Briefing on privacy management and data sharing for PCN Clinical Leads (and PCN leadership councils)

[draft tool 2 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), supporting primary-care (PC) practices in building an effective privacy management and data sharing (PMDS) program. 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 supporting primary-care practices in building an effective PMDS program

Primary Care Networks (PCNs) have **five functions**, and for each of them a PCN Clinical Lead (and PCN leadership council) can help to demystify the related PMDS considerations:

1) connects primary care within the OHT (e.g., participant recruitment and tracking; communications)
2) bring's PC voice in OHT decision-making
3) advances clinical change management and population health management (e.g., access and attachment; chronic disease prevention and management; cancer screening)
4) facilitates access to clinical and digital supports and improvements for primary care (e.g., OAB, eReferral and Central Intake)
5) local health human resources planning.

PCNs can play an important role in supporting PMDS as a means of achieving **three types of OHT deliverables and PCN expectations**:

1) PC engagement
2) PCN Clinical Lead role, including for PC landscaping, cancer screening and PC attachment (implementation and change enablement), and PCN communications
3) PCNs as peer champions for digital solutions.

All PMDS support needs to address the full PC spectrum – from solo family physicians being paid fee-for-service to small Nurse Practitioner-Led Clinics and other small practices using patient-enrolment models (PEMs) to large Family Health Teams and Community Health Centres and to those covered by the Rural and Northern Physician Group Agreement, among others.

Four examples of data sharing in primary care

In the table below we provide four examples of data sharing involving interprofessional primary care teams (IPCTs) and primary care (PC) practices, 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**	CBI includes financial information, internal operational information, contractual and commercial information,

	• Sharing data to support PC **attachment** • Sharing data to support regional **interpretation** services	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 Ontario, 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 care

In the table below we provide four 'personas' involved in data sharing in IPCTs and PC practices, 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
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) supporting PC practices in building an effective PMDS program

In the table below we list the actions that PCN Clinical Leads (and leadership councils) can encourage PC practices to take in building 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) supporting PC practices in building an effective PMDS program

At the level of the PCN and OHT

- Set a privacy-respectful tone and foster a privacy-first culture, which includes reminding colleagues 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 PCN leadership council meetings and your OHT collaboration 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 primary-care practice → encourage your PC colleagues 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 PCN Clinical Leads (and PCN leadership councils) [tool 2 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.