Privacy-management essentials for physicians, nurse practitioners and other professionals working in small primary-care practices and healthcare organizations

[draft tool 3 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 physicians, nurse practitioners and other professionals working in small primary-care practices and other small healthcare organizations can take in building an effective privacy management and data sharing (PMDS) program to support integrated care. 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) building an effective PMDS program
Governance and accountability • Set a privacy-respectful tone and foster a privacy-first culture, which includes reminding colleagues and staff that a PMDS program is needed to demonstrate compliance with PHIPA and care for your patients, including earning and keeping their trust • Designate a privacy officer and provide them with a job description (e.g., owner of the practice or designated staff person) → see sample job description (IPC handbook page 46) • Conduct and periodically update an inventory of the personal health information (PHI) in your 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) → see best practices for destruction (IPC handbook page 35) and see guidelines for de-identifying data • Ensure your 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 • Have a business continuity and disaster recovery plan, as well as a succession plan
Policy (what and why) • Have a written privacy policy (i.e., your privacy commitments and the standards by which you manage information) → see what it should cover (IPC handbook pages 19-22) and a sample policy (pages 47-50) • Make publicly available a privacy notice (i.e., a written public statement that provides a general description of how you protect 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) → see tips for preparing one (IPC handbook page 23)

Safeguards
• Implement (and regularly review) 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., maintain authorizations on a need-to-know basis)
• Ensure 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; ensure strong contractual agreements with vendors) → see IPC guidance on procuring and using AI scribes
- Mobile devices → see IPC guidance on safeguarding privacy on 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) → see IPC guidance on detecting and deterring unauthorized access to PHI
- Take additional preventive steps, such as:
  - Avoid the use of faxes, which are a significant source of privacy breaches
  - Train staff to detect, avoid and report phishing attacks (and inform patients as well) → see links above
  - Include in employment contracts what staff – particularly those who don't normally handle PHI – should do if they receive PHI by mistake, are the subject of a phishing attempt, or suspect a cybersecurity incident

Procedures (how)

- Ensure your staff sign a confidentiality agreement annually
- Ensure your staff complete an attestation form annually 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
- Train your staff regularly (and ideally include a post-training quiz) about your policy, safeguards and procedures to ensure they can keep PHI safe and secure and know how to identify and report potential breaches (and track their training) → see tool 4, which is focused on staff
- Review access controls regularly, ensuring they remain assigned on a need-to-know basis
- Establish good record-keeping practices (e.g., service-provider agreements; third-party data-sharing agreements; staff training, confidentiality agreements and attestation forms)
- Create record retention and destruction procedures → see IPC fact sheet on disposing of electronic media and the IPC case note on secure disposal
- Establish a privacy breach response protocol → see steps to follow in the event of a privacy breach (IPC handbook pages 36-39), sample breach notification (IPC handbook pages 51-53), IPC guidance on responding to a privacy breach, and IPC cases of note related to each of breaches, cyberattacks and ransomware
- Maintain a breach log to support reporting of annual breach statistics to the IPC → see annual reporting
- Develop 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

Monitoring and review

- Oversee your privacy program via regular review
- Monitor privacy and security controls (e.g., terminate access privileges for staff whose employment or contract has ended)
- Improve based on new insights and lessons learned

Proposed citation: RISE. Privacy-management essentials for physicians, nurse practitioners and other professionals working in small primary-care practices and healthcare organizations [tool 3 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.