view confirmed appointments in the OAB solution.
- Section 5.0 All P&S requirements were reviewed by our P&S teams and all efforts were made to update requirements to align with Virtual Visits updated Standard.
- Removed 5.3 (requirement to have designated Security employee)
- Removed 5.13 (input validation and data sanitization controls)

Online Appointment Booking Service Standard

1) Introduction

Self-booking a healthcare appointment online is less common in Ontario than it should be. In 2022 Canada Health Infoway conducted an in-depth analysis, and, at that time, 75% of patients indicated they would like to make an appointment with their doctor electronically, however, only 18.2% have booked an appointment with their doctor electronically in the last 12 months[1].

In 2019, the Ministry of Health launched a 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 (OAB) is one of them.2 OAB is an "option" available to patients, and the goal is not to discontinue telephone appointments rather to provide an efficient and easy way patients and/or caregivers can self-book.

Offering OAB to book health care appointments may decrease providers' no-show rates, amount of time administrative staff 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 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

[1] Canada Health Infoway 'Interest in Digital Health Services, 2022 Canadian Digital Health Survey, insights.infoway-inforoute.ca/2022-interest-in-and-use-of-digital-health-services/.

[2] Ministry of Health, 'Connected Care Update', *Ministry of Health*, 2019, 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, 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).

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 or Patient Portal Standards, please refer to ontariohealth.ca/system-planning/digital-standards.

a) Terms and Abbreviations

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

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

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

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

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

Conformance Language
The following definitions of the conformance verbs are used in this document:

- Shall/Must: Required/Mandatory
- Should: Best Practice/Recommendation
- May: Acceptable/Permitted/Encouraged

2) Definitions

ONLINE APPOINTMENT BOOKING

Online appointment booking solutions allow people 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.
The use of email addresses and online enquiry forms for booking purposes are not OAB solutions.

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.

STANDALONE SOLUTIONS

Standalone OAB solutions can be cloud-based software designed specifically for patient-initiated OAB. These solutions may offer integration with PoS applications or be part of the PoS application itself.

MANDATORY

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

RECOMMENDED

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

ROSTER

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

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.) health.gov.on.ca/en/pro/programs/pcpm/.

3) Use Cases

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

Patient

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

b) A patient and/or caregiver would like to book a follow-up appointment to discuss the x-rays from last week. While using their computer, they access the medical clinic's website and choose from the available dates and times for an appointment next week. Unfortunately, the patient's work schedule has changed, and they must cancel the follow-up appointment and find a new time. They can easily cancel the appointment from the confirmation text and have the option to pick a new time that meets their needs.

c) A caregiver is seeking a service to help their mother, newly diagnosed with Alzheimer's. They navigate the internet with their mobile device looking for care options. They find a service that is available in their neighbourhood, delivered by a local community support agency, and book an appointment to speak with the intake staff at the program. At the time of booking, they fill out a simple request form with basic demographics and share a bit about their current health concerns and care needs. They receive a confirmation email and a reminder notification of the appointment. The email reminders include the ability to cancel or reschedule the appointment, if necessary.

The Clinician

d) The clinician's schedule is shared between the PoS and 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

e) The office assistant receives the clinic's new schedule for all the clinicians. They make the changes quickly in the EMR to reflect all the clinicians' changes. These changes are automatically reflected in the OAB solution.

f) The office assistant receives an internal message from a clinician 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) 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.

a) 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 and/or caregivers must be updated on a near real-time basis based on each clinician’s availability.
4.1.2	Enable patients and/or caregivers to view appointment options.	M	Solutions must be capable of displaying appointment options (in-person, video, or telephone) offered by the clinician to patients prior to their appointment selection.
4.1.3	Send an automatic appointment confirmation to the patient and/or caregiver.	M	Solutions must be able to automatically notify patients and/or caregivers that the appointment they selected has been confirmed within the clinician’s schedule.
4.1.4	Meet Web Content Accessibility Guidelines (WCAG) 2.0 Level AA requirements or higher.	M	Solutions should have web and user interfaces that provides accessibility to Ontarians with disabilities; and comply with the Accessibility for Ontarians with Disabilities Act (AODA). Vendors should make available upon request or publish a notice of the web accessibility level the vendor reaches relevant to its solution. At a minimum, the vendor must be able to provide an Accessibility Conformance Report or Voluntary Product Accessibility Template (VPAT).

#	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 export reports that track online booking statistics.	M	Below **are examples** of potential reports that track online booking statistics. • Number of unique online appointment bookings. • Number of appointments available for OAB/ Amount of a scheduled open for OAB (hours per month). • Number of unique patients who booked an online appointment. • Number of patients who registered for OAB. • Number of patients that have interacted with the OAB Solutions (Schedule, modify, cancel, Secure messaging). • Number of appointments cancelled/rescheduled by patient or clinician. • Reports should be easy for customers to generate; customers should be able to select the date range.
4.1.7	Enable patients and/or caregivers to download the confirmed appointment to a calendar.	R	The patient and/or caregiver 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 and French for patients.	R	Ontario Health recommends that Solution Providers begin work towards meeting this recommended requirement as it will become Mandatory in a future version of the OAB solution standard. English and French are Official languages in Ontario.

#	Requirement	Priority	Notes
4.1.9	Enable a multilingual patient interface.	R	Supports other languages in addition to English and French.

b) Booking Rules

#	Requirement	Priority	Notes
4.2.1	Enable patients and/or 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. 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 as indicated by the clinic.	M	Solutions must be capable of displaying 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 can book an appointment for their parent.
4.2.4	Enable clinic 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 the clinic to open specific appointment times in the calendar for online bookings.	M	This allows providers to easily provide periods of appointment times.

#	Requirement	Priority	Notes
4.2.6	Ability to allow the clinic to set recurring day and time blocks for online booking.	M	**For example:** Mon, Wed, Fri mornings are available for OAB.
4.2.7	Enable a clinic user the ability to approve and/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. This is a feature that clinics can choose to use depending on their clinic workflow.
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 and or 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 cancellations 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, type of appointments, reason for appointments.

c) Notifications

Solution providers and Health Service Providers should be cautious when designing notifications to ensure that no PHI is sent in unsecure notifications.

#	Requirement	Priority	Notes
4.3.1	Enable automatic sending of reminders/confirmations using one or more of the following notification channels of SMS, email, and voice or 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 automatic sending of reminders/confirmations using one or more of the following notification channels of SMS, email, and voice or upcoming appointments to patients.	M	The solution can send out appointment reminders automatically, without the need for intervention by clinic users.
4.3.3	Enable patients to choose their preferred notification channels.	M	If the solution supports multiple notifications channels, the patient can select the best modality to receive notification.
4.3.4	Enable patients to cancel appointments from reminder notifications.	M	From a reminder notification, the patient is easily able to cancel an appointment.
4.3.5	Enable clinical and non-clinical users to modify an existing appointment.	R	This can include an office assistant.
4.3.6	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.

d) 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, and Patient Portals.

#	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: Service providers' calendars are updated as patients book appointments, and patients see available time slots as providers update their calendar. Solutions using data standards that support interoperability in Ontario, and where applicable with other provinces. E.g., EMRs in Manitoba that book patients in Ontario and vice versa.
4.4.2	Enable a clinician to have access to multiple PoS using one OAB solution.	R	A clinician who works at multiple clinics with potentially different EMRs and at distinct locations.

5) 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 review 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 controls, security incident response procedures, encryption, logging and monitoring, secure operational procedures, and other mechanisms to protect the confidentiality, integrity, and availability of data.

[4] Canada Health Infoway 'Interest in Digital Health Services, 2022 Canadian Digital Health Survey, insights.infoway-inforoute.ca/2022-interest-in-and-use-of-digital-health-services/.

[5] Canada Health Infoway 'Interest in Digital Health Services, 2022 Canadian Digital Health Survey, insights.infoway-inforoute.ca/2022-interest-in-and-use-of-digital-health-services/.

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 ￼.

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 OAB solution and services.	M	At a minimum the privacy notice, statement or policy must describe: • How the Solution Provider collects, uses, discloses, and retains PHI and PI • How the Solution Provider protects the privacy rights of patients; and • Details how a Solution Provider manages role-based access to the information.

[6] Canada Health Infoway ‘Interest in Digital Health Services, 2022 Canadian Digital Health Survey, insights.infoway-inforoute.ca/2022-interest-in-and-use-of-digital-health-services/.

#	Requirement	Priority	Notes
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 (Canada's Anti-Spam Legislation (CASL) • Consent to exchange PHI (e.g., submitting an Ontario Health Insurance Plan (OHIP) number would require consent under Personal Health Information Protection Act, 2004 (PHIPA) • Consent to use de-identified PHI (e.g., Under PHIPA, the creation of de-identified information is considered a use of PHI. This use must be communicated to patients. Although PHIPA does not specify what vendors can do with de-identified information, PHIPA does require the ability to re-identify an individual is remediated). Vendors should have policies and procedures that reference de-identification and /or 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 privacy office/employee responsible for privacy must be publicly assessable on the vendor's website. Note: A generic email address is acceptable (i.e., privacy@abc.com)

#	Requirement	Priority	Notes
5.4	Have a privacy and security program that includes policies and procedures.	M	At a minimum, Solution Providers must have privacy and security policies and procedures that outline: • Rules governing the collection, use, disclosure, retention, accuracy, security, and disposal of PHI/PI • Breach management • Information security • Business continuity and disaster recovery • Role-based access controls • Privacy inquiries • Correction request

#	Requirement	Priority	Notes
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). For every instance in which a record or part of a record of personal health information that is accessible by electronic means is viewed, handled, modified, or otherwise dealt by Solutions that retain encounter summary, an electronic audit log must be maintained. The electronic audit log must include: • The type of information viewed, handled, modified, or otherwise dealt with. • The date and time, it was viewed, handled, modified, or otherwise dealt with. • The identity of all persons who viewed, handled, modified, or otherwise dealt with the PHI and/ or PI. • Identity of the individual to whom the PHI relates. Data in the audit log must not be altered, removed, or deleted, just marked as altered, removed, or deleted.

#	Requirement	Priority	Notes
5.6	Provide audit security controls to maintain audit integrity.	M	Audit trail will include all login attempts, whether successful or failed. Must log traffic that indicates unauthorized activity encountered at the application server. The log must include: • Timestamp, user ID/application ID, originating IP address, port accessed or computer name; • External ODBC connections used to execute SQL or data layer queries; • Application data stored external to the database such as attachments; • All data files used to meet other local requirements (e.g., reporting requirements); • System time must be synchronized with a trusted source to maintain audit trail integrity; 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 both in-transit and at-rest. 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	Conduct Privacy Impact Assessments (PIA)	M	Privacy impact Assessment must be conducted by the vendor for the solution offering OAB service. The Privacy Impact Assessment should include: A PIA summary which contains: 1) a table of contents of the PIA, 2) a brief description of the service, 3) A list of third parties assisting in delivering solution with agreement framework in place 4) a statement reflecting that the PIA is current, 5) the role(s) which the organization plays under PHIPA and why they believe that the authority applies, 6) A list of data elements collected, used, disclosed by vendor and/or third party assisting in delivering the solution. 7) a summary of risk findings including a likelihood and impact table or risk heat map, 8) a mitigation plan (for risk findings) and approval of the plan 9) a status on any outstanding risks 10) the name and contact information of the individual(s) and/or organization who conducted the PIA. 11) A confirmation that information security assessment was also completed. PIA should be completed by a professional with a minimum of 2 years of experience conducting PIAs in a health care context based on PHIPA or other provincial health legislation. The PIA methodology must include a legislative analysis relevant to Ontario and its

#	Requirement	Priority	Notes
5.8	Conduct Privacy Impact Assessments (PIA)	M	healthcare context and at a minimum have been completed mapped to the ten Fair Information Principles as published by the Canadian Standards Association (CSA) Model Code for the Protection of Personal Information and in accordance with the PIA guidelines issued by the Information and Privacy Commission of Ontario with respect to healthcare. The legislative analysis must include context including the identification of PHIPA authorities (e.g., role (s) and responsibilities) and provide evidence and/or rationale as to why you believe that the authority applies. PIA and risk mitigation plan must be approved by the OAB solution vendor's authorized representative of the organization or Chief Privacy Officer. The PIA must be based on the latest solution design and technical architecture for the OAB solution with no significant changes to the solution, services, or privacy program since the completion of the PIA. PIAs must be refreshed every 3 years or when there has been a change in the solution, legislation, policy, or business operations of the solution provider(s) that may have an impact to the privacy of health information or to privacy rights.

5.9	Vendors must provide an up-to-date Threat, Risk Assessment (TRA) Summary Report or SOC 2 Type 2 Audit Report	M	This requirement can be met by providing a Threat Risk Assessment (TRA) Summary Report or a SOC 2 Type 2 Audit Report to satisfy the following conditions, as applicable: • The TRA must have been completed within the last two years, while the SOC 2 Type 2 Audit must have been completed within the last year, being relevant to the Online Appointment Booking solution submitted with no significant changes to the solution and clearly indicate that Online Appointment Booking functionality was in scope for the assessment, services, or security program since the completion of the TRA or the SOC 2 Type 2 Audit The TRA or SOC 2 Type 2 Audit was performed by a qualified assessor: • For the TRA, this means that the assessor has at least five years of direct full-time security experience that includes conducting TRAs or managing security risks and in possession of an industry recognized security certification (e.g., CISSP, CISM, CISA, CRISC) that is in good standing. • For the SOC 2 Type 2 Audit report, this requires that the audit be performed by an AICPA certified third-party organization. If a TRA Summary Report is being submitted, the following, additional requirements apply: • The TRA must have been completed with a security analysis based on an industry-

5.9	Vendors must provide an up-to-date Threat, Risk Assessment (TRA) Summary Report or SOC 2 Type 2 Audit Report	M	standard risk assessment methodology (e.g., HTRA, NIST, OCTAVE, etc.) - The TRA Summary must include a table of risks, the status of risks, and a risk treatment status. Note: Any risks identified as high must be mitigated prior to Solution Provider submissions. Medium risks must have clear mitigation plans for closure within 6 months of the risks being identified. It is recommended that low risks be mitigated within 12 months. - The TRA must be refreshed every three years or whenever there is a significant change in the design of the solution, policy or applicable business operations that may impact the security posture of the solution. If a SOC 2 Type 2 Audit report is being submitted, the following, additional requirements apply: - The proposed Online Appointment booking solution was included in the SOC 2 Type 2 Audit scope. - The audit was conducted within the last year and the "Period of Examination" covers the period during which the solution/platform was developed. - The report states that in the auditor's opinion, the examined controls were suitably designed and operated effectively throughout the audit period to provide reasonable assurance that Solution Provider service commitments and system requirements will be

5.9	Vendors must provide an up-to-date Threat, Risk Assessment (TRA) Summary Report or SOC 2 Type 2 Audit Report	M	achieved under the following Trust Services and Common Criteria: - (CC3.1, CC3.2, CC3.3, CC3.4) Monitoring Activities - (CC4.1, CC4.2) Control Activities - (CC5.1, CC5.2, CC5.3) - Logical and Physical Access Controls (CC6.1, CC6.2, CC6.3, CC6.4, CC6.5, CC6.6, CC6.7, CC6.8) System Operations (CC7.1, CC7.2, CC7.3, CC7.4, CC7.5) Change Management - (CC8.1) Risk Mitigation - (CC9.1, CC9.2) Trust Services Criteria: - Availability Additional Criteria for Availability (A.1, A1.2, A1.3) Trust Services Criteria: - Processing Integrity Additional Criteria for Processing Integrity (PI1.1, PI1.2, PI1.3, PI1.4, PI1.5) Trust Services Criteria: Confidentiality Additional Criteria for Confidentiality - (C1.1, C1.2)

#	Requirement	Priority	Notes
5.9	Vendors must provide an up-to-date Threat, Risk Assessment (TRA) Summary Report or SOC 2 Type 2 Audit Report	M	• The SOC 2 Type 2 Audit must be refreshed every year or whenever there is a significant change in the design of the solution, policy or applicable business operations that may impact the security posture of the solution. No unreasonable exceptions or deviations, commonly referred to as control failures, were noted under the “Results of Tests” section. In the auditor's opinion, the examined controls were designed and operated effectively (i.e., no significant negative findings reported).
5.10	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 vendor should be asked to provide assurance regarding the hosting provider's VA scanning practices.
5.11	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 should include the application and application infrastructure where possible.

#	Requirement	Priority	Notes
5.12	Meets security and privacy controls requirements.	M	Solution Provider will provide a current copy of one of the following: ISO 27001 certification, SOC 2 Type 2 Audit Report, HITRUST certification or OntarioMD certification. Obtaining any one of these certifications will ensure that the following control objectives have been met: • Network and Operations • Physical Security • Acceptable Use of Information and Information Technology • Access to Control and Identity Management for System-Level Access • Information Asset Management • Information Security Incident Management • Threat Risk Management • Business Continuity • Cryptography • Security Logging and Monitoring • Electronic Service Provider
5.13	Provide a comprehensive agreement framework related services including for any third party it retains to assist in providing these services. The vendor is responsible for notifying 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.

#	Requirement	Priority	Notes
5.14	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 legal obligations, 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.
5.15	Ensure that all PHI is accessed from and hosted in systems located in Canada including all backups. This includes any of your third-party service provider(s).	M	Solution must be accessed from and hosted within a Canadian location including all PHI and backups. For clarity, you must be able to meet the restriction that neither you nor any of your representatives including third party service providers will not provide any services from a location outside of Canada without the prior written consent of the health information custodian.
5.16	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, but not limited to include: ● CAPTCHA ● reCAPTCHA ● Anti-spam Honeypot ● Anti-spam Plug-in

Appendix

All Rights Reserved

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 prohibited.

HL7®

HL7®, and FHIR® are the registered trademarks of Health Level Seven International and their use of these trademarks does not constitute an endorsement by HL7.
“HL7® FHIR® standard" or "HL7® FHIR®", using the ® symbol as often as is practical, at least once on each page of printed matter, generally in connection with the first or dominant usage.