Briefing on privacy management and data sharing for OHT executives and governors, and OHT member organization executives

[draft tool 1 in the privacy management and data sharing (PMDS, or privacy) toolkit]

(Last updated 3 November 2026)

This briefing provides the context for, and key actions involved in (and resources for), leading and governing an effective privacy management and data sharing (PMDS) program within and across OHT member organizations. An appendix to this briefing provides an overview of the other tools in this PMDS toolkit, as well as the tools in a complementary data-sharing agreement (DSA) toolkit.

Context for leading and governing an effective PMDS program within and across member organizations

Effective privacy management and data sharing is foundational to advancing integrated care, enabling coordinated clinical pathways, implementing programs, monitoring performance across OHTs and their member organizations, and responding directly to challenges identified by OHTs as barriers to integrated-care delivery.

As we note in the RISE brief that accompanied the DSA toolkit: "[Privacy management and data sharing need] to become the '**new normal**' and to be actively supported among OHT member organizations by OHTs and Primary Care Networks (PCNs). The potential benefits of data sharing have long been clear; now we have an opportunity to ramp up efforts to support this transition, to ensure the benefits are realized for both clients and for clinicians, and to minimize the risks for clinicians and organizations. (We use the term 'clients' to mean patients, families and caregivers, residents of long-term care homes, and other recipients of healthcare services.) 'Playing it safe' has – until now – often meant not sharing data. In future, 'playing it safe' should mean safely and efficiently [managing privacy and] sharing data in a way that complies with existing legislation (Personal Health Information Protection Act, or PHIPA, 2004) and regulations (e.g., pertaining to privacy and information management), adheres to policy and contractual obligations (e.g., Ontario Health atHome contracts prohibit storing data on servers outside Canada), respects Indigenous data sovereignty and governance, meets Ontarians' rising expectations for integrated care, adds clinical and operational value, and mitigates risk appropriately.

OHT executive directors and collaboration councils, as well as OHT member organization executives, can play an important role in leading and governing PMDS as a means of achieving **OHT deliverables** such as:

1) primary care (PC) access, attachment and enablement, including PCNs, PCN Clinical Leads, provincial digital priorities (e.g., Central Intake, eReferral, Mental Health and Addictions Provincial Coordinated Access, and Online Appointment Booking), and cancer-screening participation
2) integrated clinical priorities, including chronic disease prevention and management (CDPM) and Alternative Level of Care (ALC) planning
3) OHT capacity building, including OHT membership expansion and engagement-capable environments
4) funding for PC access and attachment, including attachment targets, submissions for new or expanded Interprofessional Primary Care Teams, clinical services for unattached patients, Supported Attachment model, Initial 12-specific activities, and lower-limb preservation (LLP) integrated clinical pathway.

As stated in article 2 (foundation for data sharing) of the DSA template:

- the Parties [OHT member organizations] agree that they have shared objectives that rest upon appropriate data sharing, and that data sharing can enable improved patient outcomes, better experiences, and more efficient use of resources
- data sharing is enabled by good data governance.

OHT executives and governors have a key role to play in achieving shared objectives and in data governance.

Four examples of data sharing in primary and integrated care

In the table below we provide four examples of data sharing involving OHT member organizations, each of which has unique PMDS considerations that the data-sharing agreement (DSA) template and related tools can help to address.

Examples	Primary-care instances	Additional notes
Sharing personal health information (PHI) with a prescribed entity like OH	• Sharing data for health-system planning, quality improvement and evaluation via the Managed File Transfer (MFT) or Data Submission Portal (DSP)	A HIC that is part of your OHT and PCN could act as the lead to compile and submit data on behalf of multiple practices, acting as a HIC-Agent
Sharing confidential business information (CBI)	• Sharing data to support primary care (PC) **recruitment, tracking and communications** • Sharing data to support PC **attachment** • Sharing data to support regional **interpretation** services	CBI includes financial information, internal operational information, contractual and commercial information, and information about a member's employees, contractors, and agents
Sharing PHI among other health information custodians (HICs) providing healthcare or assisting in the provision of healthcare	• Sharing data via a **secure messaging** application (e.g., among palliative-care team members) • Sharing data via a **web-based technology platform** such as CHRIS (for home care) and eReferrals (for specialty care)	Ontario Health is the health information network provider (HINP) for CHRIS, and also plays multiple roles for the different services and technologies it provides (e.g., prescribed organization for the provincial EHR, prescribed entity in respect of its role for cancer care, prescribed 'person' for the Ontario Cancer Screening Registry, etc.; sharing of PHI must be authorized by a 'lane' (e.g., circle of care purpose)
Sharing PHI among other HICs and among non-HICs (acting as HIC-Agents) providing healthcare or assisting in the provision of healthcare	• Sharing data to support **EMR creation** for newly attached patients • Sharing data to support integrated **chronic disease prevention and management** or to support **cancer screening**	One member may provision accounts on its information system (e.g., EMR) to employees, contractors, or its agents drawn from other members (e.g., outside clinicians like a shared nurse, service providers like Meals on Wheels); sharing of PHI must be authorized via a 'lane' (e.g., circle of care purpose)

Four 'personas' involved in PMDS in primary and integrated care

In the table below we provide four 'personas' involved in PMDS in OHTs, the challenges they may encounter, and possible solutions to these challenges.

'Persona'	Challenges → possible solutions
Family physician or nurse practitioner (as a HIC-based regulated health professional)	• Technical capacity and workload constraints, particularly for solo or small HICs → Consider working with a HIC-Agent supported by your OHT and PCN • Double documentation (with own EMR and any 'separate' technology) → Consider how to leverage interoperability

'Persona'	Challenges → possible solutions
Medical office assistant (as a HIC-based non-regulated health professional)	• Technical capacity and workload constraints → Consider taking the last three steps on the next slide (policies and procedures, safeguards, and training)
Home care coordinator (acting as the HIC-Agent of a medical clinic HIC) who provides services on behalf of the clinic (e.g., navigation, referrals to community supports)	• Same as above and below (recognizing that the first solution in row 1 above is the scenario here)
PCN partners who you may agree can be provisioned with an account on your information system (e.g., EMR) as part of a circle of care	• Risk aversion and liability concerns → Consider taking all of the steps on the next slide (including a data sharing agreement, minimum privacy and security standard, and privacy contact person)

Key actions involved in (& resources for) leading and governing an effective PMDS program

In the table below we list the actions that OHT executives and governors (and membership organization executives) can take in leading and governing an effective PMDS program. The list draws heavily on the IPC privacy-management handbook for small healthcare organizations, and can be considered a 'cheat sheet' for this helpful resource (albeit not a comprehensive summary with, for example, privacy-impact assessments not covered).

Actions involved in (and resources for) leading and governing an effective PMDS program
At the level of the OHT • Set a privacy-respectful tone and foster a privacy-first culture, which includes reminding fellow executives and governors that a PMDS program is needed to demonstrate compliance with PHIPA and care for their patients, including earning and keeping patients' trust • Ensure your OHT's collaborative decision-making agreement (and any related PCN agreement) endorse PMDS in support of primary- and integrated-care initiatives • Discuss periodically, in your OHT collaboration council meetings (and PCN leadership council meetings), successes and challenges in PMDS in support of primary- and integrated-care initiatives
For any primary- and integrated-care initiative that involves PMDS • Encourage all involved parties to sign a data-sharing agreement (DSA) → see the appendix for a DSA template that can be adapted to local needs, as well as four tools to support its use   ○ Note that schedule A in the DSA template refers to a minimum privacy and security standard that touches on many of the points below (e.g., privacy contact person, policies and procedures, safeguards, and training) • Ensure any agreements with service (e.g., EMR) providers adhere to PHIPA requirements (e.g., by ensuring an EMR is certified by OntarioMD or a virtual-visit solution is verified by Ontario Health) and align to the terms set out in schedule D of the data-sharing agreement (DSA template) including in our DSA toolkit

At the level of a member organizations, particularly PC practices → encourage them to use **tools 3 and 4** to identify actions that can be taken at the practice leader and staff levels, respectively, and resources that can be easily adapted for use
• Have appropriate governance and accountability mechanisms in place
  ○ Designated privacy officer with a job description
  ○ Inventory of the PHI in its custody and control (updated periodically)
  ○ Business continuity and disaster recovery plan, as well as succession plan

- Have a written privacy policy (i.e., its privacy commitments and the standards by which it manages information) and make publicly available a privacy notice
- Have appropriate safeguards in place
  - Technical safeguards (e.g., use only practice/organization-approved email, messaging and videoconference accounts; use strong passwords; verify a patient's identity before engaging)
  - Physical safeguards (e.g., keep technology in a secure location)
  - Administrative safeguards (e.g., maintain authorizations on a need-to-know basis)
  - Safeguards specific to: 1) email and secure-messaging applications; 2) videoconferencing; 3) artificial intelligence (AI), such as AI scribes; and 4) mobile devices
  - Enable logging (of events in digital systems), audit (the logs and other records), and monitor (for unusual patterns and anomalies that may be indications of attacks or unauthorized activities)
  - Take additional preventive steps, such as avoiding the use of faxes, which are a significant source of privacy breaches, and training staff to detect, avoid and report phishing attacks (and inform patients as well)
- Have procedures in place
  - Staff signing confidentiality agreements
  - Staff completion of an annual attestation form to acknowledge they have read, understood and agree to comply with policy, safeguards, and procedures and that they understand the potential consequences of non-compliance
  - Staff training about policy, safeguards and procedures to ensure they can keep PHI safe and secure and know how to identify and report potential breaches (and tracking of the training)
  - Access controls assigned on a need-to-know basis
  - Record-keeping practices (e.g., service-provider agreements; third-party data-sharing agreements; staff training, confidentiality agreements and attestation forms)
  - Record retention and destruction procedures
  - Privacy breach response protocol, including for cyberattacks and ransomware
  - Breach log to support reporting of annual breach statistics to the IPC
  - Procedures to respond to patients who make access or correction requests (e.g., standardized form, timelines, fees, and redaction procedures), or who have complaints or inquiries about privacy practices
- Monitor and periodically review the PMDS program

DRAFT

Proposed citation: RISE. Briefing on privacy management and data sharing for OHT executives and governors, and OHT member organization executives [tool 1 in the OHT privacy management and data sharing (PMDS, or privacy) toolkit]. Hamilton: McMaster Health Forum, 2026.

Note from RISE: This tool is meant to be read in conjunction with an appendix that provides an overview of the other tools in this PMDS toolkit, as well as the tools in a complementary data-sharing agreement (DSA) toolkit. RISE prepares both its own resources (like the RISE brief) that can support rapid learning and improvement, as well as provides a structured 'way in' to resources prepared by other partners and by the ministry. RISE is supported by a grant from Ontario Health to the McMaster Health Forum. The opinions, results and conclusions are those of RISE and are independent of Ontario Health and the Ontario Ministry of Health. No endorsement by Ontario Health or the ministry is intended or should be inferred.



This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International license, which enables re-users to distribute, remix, adapt, and build upon the material in any medium or format for non-commercial purposes only, and only so long as attribution is given to the creator.