



15 questions before your AI touches **health** or **financial** data.

Drawn from Érable's 60-question AI Governance & Compliance Readiness Review, for Canadian health-tech, credit unions and fintech. Each question cites its source. Tags: [L] law in force · [NIF] enacted, not in force · [B] bill · [G] regulator guidance.

-
- 01** **ACCESS · AC-05**
Is privileged access to your AI platform (model deployment, prompt and guardrail changes, log deletion, keys) restricted, approved and logged?
OSFI B-13 §3.2.7 [G] · PHIPA s.12(1) [L] [S12, S7]
 Yes ☐ Partly ☐ No ☐
-
- 02** **AUDIT LOGGING · AL-01**
Is every AI interaction logged with who asked, when, which records it touched, and whose information it was about?
PHIPA s.10.1 audit log: enacted, not yet in force [NIF] · PHIPA s.12(1) [L] [S7]
 Yes ☐ Partly ☐ No ☐
-
- 03** **AUDIT LOGGING · AL-06**
Are AI-specific incidents (leakage through outputs, cross-user retrieval) recorded as breaches of safeguards?
PIPEDA s.10.3 breach records [L] [S6]
 Yes ☐ Partly ☐ No ☐
-
- 04** **PII / PHI · PH-01**
Is personal or health information detected and redacted before prompts leave your trust boundary?
PHIPA s.30(1) [L] · PIPEDA Sch.1 Principle 4 [L] [S7, S6]
 Yes ☐ Partly ☐ No ☐
-
- 05** **PII / PHI · PH-03**
Have you checked your model provider's prompt-retention and training-on-your-data settings, and documented them?
OPC generative-AI principles [G] · PIPEDA Sch.1 Principle 5 [L] [S8, S6]
 Yes ☐ Partly ☐ No ☐
-
- 06** **DATA RESIDENCY · DR-01**
Do you know where prompts, outputs, embeddings, logs and backups are stored and processed, by region?
PIPEDA Sch.1 cl.4.1.3 [L] · OSFI B-10 [G] [S6, S11]
 Yes ☐ Partly ☐ No ☐
-
- 07** **DATA RESIDENCY · DR-04**
Where data is processed outside Canada, is there a documented cross-border risk assessment and comparable protection by contract?
PIPEDA Sch.1 cl.4.1.3 [L] · OPC cross-border guidelines [G] [S6, S21]
 Yes ☐ Partly ☐ No ☐
-
- 08** **PROMPT INJECTION · PS-01**
Is untrusted content (documents, emails, web pages, tool outputs) isolated so it can't override the model's instructions?
OPC generative-AI principles name prompt injection as a threat [G] [S8]
 Yes ☐ Partly ☐ No ☐

09 **PROMPT INJECTION · PS-02**
Are agent tool calls limited to an allow-list, with server-side validation and human confirmation for risky actions?

OSFI B-13 §3.2.1 [G] · OPC generative-AI principles [G] [S12, S8]

Yes ☐ Partly ☐ No ☐

10 **PROMPT INJECTION · PS-07**
Do you red-team for prompt injection, jailbreaks and data leakage before release and after major changes?

OSFI B-13 §3.1.2 [G] · OPC generative-AI principles [G] [S12, S8]

Yes ☐ Partly ☐ No ☐

11 **HUMAN OVERSIGHT · HL-02**
For high-impact outputs (clinical, credit, AML), is human approval mandatory and enforced, so the system can't act alone?

OSFI E-23, effective May 1, 2027 [G] · IPC-OHRC AI principles [G] [S10, S19]

Yes ☐ Partly ☐ No ☐

12 **HUMAN OVERSIGHT · HL-05**
Can a person affected by an AI-influenced decision challenge it and get a human review?

OPC generative-AI principles [G] · Bill C-36, first reading only [B] [S8, S2]

Yes ☐ Partly ☐ No ☐

13 **EVALUATION · ME-01**
Do you keep an inventory of every AI use case, including vendor and embedded models?

OSFI E-23 Principle 2.1 [G] (benchmark for non-FRFIs) [S10]

Yes ☐ Partly ☐ No ☐

14 **EVALUATION · ME-03**
Are production quality and drift monitored, with thresholds, alerts and a named owner?

OSFI E-23 Principle 3.6 [G] [S10]

Yes ☐ Partly ☐ No ☐

15 **VENDORS · VR-02**
Do contracts limit your AI vendor's use of your data to the service, with no training on it unless you agree?

O. Reg. 329/04 s.6(1) [L] · PHIPA s.17 [L] · PIPEDA cl.4.1.3 [L] [S9, S7, S6]

Yes ☐ Partly ☐ No ☐

12–15 Yes

Strong. Get independent evidence of it.

7–11 Yes

Developing. Gaps cluster in logging and vendors.

0–6 Yes

Fix this before the next AI release.

S2 Bill C-36 (45-1), LEGISinfo · parl.ca/legisinfo/en/bill/45-1/c-36

S6 PIPEDA, S.C. 2000, c. 5 · laws-lois.justice.gc.ca/eng/acts/P-8.6

S7 PHIPA, 2004 (e-Laws) · ontario.ca/laws/statute/04p03

S8 OPC et al., Principles for responsible generative AI (2023) · priv.gc.ca

S9 O. Reg. 329/04 under PHIPA · ontario.ca/laws/regulation/040329

S10 OSFI Guideline E-23 (2027) · osfi-bsif.gc.ca

S11 OSFI Guideline B-10 · osfi-bsif.gc.ca

S12 OSFI Guideline B-13 · osfi-bsif.gc.ca

S19 IPC Ontario & OHRC, AI principles (Jan 21, 2026) · ipc.on.ca

S21 OPC, cross-border processing guidelines · priv.gc.ca

Want the other 45 questions answered for you?

The AI Risk Sprint is three days on one AI system, with prompt-injection and data-leakage tests and a scored findings report. CAD \$2,500 + HST, credited toward a full Readiness Review. Email ayeshanajib5@gmail.com.

Sources accessed Oct 13, 2026. PHIPA s.10.1 is enacted but not in force. OSFI E-23 takes effect May 1, 2027 and binds federally regulated financial institutions only; for others it's a voluntary benchmark. Bill C-36 is at first reading. This checklist is general information, not legal advice.