Ontario Chiropractic Association

What To Ask Vendors Before Adoption

PHIPA, Section 17(2)

"A health information custodian shall ensure that its agents are appropriately informed of their duties under this Act."

(PHIPA, S.O. 2004, c. 3, Sched. A, s. 17 (2))

PIPEDA, Schedule 1, Principle 4.1.3

"An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party."

(PIPEDA, S.C. 2000, c. 5)

1. **Data Handling & Storage**
   - Details on **data residency** (preferably in Canada)
     - Where is the data stored? Is it in Canada?
   - Is personal health information (PHI) encrypted at rest and in transit?
   - How is access to PHI controlled and logged?

2. **Compliance & Legal Safeguards**
   - Can you provide a Privacy Impact Assessment (PIA)?
   - Are you compliant with PHIPA and PIPEDA?
   - Do you have a breach notification protocol?
     - Can you provide a copy?
     - How often is it updated?

3. **Vendor Oversight & Subcontractors**
   - Do you use any third-party subcontractors? If so, are they also PHIPA-compliant?
   - Can you provide copies of your data processing agreements?

4. **Security Practices**
   - What cybersecurity frameworks do you follow (e.g., ISO 27001, SOC 2)?
   - How often do you conduct penetration testing or security audits?

5. **Incident Response**
   - What is your average response time to a data breach?
   - How will you notify us and affected individuals?

6. **Data Retention & Disposal**
   - What is your data retention policy?
   - How is data securely deleted when no longer needed?

Ontario Chiropractic Association

What To Ask Vendors Before Adoption

Red Flags to Watch For

- Vague or evasive answers about data residency or encryption
- No documented privacy or security policies
- Use of offshore data centers without safeguards
- No breach history disclosure or incident response plan
- Refusal to sign a Business Associate Agreement (BAA) or equivalent
- Lack of transparency about subcontractors

Industry Standards to Ask About

- **ISO/IEC 27001**: International standard for information security management.
- **SOC 2 Type II**: Audit standard for service providers handling sensitive data.