FREE RESOURCE — 2026 EDITION

PHIPA Compliance Guide for Ontario Healthcare Providers

Step-by-Step Guide for Clinics, Dental Practices, Pharmacies & Allied Health

DSIT Professional Services Inc. | dsitpro.com | Ontario, Canada

Legislation	Personal Health Information Protection Act (PHIPA), Ontario — R.S.O. 2004
Applies To	Health Information Custodians (HICs): physicians, dentists, pharmacies, labs, hospitals, allied health
Regulator	Information and Privacy Commissioner of Ontario (IPC) — ipc.on.ca
Key Risk	Failure to comply can result in fines up to $500,000 and mandatory OPC/IPC reporting

WHAT IS PHIPA AND WHO MUST COMPLY

- PHIPA governs the collection, use, and disclosure of personal health information (PHI) in Ontario.
- Any organization acting as a Health Information Custodian (HIC) is subject to PHIPA.
- HICs include: physicians, nurse practitioners, dentists, pharmacists, optometrists, hospitals, labs, and long-term care facilities.
- If you collect, store, or use a patient's name, health card number, diagnosis, treatment records, or test results — PHIPA applies to you.

DEFINING PERSONAL HEALTH INFORMATION (PHI)

- PHI includes: identifying information about an individual's physical or mental health, health card numbers, health history, healthcare provider information, substitute decision-maker information.
- PHI is broadly defined — even a patient's name combined with the fact they attended your clinic qualifies.
- De-identified information (no reasonable expectation of re-identification) is not PHI.

TECHNICAL SAFEGUARDS REQUIRED

- Encryption at rest: all PHI stored on servers, workstations, and portable devices must be encrypted.
- Encryption in transit: all PHI transmitted over networks must use TLS 1.2 or higher (HTTPS).

- Access controls: PHI access limited to staff with a need to know — role-based access mandatory.
- Multi-factor authentication (MFA): required on all systems containing PHI.
- Audit logging: all access to PHI must be logged with user, date, time, and action.
- EMR/EHR security: your electronic medical record system must be configured per vendor security guidelines.
- Remote access security: VPN with MFA required for any remote access to PHI systems.
- Portable device management: laptops, tablets, and phones containing PHI must be encrypted and enrolled in MDM.

ADMINISTRATIVE SAFEGUARDS REQUIRED

- Written privacy policies and procedures — reviewed and updated annually.
- Designated Privacy Officer — named in writing with defined responsibilities.
- Staff training — all staff handling PHI must receive documented privacy training at hire and annually.
- Third-party agreements — any vendor or service provider handling PHI must sign a Business Associate Agreement (BAA) or equivalent.
- Retention schedule — PHI must be retained for a minimum of 10 years (or 10 years after a minor turns 18).
- Secure destruction — PHI must be destroyed in a manner that makes recovery impossible (shredding, certified wiping).

BREACH NOTIFICATION REQUIREMENTS

- A privacy breach occurs when PHI is collected, used, or disclosed in a manner not authorized by PHIPA.
- You must notify the IPC of breaches that create a real risk of significant harm to patients.
- You must notify affected individuals if there is a real risk of significant harm.
- Breach notification must occur as soon as reasonably possible — no specific time limit, but delay is scrutinized.
- All breaches must be logged — even those that do not meet the notification threshold.
- A written breach response plan must exist and be tested annually.

PHIPA COMPLIANCE CHECKLIST — QUICK REFERENCE

■ **Written privacy policy in place**	Reviewed this year	■ **Privacy Officer designated**	Name documented
■ **PHI encrypted at rest**	Tool confirmed	■ **PHI encrypted in transit**	SSL/TLS verified
■ **MFA on all PHI systems**	Audit completed	■ **Audit logging active**	Logs reviewed monthly
■ **Staff privacy training completed**	Records on file	■ **EMR security settings reviewed**	Vendor hardening applied
■ **Remote access via VPN + MFA only**	Configured and tested	■ **Portable devices encrypted + MDM**	Policy enforced
■ **Third-party BAAs in place**	All vendors covered	■ **Retention schedule documented**	10-year minimum PHI

■ **Breach response plan written**	Tested this year	■ **Destruction process documented**	Certified method used
■ **IPC contact information on file**	ipc.on.ca bookmarked		

GETTING HELP

PHIPA compliance is complex and the consequences of non-compliance are significant. DSIT Professional Services Inc. specializes in PHIPA technical implementation for Ontario healthcare providers — from EMR security hardening and MFA deployment to breach response planning and staff training.

- Book a free PHIPA compliance consultation: dsitpro.com/contact
- Learn more about DSIT's healthcare IT services: dsitpro.com/services