Rapid PHIPA Compliance Gap Assessment Tool

Internal Audit Tool for Ontario Health Information Custodians (HICs)

Use this checklist to identify gaps in your clinic's adherence to the Personal Health Information Protection Act (PHIPA). Check the box for every "Yes" or "Fully Implemented" item.

1. Administrative Safeguards & Accountability

PHIPA requires a designated Health Information Custodian (HIC) to take responsibility for the clinic's information practices.

- ❑ **Designated Privacy Officer:** Have you formally appointed a Privacy Officer to oversee compliance and handle inquiries/complaints?
- ❑ **Written Privacy Policies:** Do you have a comprehensive, written privacy policy that is reviewed and updated annually?
- ❑ **Staff Training:** Is every staff member (including contractors and students) trained on PHIPA requirements upon hiring and through annual refreshers?
- ❑ **Privacy Impact Assessment (PIA):** Has a PIA been conducted for any new software or workflows implemented in the last 12 months?

2. Consent and Collection Limits

Compliance hinges on the principle that PHI should only be collected with consent and for legitimate purposes.

- ❑ **Notice of Purposes:** Is there a "Notice to Patients" posted in your waiting area or on your website explaining why you collect their data?
- ❑ **Implied vs. Express Consent:** Does your staff understand when implied consent is sufficient for the "circle of care" and when express written consent is mandatory?
- ❑ **Minimal Disclosure:** Are workflows designed to ensure only the minimum amount of PHI necessary is shared for a specific task?

3. Physical and Technical Safeguards

The "Reasonable Steps" standard in PHIPA requires robust protection against theft, loss, and unauthorized access.

- ❑ **Access Controls:** Does your clinical software utilize Role-Based Access Control (RBAC) to ensure employees only see the data required for their specific job?
- ❑ **Encryption:** Is all PHI encrypted "at rest" (on servers/hard drives) and "in transit" (when sent via email or portal)?
- ❑ **Audit Logs:** Can your system produce a log showing exactly who accessed a specific patient record and when?
- ❑ **Physical Security:** Are paper files locked in cabinets and are computer screens positioned so they cannot be viewed by unauthorized persons?

4. Breach Protocol and Data Subject Rights

Under PHIPA, patients have the right to access their records, and custodians have a legal duty to report breaches.

- ❑ **Breach Notification Plan:** Do you have a step-by-step plan for notifying the Information and Privacy Commissioner (IPC) and affected individuals in the event of a data breach?
- ❑ **Access Requests:** Is there a formal process to provide patients with access to their records within the 30-day legal timeframe?
- ❑ **Correction Requests:** Is there a documented procedure for patients to challenge the accuracy of their PHI and request corrections?

Gap Scoring Key

"Yes" Score	Status	Action Required
0-5	**High Risk**	Immediate overhaul of privacy infrastructure is needed.
6-10	**Moderate Risk**	Significant gaps in documentation or technical safeguards.
11-14	**Low Risk**	Strong foundation; focus on annual audits and training.