Ontario

Ontario Health Teams

Harmonized Information Management Plan (HIMP): Guidance Document

March 31, 2021

Ontario

Table of Contents

Ontario

Ontario Health Teams

Harmonized Health Information Management Plan: Guidance Document

Introduction

Implementation of Ontario Health Teams (OHTs) is fundamental to the government's plan to build a modern, sustainable and integrated health care system that better connects health care providers and provides services focused on the patient/client. OHTs require timely and shared access to quality data and information to enable effective and efficient care delivery.

Developing and implementing a solid and resilient harmonized information management plan (HIMP) will ensure emphasis on acquiring and managing the data and information required to meet the OHT's goals of integrated care, while protecting privacy. This includes plans to enable authorized members of an OHT to securely collect personal health information (PHI) and disclose PHI to one another where needed for the purposes of integrated care delivery, planning (e.g., pooling or aggregating information to understand population health needs and cost drivers, for population segmentation, integrated care pathway design, etc.), quality improvement, and evaluation.

The HIMP would also guide the OHT's activities in the protection of privacy and confidentiality of individuals' PHI, and personal information (PI) where relevant, to ensure legal requirements are met and high standards of information protection and ethical practices are consistently observed across all members of the OHT. OHTs would need to consider their needs for the collection, use and disclosure of PHI, and where statistical/aggregate information and/or de-identified data would be sufficient. The plan may also touch on implications for the security of the data.

The purpose of this guidance document is to provide some common concepts and links to resources to assist OHTs in the development of their HIMPs, that are to be based on each OHT's unique circumstances. **This document is not meant to be a comprehensive resource and is subject to change without notice. It is not intended to provide any legal or privacy compliance advice, as OHT members would need to seek their own independent legal advice in the development and implementation of their plans.**

As a requirement of the Implementation Support Transfer Payment Agreement between the Ministry of Health (the ministry) and each OHT, the OHT will be asked to summarize its HIMP in a template which will serve to attest to the completion of the OHT's HIMP. Note that the ministry will not be approving HIMPs, and does not need to review the detailed components of a HIMP.

The ministry will use the summary submitted in the template as part of the ongoing dialogue to understand OHT needs and priorities, identify best practices as well as obstacles encountered by OHTs, and to determine additional supports that might be required in 2021/2022 and beyond.

Key content topics to include in a HIMP

(*detailed HIMP not to be submitted to the ministry)

- The 2021/2022 OHT clinical activities and program or service objectives (for example, for clinical care, service integration, care coordination, and patient/client impact), and the goals related to the management of information resources to meet those objectives.
- Identification of the OHT's information management (IM) needs and priorities based on the OHT model i.e., common OHT members' needs towards achieving the quadruple aim (population health, patient/client experience, efficiency and provider experience).
- The OHT's plans and tactics for IM and privacy, and security where relevant, that would meet the above objectives, with associated timelines and key milestones.
- Identification of known gaps, challenges and risks associated with information management and privacy, and mitigation strategies.
- Relevant components:
    - Information governance and accountability structures and processes (including providing clarity around accountability, responsibilities and decision making), including for data management and privacy.
    - Data management - would include identifying core data sets and data sources, as well as data flows between OHT members and with other health system partners - to enable collection/use/disclosure of PHI, and for sharing of statistical/aggregate information and/or de-identified data. Related topics might be data sharing needs, agreements, data quality, and standards between OHT members. Data flow diagrams and analyses of the data flows would help to identify the effects and/or implications throughout the different stages of IM (planning, creation, collection, organization and storage, use, and disposition).

- Where appropriate, the plans would describe what provincially available digital health solutions (e.g., provincial clinical viewers) or other digital health solutions the OHT is using or proposing to use to support the implementation of their plans and tactics for information management.
- Privacy considerations and implications, such as key privacy assessment findings; privacy authorities; harmonizing privacy policies, practices and procedures; and controls and safeguards to ensure the protection of PHI (for example, monitoring systems access through scheduled or ad-hoc audits, role-based access, notifications for breaches, consent management, etc.)
- Any technical and security considerations, highlighting any additional measures that may need to be put in place.

At a provincial level, the ministry has received comments on potential issues hindering OHT implementation towards the mature end-state, for example, related to information sharing within the OHT for population health planning purposes. In their plans, OHTs would need to identify IM issues that are hindering OHT implementation and approaches to achieve the outcomes within the current environment (for example, given the current operational, financial, legislative and regulatory landscape).

The HIMP as a tool to support development to maturity

A living document that is expected to evolve over time, the initial HIMP would reflect the OHT's near-term objectives in the current environment (for example, with respect to current target populations, care re-design priorities, and financial, legislative and regulatory landscape, etc.). As the OHT matures, plans would incorporate longer-term IM strategies and tactics towards organizing and delivering care that is more connected to patients/clients in their local communities.

Ideally the HIMP should be reviewed for updates regularly (for example, annually), as well as revised when there are material changes that would impact implementation plans. For example, when new members are added, when populations are expanded, or when their plans grow to encompass the requirement for additional data flows.

Key references

The following topics and resources may assist OHTs in creating their HIMPs.

IM and Privacy Planning
A strong plan documents the approach to dealing with IM and privacy factors that affect the specific planned services and objectives of an OHT, complementing operational, financial, human resource, information technology, and other related plans, to target the quadruple aim (population health, patient/client experience, efficiency and provider experience). A mature plan would include activities to ensure timely and shared access by OHT members to quality data and information for the purposes of integrated care delivery, planning, quality improvement and evaluation. The planning would take into consideration privacy and security measures to ensure the secure management of data and information throughout its lifecycle.
Information Management (IM)
What is IM? IM means the planning, implementation, supervision and control of explicit and iterative processes, procedures and structures that govern the collection, use, disclosure, retention and disposal of information in accordance with the law, policy and standards. It includes establishing disciplined and consistent practices related to the strategic management of IM life cycle: planning, creation, collection, protection and evaluation/disposition of data and information assets. **Why is this important to OHTs?** Effective IM and data flows between members and with other health system partners are key to enabling OHTs' goals and objectives: • For providers, enables their access to the quality information they need, when they need it, and streamlined channels for delivering services, in order for them to provide quality care. • For organizations, equips OHTs with IM policies and processes that allow them to focus their efforts on providing care to patients/clients while minimizing time lost to inefficient and redundant activities related to data and information. • For patients/clients and caregivers, provides reassurance that their privacy and confidentiality of individuals' PHI is protected, and ensures appropriate access

to their PHI. It also means that patients/clients don't need to tell their story over and over. Other benefits include:

- Provides transparency for patients/clients in how their information is being used by OHT members to improve their care.
- Gives patients/clients and caregivers guidance on how to address issues related to information, for example for access requests or in the case of a breach.

Why a "harmonized" IM plan?

Developing plans to harmonize approaches across OHT members over time, where relevant and feasible, will help facilitate the achievement of the OHT's goals. "Harmonized" is intended to reflect how OHT members have collaboratively assessed their needs, priorities and risks, and developed plans that may reflect, for example, new or shared policies and practices; standards adoption; education and training; or business management, with respect to the OHT's IM activity.

This could include leveraging existing processes, structures, and documents, and adopting best practices over time, while providing an opportunity to identify innovative approaches. The plan would also take into consideration individual and collective responsibilities across OHT members, and identify approaches to shared decision-making around information management and privacy, where relevant.

Given the wide range of members within an OHT, development of a HIMP would provide a mechanism to facilitate early discussions on information governance and accountability structures and processes, for example for data quality management, privacy and security. It also helps inform shared goals amongst OHT members.

Privacy*

Privacy is a fundamental right of every Ontarian. In order to protect that right, Ontario's laws, including FIPPA and PHIPA, contain rules to protect people's PHI and PI, including rules for how PHI and PI are collected, used and disclosed.

Why is this important to OHTs?

For purposes of the delivery of health services, OHTs should collectively review the health information privacy landscape and related accountabilities and responsibilities under law. Important obligations exist under Ontario's privacy legislation, applied

respectively to individuals, provider staff, management, organizations, and boards, including private firms in some cases.

OHTs should consider and determine IM practices against their connected care objectives. Privacy needs to be at the core of integrated care planning and design. The services provided and the model of integrated care should inform and drive reviews amongst OHT partners, including consideration of coordinated safeguards to protect privacy and confidentiality. OHTs should consider their needs and legal authorities for the collection, use and disclosure of PHI and PI, and where statistical/aggregate data or de-identified data would be sufficient.

Harmonizing relevant privacy policies and procedures over time would help to ensure common privacy standards, practices and processes across OHT members, for example, for privacy breach management, and for complaints and inquiries management.

Key definitions

Personal health information (PHI) means identifying information about an individual in oral or recorded form, if the information relates to the physical or mental health of the individual, the health history of the individual's family, the identification of an individual's health care provider, eligibility for coverage or payment for health care, and the individual's health number, as defined under the *Personal Health Information Protection Act, 2004 (PHIPA)*.

PHIPA's purposes include, but are not limited to, establishing the rules for the collection, use and disclosure of PHI to protect individuals' privacy, while facilitating the effective provision of care; to provide individuals with a right of access to PHI about themselves and the right to seek correction of such information, with limited exceptions; and to provide effective remedies for contraventions of the Act.

Note that under PHIPA, PHI also includes identifying information about an individual that is not health-related but that is contained in a record that includes PHI about the individual. Such records are referred to as "mixed records" and considered as PHI.

Personal Information (PI) is recorded information about an identifiable individual (such as name, address, telephone number, age, etc.) under

- the *Freedom of Information and Protection of Privacy Act (FIPPA)* and
- the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)*.

Information can be recorded in any format, such as paper records, electronic records, digital photographs, videos or maps.

FIPPA also provides a right of access to information (non-PI) by the public under the custody and control of "institutions", with limited exemptions and exclusions, and requires government organizations to protect PI and to provide individuals with a right of access to their own PI. Some OHT member organizations (e.g., hospitals) are institutions under FIPPA.

* Please refer to PHIPA, FIPPA, MFIPPA and any other applicable laws for the relevant legislative and regulatory requirements. Some resources are listed at the end of this document for further reference.

Privacy Risk Assessment

Why is this important to OHTs?

This process ensures that OHTs have assessed IM and privacy factors in OHT planning, options analysis, and ultimate service delivery. Documentation including Privacy Impact Assessments (PIA) and Threat Risk Assessments (TRA) demonstrate a comprehensive approach to service delivery planning and use of best practices for OHTs. Key findings and relevant mitigations from relevant PIAs and TRAs would be factored in the OHT's HIMP over time.

A PIA is a formal risk management tool used to identify and document the actual or potential effects that a proposed or existing information system, technology or program may have on individuals' privacy. A PIA also identifies ways in which privacy risks can be mitigated. Please refer to the Privacy Impact Assessment (PIA) Guidelines for PHIPA for a self assessment tool on the IPC website.

Information sharing within the OHT

To enable privacy-protected information sharing between OHT members, thorough identification of needs and options analysis should be conducted. Options would take into consideration approaches for the OHT to address its needs, such as, but not limited to, considerations around: authorities to collect/use/disclose PHI along the data flows; and express consent vs implied consent.

An assessment of approaches to share PHI, for example, would take into consideration authorities and responsibilities of OHT members as one or more of the following (not an exhaustive list): a health information custodian (HIC), Single HIC,

non-HIC, agent, Health Information Network Provider (HINP); and the use of digital health and other enablers.

OHTs should be aware that some OHT members (for example, school boards) may not be HICs under PHIPA, and, as such, information sharing between and among these organizations may be affected.

Please refer to PHIPA and the IPC website for more information. The application to act as a Single HIC can be found here.

Key resources

The following are some resources OHTs may leverage in the development of their plans:

Ontario Information and Privacy Commissioner	
Circle of Care – Sharing PHI for health care purposes	Link
Frequently asked questions PHIPA	Link
Privacy Diagnostic Tool (*is focussed on PI)*	Link
Privacy Impact Assessment Guidelines for PHIPA	Link
De-Identification Guidelines for Structured Data	Link
Applying PHIPA and FIPPA/MFIPPA to PHI	Link
Ontario's Freedom of Information and Protection of Privacy Act – A Mini Guide	Link
Health Information Custodians Working for Non-Health Information Custodians – Fact Sheet	Link
Ontario's Municipal Freedom of Information and Protection of Privacy Act – A Mini Guide	Link
Other resources	
CIHI's Data Source Assessment Tool	Link
Application to act as a single health information custodian	Link