Privacy-management essentials for staff of health and community care organizations
[draft tool 4 in the privacy management and data sharing (PMDS, or privacy) toolkit]
(Last updated 3 November 2026)

In the table below we list the actions that the staff of health and community care organizations – particularly those involved in integrated-care initiatives led or supported by an Ontario Health Team (OHT) or Primary Care Network (PCN) – can take in operationalizing an effective privacy management and data sharing (PMDS) program. Staff include employees (full-time and part-time), contractors and volunteers. 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). The handbook notes (on page 14) that "the actions of employees, through human error or negligence, are the largest cause of security breaches." Staff acting as HIC-Agents should be clear about the purposes for which they (as agents) are permitted to collect, use and disclose personal health information (PHI), including any limitations, conditions or restrictions, and should understand their role and responsibility to comply with PHIPA and its regulations. All staff may receive PHI by mistake, may be the subject of a phishing attempt, or may suspect a cybersecurity incident.

Actions involved in (and resources for) operationalizing an effective PMDS program

Governance and accountability

- Contribute to a privacy-respectful tone and to a privacy-first culture, which includes reminding fellow staff that a PMDS program is needed to demonstrate compliance with PHIPA and care for your patients, including earning and keeping their trust
- Know who your privacy officer is (e.g., owner of the practice or designated staff person) and how they can help
- If asked by your privacy officer
  - Participate in conducting and periodically updating an inventory of the personal health information (PHI) in your organization's custody and control (types and, for each type, its sensitivity, authority under which it was collected, how it is being used or disclosed, and how long it should be retained)

Policy (what and why)

- Read and periodically re-read your organization's privacy policy (i.e., its privacy commitments and the standards by which it manages information)
- Read (and periodically re-read) your organization's privacy notice (i.e., the written public statement that provides a general description of how your organization protects and handle PHI, how to contact your privacy officer, how to make a request to access or correct PHI, and how to make a privacy complaint)

Safeguards

- Adhere to your organization's security controls, including:
  - 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., ensure your authorizations are on a need-to-know basis)
- Adhere to specific safeguards for:
  - Email and secure-messaging applications (e.g., verify address; encrypt or password-protect document attachments; securely delete emails after they are documented in the patient's record; detect, avoid and report phishing attempts) → see IPC fact sheet on email and IPC fact sheet on phishing
  - Videoconferencing (e.g., use headphones and a closed room; verify patient identity by, for example, asking them to hold up their health card) → see IPC guidance on virtual healthcare visits

- Artificial intelligence (AI), such as AI scribes (e.g., obtain patient consent before use) → see IPC guidance on procuring and using AI scribes
- Mobile devices → see IPC guidance on safeguarding privacy on mobile devices

- Know that your access to and use of digital systems will be logged (i.e., events in digital systems will be recorded), audited (the logs and other records will be examined), and monitored (for unusual patterns and anomalies that may be indications of unauthorized activities) on an ongoing, targeted and random basis
- Take additional preventive steps, such as:
  - When possible, avoid the use of faxes, which are a significant source of privacy breaches
  - Know how to detect, avoid and report phishing attacks (and inform patients as well) → see links above

Procedures (how)

- Sign a confidentiality agreement annually
- Complete an attestation form annually to acknowledge that you: 1) have read, understood and agree to comply with your organization's policy, safeguards, and procedures (including that you will notify your organization of any privacy breach at the first reasonable opportunity); and 2) understand the potential consequences of non-compliance (including corrective measures and disciplinary action)
- Successfully complete annual training – ideally with a post-training quiz – about your policy, safeguards and procedures to ensure you can keep PHI safe and secure and know how to identify and report potential breaches
- Check your access controls regularly, ensuring yours remain assigned on a need-to-know basis
- At the end of your employment or contract, return all property, including any PHI you may have
- If asked by your privacy officer
  - Contribute to good record-keeping practices (e.g., service-provider agreements; third-party data-sharing agreements; staff training, confidentiality agreements and attestation forms)
  - Contribute to record retention and destruction procedures
  - Follow 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
  - Know your role in your organization's privacy breach response protocol, which may be activated with a breach, cyberattack and ransomware
  - Know your role in your organization's business continuity and disaster recovery plan, and succession plan

Monitoring and review

- If asked by your privacy officer
  - Participate in the regular review of your privacy program
  - Contribute to monitoring privacy and security controls (e.g., terminate access privileges for staff whose employment or contract has ended)
  - Contribute to improving based on new insights and lessons learned

Proposed citation: RISE. Privacy-management essentials for staff of health and community care organizations [tool 4 in the 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.