Ontario Chiropractic Association

Vendor Evaluation Checklist for PHIPA and PIPEDA Compliance

This checklist is designed to help healthcare providers in Ontario evaluate vendors for compliance with the Personal Health Information Protection Act (PHIPA) and the Personal Information Protection and Electronic Documents Act (PIPEDA). *All items are highly recommended but only those indicated are mandatory.*

Data Handling & Storage

- ☐ The data is stored in Canada
- ☐ Personal Health Information (PHI) encrypted at rest and in transit

Compliance & Legal Safeguards

- ☐ Privacy Impact Assessment (PIA) provided
  - When was the PIA performed? _____
- ☐ Vendor is compliant with PHIPA and PIPEDA *mandatory*
- ☐ Breach notification protocol provided

Vendor Oversight & Subcontractors

- ☐ Subcontractors are PHIPA-compliant *mandatory*
- ☐ Copies of data processing agreements are provided

Security Practices

- Cybersecurity frameworks
  - ☐ ISO 27001
  - ☐ SOC 2
  - ☐ Other: _____
- ☐ Frequency of penetration testing or security audits provided
  - Penetration testing frequency _____ Last testing performed _____
  - Security audit frequency _____ Last audit performed _____

Incident Response

- ☐ Average response time to a data breach provided. _____
- ☐ Notification process provided

Data Retention & Disposal

- ☐ Data retention policy provided
- ☐ Data disposal process provided