Ontario Health

Patient Portal (PP) Provincial Service Standards

June 2021

TABLE OF CONTENTS

Acknowledgements

The requirements listed in this document are informed by other provincial standards, including *the Virtual Visits Solution Requirements, Online Appointment Booking standards* and have been reviewed by regional leaders, and internal experts.

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

Dale Anderson - Health Information Technology Services E-Health at Hamilton Health Sciences
John Haywood - Health Information Technology Services E-Health at Hamilton Health Sciences
Devi Pandya - Health Information Technology Services E-Health at Hamilton Health Sciences
Mark Berry - Health Information Technology Services E-Health at Hamilton Health Sciences
Marzena Cran - Health Information Technology Services E-Health at Hamilton Health Sciences
Josh Sinclair - Health Information Technology Services E-Health at Hamilton Health Sciences

Patient Advisors
Ontario Health
Ministry of Health
Patient Portal Vendors

Disclaimer

This document relates to, but is not specific to, the provincial services of Ontario Health or other provincial health organizations. The standard detailed in this document is a non-normalized standard and therefore errors, omissions and revisions may occur. This document is not intended to be, nor should it be deemed, legal advice. Ontario Health encourages legal counsel be engaged as required.

Need this information in an accessible format?
1-877-280-8538, TTY 1-800-855-0511 info@ontariohealth.ca.

1. Introduction

Digital technologies for health are increasingly offering care teams an avenue to deploy information and communications technology tools to patients. These tools enable patients, caregivers, and healthcare professionals more efficient access to data and information, thus improving the quality of health outcomes. Patient portals are capable of serving as an effective platform to support patient interactions with their healthcare teams and access to medical records and health education resources in a safe and secure manner. The purpose of this standard is to facilitate the selection and implementation of digital patient portal solutions.

The purpose of these standards is to:

- Define the general functional and non-functional requirements for digital solutions used by health care organizations and clinicians to support patient portal platforms (PPP) that digitally share Clinical information with users (patients).
- Outline a framework and mandatory requirements that the platform must demonstrate concerning the digital release of clinical information to users.
- Assist health service providers in selecting solutions that are designed to support safe, privacy and security-enhanced clinical data with users and advance interoperable health information exchange.
- Guide health care organizations, including Ontario Health Teams (OHTs), who are interested in procuring a PPP solution.
- Equip OHTs with recommendations and considerations necessary for maximizing the value of their investment in acquiring a first PPP or upgrading an existing one.

This document urges readers to recognize that the standards do not attempt to define requirements for every function of the platform, neither does it recommend any specific PPP.

1.1 Guiding Principles

Where an organization(s) decides to release clinical information to users digitally, they should follow the key foundational principles within healthcare in addition to the Patient Declaration of Values for Ontario[1]:

1. The patient owns their Personal Health Information (PHI), which should be designed in a user-friendly and portable format.
2. The patient has the right to fully access their PHI anytime via the source facilities release of information office.
3. All efforts should be made to allow PHI to patients with little or no restrictions; failing that, a clear pathway to real-time access should be in place.
4. The patient has the right to be informed and control who accesses the relevant PHI being shared.
5. The patient has the right to ensure the accuracy and completeness of their PHI.

2. Glossary

The definitions provided in this section are drawn from various sources and are outlined for the purposes of providing non-technical, simplified descriptions of some of the terms used in this document.

Patient Portal Platform (PPP)
Patient portal platforms (PPPs) are digital health applications designed to automate patient outreach and keep patients engaged throughout the continuum of their care. Common PPPs include patient portals, mobile applications for Android/iOS platforms, and messaging chatbots. PPPs can make patients feel connected and cared for and improve the patient experience and satisfaction.[2]

Online Appointment Booking (OAB)
Online appointment booking (OAB) solutions allow patients 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, or voice recordings.[3]
Email addresses and online inquiry forms are not OAB solutions as they require human interaction to confirm appointment availability.

Virtual Visits
A virtual visit is defined as a digital interaction where one or more clinicians, including physicians, nurses or allied health, provide health care services to a patient or their caregiver.

Digital Health
Digital Health describes the many uses of information technology that support patient care delivery in the health system. This can include the coordinated use of the web, mobile and cloud technologies to integrate points of care.[4]

Health Literacy
Health literacy is the degree to which an individual has the capacity to obtain, communicate, process, and understand basic health information and services to make appropriate health decisions.[5]

Interoperability
Interoperability means the ability to capture, manage, communicate and exchange data accurately, effectively, securely, and consistently with different information technology systems, software applications and networks in various settings, and exchange data so that the use of clinical or operational purpose and meaning of the data is unchanged.[6]

Patient Portal
Patient portals are technological innovations that enable patients with electronic access to their PHI.[7]

Patient Reported Outcomes Measures (PROM)
PROMs are measurement instruments (i.e. surveys) that patients complete to provide information on aspects of their health status and quality of life, including symptoms, function, pain and physical and mental health. Examples of PROMS that could be delivered to patients via a patient portal are Oxford Hips and Knees Scores.[8]

Patient Reported Experience Measures (PREM)
PREMs are measurement instruments (i.e. questionnaires) that patients complete to provide information on their perspective of the level of care they‘ve received.[9]

Mandatory (M)
Mandatory (M) refers to a requirement that must be met.[10]

Recommended (R)
Recommended (R) refers to a requirement that would be optional.[10]

Future (F)
A requirement that is planned for the future.

3. Patient Digital Access to their Health Records

3.1 Functional Requirements

All patient engagement solutions should adhere to a core set of functional requirements, in addition to solution-specific functional requirements (i.e. patient portals, appointment booking etc.). The following are the common functional requirements to be considered with all solutions:

- Secure – encryption, secure login in etc.
- Current – data release guidelines, minimize delays
- Complete – limit the restricted sections – show all information in the patient record as much as possible
- Portable – allow for offline use, sharing with other healthcare professionals out of province, out of country
- Upload-able – personal health records to be tracked and updated by the user (fitness data, etc.)
- Shareable – delegation – and ability to share with caregivers (upload to other EMRs – see also portable)
- Restrict-able – user can restrict data shared with caregivers and delegates
- Auditable – use of the application should be reviewable

In addition to general AODA compliance, the following list of common functionalities should be referred to when building or procuring patient portal software that will be public-facing.
The following sections contain tables of requirements that use the following column headings:

- # - the unique requirement ID
- Requirement – a statement describing a need that patient portal 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.

General Functionality

#	Requirement	Priority	Notes
3.1.1	The platform enables users to register/log-in to accounts.	M	Enrollment shall be linked to a user's profile.
3.1.2	Platform must have the ability to provide and edit/remove delegate and proxy access.	M	Allows authorized access to registered caregivers.[11]
3.1.3	The platform shall be able to retrieve data from different sources using a common matching criteria.	M	Examples include: Healthcard number, MRN (medical record number), Date of Birth.
3.1.4	The platform shall ensure that any existing platform users can also view their PHI from their existing patient portal profile (if implementing or upgrading an existing solution).	M	Access to the platform shall be un-affected by system changes and updates.
3.1.5	Provide access for a user to view lab tests and Diagnostic Imaging.	M	Expectations regarding timing of availability of results on platform shall be provided. Medical terminology interpreted.
3.1.6	Provide the user with a view of both historical and upcoming appointments.	M	List of past and future appointments.
3.1.7	Provide users the ability to print and/or save an offline copy of aspects regarding their PHI.	M	Medical records and clinical summaries with relevant and actionable information about user's health care[1].
3.1.8	Enables user to receive, fill, and send completed registration forms/questionnaires back to service provider.	M	Forms sent to the user shall be editable and user given the option to submit.
3.1.9	The platform shall accommodate alternative patient matching criteria when a healthcard number is not available.	R	The following sources refer to medically uninsured patient groups who do not have access to a healthcard number: OHIP For All Healthy Debate
3.1.10	The platform shall allow for the user to access their provider through virtual visit (VV).	R	Please see VV requirements https://otn.ca/wp-content/uploads/2020/03/virtual-visits-solution-standard1-1-1-1.pdf

#	Requirement	Priority	Notes
3.1.11	The platform should be capable of using and displaying accepted terminology requirements such as SNOMED, LOINC, pCLOCD etc.	R	The intent is not to have the patient portal translate or transcribe information from the sources, but rather, be able to leverage the additional information available through such terminology standards. Examples of terminology requirements include: • SNOMED CT (Systematized Nomenclature of Medicine – Clinical Terms) - International clinical terms controlled terminology requirements • LOINC (Logical Observation Identifiers Names and Codes)- International Lab and document ontology controlled terminology requirements • pCLOCD (Pan-Canadian LOINC Observation Code Database)- Canadian Lab controlled terminology requirements • HL7 FHIR Value Sets - value sets defined for use with HL7 FHIR; includes controlled terminology requirements • Pan-Canadian Terminology Subsets - CHI terminology sets published based on Canadian needs; includes controlled terminology requirements based on international terminology requirements • ICD-10-CA (International Statistical Classification of Diseases and Related Health Problems, 10th Revision – Canadian Enhancement) - requires licensing under CIHI; International clinical disease classification system with Canadian extensions • CCI (Canadian Classification of Health Interventions) - requires licensing under CIHI; International clinical intervention classification system with Canadian extensions

#	Requirement	Priority	Notes
3.1.12	Provide a notification within the platform to highlight when new or modified information is retrieved.	R	Timely push notifications which are relevant to the user, reflect priority levels and can be archived.
3.1.13	Allow for platform use as a central location to input/aggregate their PHI from external sources.[2]	R	Various data-entry options including free-text and the ability to synchronize with other data sources including third party apps e.g. Fitbit, vaccination records, health/fitness apps, medical devices.
3.1.14	Enables user to engage with their providers through a secure messaging system[3].	R	Bidirectional communication system with end-to-end encryption or ability to integrate with a third party solution. For more details please reference Virtual Visits Standard which has provincial DTP Secure Messaging requirements https://otn.ca/wp-content/uploads/2020/03/virtual-visits-solution-standard1-1-1-1.pdf
3.1.15	Allows user to request for access or transfer of health records and summaries between service providers.	R	From the user's current or previous service providers who use the same platform or connect to other platforms.
3.1.16	Enables user to engage in medication management activities and request for prescription refills.	R	List of medications, dosages with clear instructions (devoid of abbreviations); option to send request for prescription refills. Or ability to integrate with a third party solution.

Auditing and Security

#	Requirement	Priority	Notes
3.1.17	The platform must be able to produce audit logs related to user account activity.	M	List of previous logins displaying the date, time and device type.
3.1.18	Allows users to log out from their online profile.	M	Pop-up messages to confirm selection of log out option and then successful log out by user.

#	Requirement	Priority	Notes
3.1.19	Allow users to view and perform audits of their own account activity.	R	It is recommended that the organizations allow users to self-audit.

Design and UI

#	Requirement	Priority	Notes
3.1.20	Ensure that the platform and the data displayed are accessible from a Desktop (Mac/PC/Linux) and Mobile (Android/IOS) platforms.	M	The platform shall be designed to be compatible with existing operating systems.
3.1.21	Ensure that the platform displays user's health information in an organized format e.g. diagnosis, treatment plan, lab-results, etc.	M	The information shall be available under sub-headings.
3.1.22	Allows users to communicate with their service provider by supporting the ability to request, receive, and/or upload documents.	M	Preferred format for files shall be the widely-accepted ones and specified as pdf, doc and jpeg files.
3.1.23	Ability for the platform to include a robust user help functionality.	M	Examples include: Incorporating appropriate descriptions or tool tips to help users with limited health literacy find and understand the data groupings throughout the platform. Incorporating the use of visual aids (icons or images) to help users better understand the types of health information groupings.
3.1.24	Enable an English and French interface for users.	R	OHTs must ensure they meet the French language health service needs of their local community, including any legislative requirements where applicable

#	Requirement	Priority	Notes
3.1.25	Ability for the platform to display the data in a user-friendly format.	R	Organizing the aggregated may not be easy, however, it is necessary in providing users with a single, straightforward way to access their medical data with the best possible user experience in mind. A study by Vreeman and Richoz (2015) suggests that "the plethora of idiosyncratic conventions for identifying the same clinical content in different information systems is a fundamental barrier to fully leveraging the potential of EHRs".[11]
3.1.26	Enable a multi-lingual patient interface.	R	Supports languages other than English and French.

Administration

#	Requirement	Priority	Notes
3.1.27	Provide OHTs/Provider Organizations the ability to specify content for portions of the platform to allow for customized communications and targeted delivery.	M	Content and timing of information sent shall be relevant to meet the user's health information needs.
3.1.28	Ability for the solution to block or delay specific clinical records.	M	There are some instances where the organization deems that information shall be restricted or delayed through clinical or safety reasons.
3.1.29	Provide users with an area that will give them details about the platform and what it can provide them.	R	An introductory video to enlighten user on how to navigate, explain the core features and potential benefits.
3.1.30	Ensure the platform has an information material section.	R	In order to keep users informed on how to use the platform and different options within the application itself. Periodically update user manual, tagging the date of last review.
3.1.31	Provide users with the ability to request update of medical record.	R	Not Applicable
3.1.32	Provide users with the ability to make eBill payments.	R	Not Applicable

Integrations

Independent of the ability for a platform to display data from the assorted repositories and data sources, organizations must ensure that the correct data sharing agreements are in place with the HICs.

#	Requirement	Priority	Notes
3.1.33	Enable the platform to adhere to common Interoperability requirements such as DHIEX.	M	Ontario (2020, April 20). Digital Health Information Exchange Policy.
3.1.34	Ability for the platform to support common Integration of VV Technology and align with VV emerging Standard.	M	https://otn.ca/wp-content/uploads/2020/03/virtual-visits-solution-standard1-1-1-1.pdf
3.1.35	Enable the platform to adhere to common requirements for conformance, validation and implementation.	M	Not applicable.
3.1.36	Enable the platform to display data from the Ontario Laboratories Information System (OLIS).	R	OLIS is a single provincial domain repository that allows all Ontario laboratory test order and result information to be exchanged electronically and securely between authorized practitioners and laboratory service providers. Integration to the OLIS repository is possible through the OLIS HL7 FHIR specification. OLIS Display Specification: Please refer to A Guide to the OLIS Nomenclature for OLIS's series of defined standards related to the display of their information.
3.1.37	Ability for the platform to display data from EMRs in Primary Care.	R	At this time, there is no common FHIR interface for Consumers. Organizations looking to integrate with EMRs will need to ensure the proper agreements are in place as HICs in order to share this data with their clients.[12]

#	Requirement	Priority	Notes
3.1.38	Ability for the platform to display data from various Acute Care Health Information Systems.	R	As there is no common Health Information System application in Ontario, integrations with specific instances of HIS will require close work with the HIS providers (Acute Care generally) and their vendors on a case by case basis from both a technical and from an agreements basis. **Key Ontario HIS:** **Cerner** FHIR resources: Cerner FAQs Documentation: Cerner Millennium **EPIC** FHIR resources: Epic FHIR **Meditech** FHIR resource: Patient Health Data API
3.1.39	The platform should include data from at least 3 health sectors	R	Examples of data sources could include but should not be limited to: - EMRs - HIS - Other clinical systems - Provincial repositories and data sources - Private laboratory and diagnostic service providers
3.1.40	Ability for the platform to connect to the SMART App Launch Framework to connect third party applications and either launch standalone/portal or be launched	R	The SMART App Launch Framework connects third party applications to Electronic Health Record data, allowing apps to launch from inside or outside the user interface of an EHR system SMART App Launch Framework

#	Requirement	Priority	Notes
3.1.41	Ability for the platform to display data from one of the Provincial viewers.	F	While it is possible to connect to individual hospitals directly, and resources are provided below, it is advised that it would be easier and more effective for organizations to integrate with one of the provincial viewers (ClinicalConnect or Connecting Ontario) as the technical aspects of the integration with multiple hospitals has been completed. This would allow organizations to focus on obtaining data sharing agreements with the various hospitals to provide access. Currently, ClinicalConnect has a consumer facing API available and implemented. **Provincial Viewers:** **ClinicalConnect** About ClinicalConnect eHealth Ontario ClinicalConnect **Connecting Ontario** ConnectingOntario ClinicalViewer
3.1.42	Ability for the platform to display data from Digital Health Immunization Repository (DHIR).	F	DHIR is the current immunization repository for the province of Ontario. It contains public health immunization information and over 90 million standardized immunization records for over 6 million clients, with over 2000 registered users.
3.1.43	Ability for the platform to display data from the Acute and Community-Care Clinical Data Repository (acCDR).	F	The Acute and Community Care Clinical Data Repository provides access to user information from hospitals and home and community care organizations across Ontario.
3.1.44	Ability for the platform to display data from the Digital Health Drug Repository (DHDR).	F	The Digital Health Drug Repository (DHDR) is an electronic repository of dispensed drug and pharmacy service information. The DHDR currently includes records relating to publicly funded drugs, monitored drugs and pharmacy services representing approximately 70% of the total dispensed medications in Ontario.

#	Requirement	Priority	Notes
3.1.45	Ability for the platform to display data from the Diagnostic Imaging Repository (Diagnostic Imaging- Common Services DI-CS).	F	Diagnostic imaging repositories contain healthcare client diagnostic imaging reports and digital images such as x-rays, magnetic resonance imaging (MRIs), and ultrasounds. There are four diagnostic imaging repositories in Ontario (known as DI-Rs), each serving a different geographical area in the province.

Identity, Access and Authorization

#	Requirement	Priority	Notes
3.1.47	Platform needs to support user authentication(s) that meet provincial standards (e.g. ICA Policy) before releasing PHI.	M	Multi-layer of authentication to verify patient identity. The platform needs at least to support users to be identified by their Health Card #, DOB and last name

#	Requirement	Priority	Notes
3.1.48	Ability for the platform to support Patient Digital Identity, Authentication and Authorization (IAA).	M	OH is currently procuring a Digital Wallet and Verifiable Credential solution in support of several OH Patient facing applications and APIs. The intent of this solution will be to: Provide a simple user and provider (future aspiration) access to OH (and broader health care sector) healthcare services through a set of published APIs or a set of Applications. Minimize the need to share or produce the same personal information repeatedly with each of the health care services a user wishes to use. Only share that amount of personal information required for the particular service and for identifying the individual in question. Minimize the different login IDs and passwords users must utilize and remove the need for passwords in general. Simplify the process of identifying and registering for services and making authentication to various services seamless and as transparent as possible. As this solution is still unavailable, current implementations of patient-facing solutions would benefit from utilizing this solution and or approach.
3.1.49	The platform should be able to implement some form of multi-factor authentication (MFA) for users logging into the site.	R	It is strongly recommended that user log-ins have at least the same rigour as financial institutions, if not more.

Registration

#	Requirement	Priority	Notes
3.1.50	Provide a simple and user friendly way for users to register.	M	For example: Users will require a valid email address and will be required to submit the email address when registering for the platform, in addition to identifying information. (Ex. First/Last name, Healthcard number).
3.1.51	Standard enrollment emails will be delivered to the email the user has provided when registering.	M	Not applicable

3.2 Non-Functional Requirements

In addition to functional requirements, there are additional non-functional requirements that must be considered for all software.

#	Description	Priority	Notes
3.2.1	**Performance** Ability for the user interface to perform optimally according to industry specifications.	M	Example: Application responsive time to complete the following tasks: a) Initial Screen load, no more than 3 seconds b) 80% of the screens must not exceed a latency in response time of more than 3 seconds.
3.2.2	**Capacity** Ability for the platform to support an appropriate number of concurrent user sessions at any given time.	M	Dependent on the size of the expected user base.
3.2.3	**Availability** Ability for the platform to always be available 24 hours per day, 365 days per year.	M	This availability excludes scheduled service outages.
3.2.4	**Scalability** Ability for the platform to be scalable to support increases in registered users while still meeting performance requirements.	M	Not Applicable
3.2.5	**Ease of use** Ability for the platform to be user-friendly with instructions written in simple, clear language and the menus easy to tap to enable easy completion of tasks.	M	Not Applicable

#	Description	Priority	Notes
3.2.6	**Accessibility** Ability for the platform to be accessible to the user in formats that comply with AODA requirements.	M	Refer to the AODA website for details
3.2.7	**Privacy** Ability for the platform to display information that is compliant according to PHIPA legislation. Maintain the confidentiality of information relayed must as per policy.	M	Not Applicable
3.2.8	**Security** Carry out user identification using a health card number and unique ID/password. Implement data protection measures to avert and reinforce security breaches.	M	Not Applicable
3.2.9	**Interoperability** Ability for the platform to be interoperable with provincial repositories.	M	Not Applicable
3.2.10	**Portability** Ability for the platform to be used on different operating systems, browsers and devices without any change in performance.	M	Not Applicable
3.2.11	**Reportable** Ability for the platform to report the number of users who are registered to the application, are using the application, and how much use is occurring.	M	See below: OHDS Playbook Policy Direction Needs to comply with the Digital Health Reporting and Performance Policy

3.3 Virtual Visits

For further information, please refer to the Virtual Visits Solution Requirements.

3.4 Online Appointment Booking (OAB)

For further information, please refer to the OAB requirements.

4. User Interface Requirements

4.1 Information Content Management

Information Content Management refers to the process of collecting, delivering, retrieving, governing, and managing information. For the purpose of this document, information content management is being explored in the context of health information being collected, delivered, retrieved, governed, and managed by health care consumers. The Information Content Management section of this document will describe data requirements for PPPs, data contribution readiness requirements, data release guidelines, clinical considerations, and a guide for organizing information within a PPP. This supports the *Digital Health Information Exchange Policy* , which states that filling the gaps to enable seamless access to integrated patient records is necessary to reduce fragmentation, redundancies and inconsistent user experiences.[4] Regarding PPPs (other than legislative requirements as described in PHIPA), based on an information content perspective, established standards do not exist regarding the minimum data sets that should be made digitally available via patient access channels. Various factors need to be considered before an organization decides to digitally release PHI. Fundamentally, this document advocates for users having easy access to all of their medical data.

4.2 Minimum Data Requirements

The platform needs to be able to display the data as listed in the table below, as drawn from the IPS minimum data set guidance. Please refer to the IPS Composition for more details.

#	Requirement	Priority	Notes
4.2.1	Medication Summary	R	Gives a history of current and previous medications.
4.2.2	Allergies	R	Gives a list of known documented allergies.
4.2.3	Problem List	R	Provides a list of current documented conditions.
4.2.4	Immunization	R	Provides a history of immunizations.
4.2.5	History of Procedures	R	Provides a history of visits and procedures attended.
4.2.6	Medical Devices	R	Provides a list of medical devices used by the user e.g. insulin pump, central lines, etc.
4.2.7	Diagnostic Results	R	Should include all forms of diagnostic test results, e.g. lab, Radiology, Cardiology.

4.2.8	Clinical Notes	R	Provides the notes from clinical interactions.
4.2.9	Vital signs	R	A history of recorded vital signs e.g. BP, Height, weight, BMI.
4.2.10	Past History of Illness	R	Details and summary of past history of illnesses.
4.2.11	Pregnancy	R	Details on current or historical pregnancies.
4.2.12	Social History	R	Social, economic and cultural information.
4.2.13	Functional Status	R	Current and historical results from any functional status evaluations e.g. PROMs, details from home and Community Care related to activities of daily living.
4.2.14	Plan of Care	R	Provides any care plans developed both current and historical. Information should be dynamic to reflect real time changes.
4.2.15	Advanced Directives	R	Provides details on any current and previous directives, includes any code status. [13]
4.2.16	Appointments	R	Ref. OAB requirement plus hospital appointments.
4.2.17	e-Referrals	R	Provides current and historical information on e-Referrals.
4.2.18	Education Materials & Resources	R	Educational materials and resources for both using the solution and health related information.

5. Technical Requirements

5.1 Provincial Health Information Protection Act (PHIPA)

Refer to Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, Sched. A

5.2 Privacy and Security Requirements

Privacy

PPPs involve the collection, use and disclosure of PHI and personal information (PI). As a result, organizations and clinical users of PPPs 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. Other statutes that may apply include the Personal Information Protection and

Electronic Documents Act (PIPEDA) for personal information exchange and Canadian Anti-Spam Legislation (CASL) for secure messaging and emailing.[14] Delivering clinical health information electronically can present certain risks that must be considered. The following situations should be planned for by organizations and teams using PPPs:

PATIENT PORTAL

- Patient's clinical information gets into the hands of the wrong patient
- Sharing clinical information with the wrong patient
- Change in custody resulting in unauthorized access to pediatric patient's PHI
- Secure message sent to the wrong patient
- Sensitive information that could cause harm if seen by the patient is released unintentionally

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 and patient portal platforms that meet a minimum set of privacy and security requirements. This includes taking reasonable steps to confirm that technologies used by the platform's users permit PHI to be shared in a private and secure manner.[15]

Information Security

Health care organizations and clinical users should ensure their 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 information, security incident response, encryption, logging & monitoring, operational procedures, and other mechanisms.

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

The following requirements are guided by privacy considerations:

#	Requirement	Priority	Notes
5.2.1	Publish a notice of its information practices relevant to its PPP and services.	M	At a minimum, the notice must describe how the vendor handles and protects personal and health information and privacy rights of users.
5.2.2	Have a designated employee responsible for privacy.	M	Contact information for the designated privacy official must be publicly accessible on the vendor's website.
5.2.3	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

#	Requirement	Priority	Notes
			management, information security, business continuity and disaster recovery, access, correction and complaint practices.
5.2.4	Provide an electronic audit trail of all encounters including a log of all accesses and transfers of PHI.	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 PHI; and • 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.
5.2.5	Provide an electronic audit trail of access to the solution trail.	M	The 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)

#	Requirement	Priority	Notes
			• System time must be synchronized with a trusted source to maintain audit trail integrity • Be protected to ensure audit integrity and from unauthorized access, modification, and destruction
5.2.6	Implement 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 PHI 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.
5.2.7	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 of seeking to participate in the Verification program. • PIA must have been completed by a certified professional with any of the following credentials: obtained through the International Association of Privacy Professionals (IAPP): Certified Information Privacy Professional (CIPP/C); Certified Information Privacy Manager (CIPM); Certified Information Privacy Technologist (CIPT) or 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 healthcare context, a description of the data flows 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 per the PIA guidelines issued by the Information and Privacy Commission of Ontario[11] concerning healthcare.

#	Requirement	Priority	Notes
			• 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 a status on 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 utilized. Risks assessed as medium must have a clear mitigation plan with timelines for closure within six months of risk being identified. Medium risks must be updated once mitigation activities have been deployed • 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 OH. • PIAs must be refreshed every 3 years or earlier if/when there has been a change in the solution, legislation, policy or business operations of the solution provider(s). e.g., if there is a change in the way the information is collected, used and/or disclosed, that may impact the privacy of health information or to privacy rights.
5.2.8	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 the PPP solution submitted to this process 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).

#	Requirement	Priority	Notes
			• 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 used. Medium risks will show clear mitigation plans for closure within 6 months of these risks being identified. It is recommended that low risks be identified, monitored, and closed where practical and summary are shared with and reviewed by OH. • The TRA must refreshed every 3 years or earlier if / when there is a change in the solution, legislation, policy or business operations of the solution provider(s)). e.g., if there is a change in the way the information is collected, used and/or disclosed, that may impact to the privacy and/or security of health information or to privacy rights. The TRA must include the results of a vulnerability scan and penetration test.
5.2.9	Perform periodic vulnerability assessment scans/.	M	Vulnerability assessment scans are to be done at a minimum on a quarterly basis or when there has been a major software release, change in architecture or infrastructure. Vulnerability scans must include the application and application infrastructure. For hosted environments, the hosting provider may need to submit their own VA scan results. Latest vulnerability scan results are to be submitted with the TRA. Evidence that quarterly scans have been completed may be requested within the 3-year TRA refresh cycle.
5.2.10	Will perform periodic penetration tests.	M	Penetration tests are to be done, at a minimum, on an annual basis or when there has been a major software release, change in architecture or infrastructure. Penetration tests must include the application and application infrastructure where possible. For

#	Requirement	Priority	Notes
			hosted environments, the hosting provider may need to submit their penetration test results. The latest penetration test results are to be submitted with the TRA. Evidence that annual tests have been completed may be requested within the 3-year TRA refresh cycle.
5.2.11	Will meet security and privacy controls.	M	Solution providers must follow general security guidance based on ISO 27002 control objectives. Please refer to the 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, 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 • Cryptography • Security Logging and Monitoring • Electronic Service Provider
5.2.12	Will provide a comprehensive agreement framework for the PPP solution and related services, including for any third party it retains to assist in providing these services.	M	Solution and third-party provider agreements will at a 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 to comply with applicable legislation, including but not limited to those listed above.

#	Requirement	Priority	Notes
5.2.13	Will support healthcare organizational or clinician retention obligations and policies.	M	Solutions facilitate or enable 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.
5.2.14	Will ensure solution provider stores all PHI on systems located inside Canada.	M	Storing PHI on servers hosted within a Canadian data centre (including backups) will likely increase users' confidence and comfort and their willingness to use the platform.
5.2.15	Will ask users to consent to PHI being stored outside their province of residence.	M	Users shall be advised the system may store PHI outside their province of residence and their consent to that storage. This can be done through a "Terms of Use" or "User Agreement", written in plain language, that must be accepted during the user account creation process.

Appendix A: Recommendations to Phasing Compatibility Standards

While this document cannot prescribe the methodology for phasing compatibility standards, it would make the following recommendations:

1. Clearly determine current compatibility shortfalls
   Itemize and clearly delineate the exact areas or items that are not meeting the specific criteria
2. Size the effort to remove the shortfalls
   Determine the overall cost in effort, time, and resources to close the gaps in compatibility. Note that in cases where existing solutions are in place, the cost of remediation may be greater than sourcing a new solution
3. Consult all stakeholders
   Determine priorities based on gathering feedback from all stakeholders
4. Establish a roadmap
   Based on this feedback, determine where your organization wishes to invest their efforts

Endnotes

[1] Ministry of Health (2019, October 15). *Patient Declaration of Values for Ontario*.
[2] Walker, J., Leveille, S. G., Ngo, L., Vodicka, E., Darer, J. D., Dhanireddy, S., ... & Delbanco, T. (2011). *Inviting patients to read their doctors' notes: patients and doctors look ahead: patient and physician surveys. Annals of internal medicine*, *155*(12), 811-819.
[3] Maybee, A., & Greenberg, A. (2019, March 7). *Progress with patient portals. Health Quality Ontario*.
[4] Ontario Health. (2020a). *Draft Digital Health Information Exchange Policy*.
[5] Kindig, D. A., Panzer, A. M., & Nielsen-Bohlman, L. (Eds.). (2004). *Health literacy: a prescription to end confusion.* National Academies Press.
[6] HIMSS (n.d.). *Interoperability in Healthcare*.
[7] HMT Mag. (2013, February 21). *Empowering patients through advanced EMR use. Healthcare Innovation*.
[8] Health Quality Ontario. (n.d.). *Patient Reported Outcome Measures (PROMs)*.
[9] Kingsley, C., & Patel, S. (2017). *Patient-reported outcome measures and patient-reported experience measures*. Bja Education, 17(4), 137-144.
[10] eHealth Ontario. (n.d.). Single Sign On - Patient Context Sharing Standard.
[11] Vreeman, D. J., & Richoz, C. (2015). *Possibilities and implications of using the ICF and other vocabulary ps in electronic health records. Physiotherapy Research International, 20*(4), 210-219.
[12] OntarioMD (n.d. c). *EMR Specifications Library*.
[13] Lehmann, C. U., Petersen, C., Bhatia, H., Berner, E. S., & Goodman, K. W. (2019). *Advance directives and code status information exchange: A consensus proposal for a minimum set of attributes*.
[14] Office of the Privacy Commissioner of Canada (2019). *Privacy Laws in Canada*.
[15] Alpert, J. M., Krist, A. H., Aycock, R. A., & Kreps, G. L. (2016). Applying multiple methods to comprehensively evaluate a patient portal's effectiveness to convey information to patients. *Journal of medical Internet research*, *18*(5), e112.

References

Canada Health Infoway (n.d.*). Standards Access*.
Cerner (n.d. a). *DSTU 2 Overview*.
Cerner (n.d. b). *FAQs*.
ClinicalConnect (n.d.). *About ClinicalConnect*.
Epic (n.d.). *Epic on FHIR*.
Ontario. (2019, December 1). *Ontario Health Teams: Digital Health Playbook*.
Ontario (2020, April 20). *Digital Health Information Exchange Policy*.
Ontario Health Quality (2020, March 12). *Adopting and Integrating Virtual Visits into Care: Draft Clinical Guidance*.