Ontario Chiropractic Association

Common Privacy Policy Updates for Ontario Health Care Practitioners

Email and Communication Security

- Define acceptable use of email for transmitting PHI.
- Require encryption for all outbound emails containing PHI.
- Prohibit use of personal email accounts for patient communication.
- Include procedures for verifying patient identity before sharing information electronically.

Use of Artificial Intelligence (AI) Tools

- Prohibit uploading PHI into non-compliant AI platforms (e.g., ChatGPT, Gemini).
- Require a privacy impact assessment (PIA) before adopting AI tools.
- Define roles and responsibilities for monitoring AI outputs and ensuring human oversight.

Remote Work and Mobile Device Use

- Require use of secure, encrypted devices for remote access.
- Prohibit storage of PHI on personal or unencrypted devices.
- Include protocols for lost or stolen devices.

Third-Party Vendor Management

- Require written agreements with all vendors handling PHI.
- Mandate annual reviews of vendor privacy and security practices.
- Include breach notification obligations in vendor contracts.

Access Controls and Role-Based Permissions

- Define who has access to what types of PHI and under what circumstances.
- Require periodic reviews of user access rights.
- Include procedures for revoking access when staff leave or change roles.

Website and Online Forms

- Require CAPTCHA and encryption for all online intake or contact forms.
- Prohibit collection of unnecessary personal data through web forms.
- Include a clear privacy notice on the website explaining data use.

Breach Response and Reporting

- Define what constitutes a privacy breach under PHIPA.
- Include step-by-step breach response procedures.
- Require documentation and reporting to the IPC and affected individuals when applicable.

Training and Accountability

- Mandate annual privacy training for all staff.
- Include simulated phishing tests and breach drills.

OCA advance

- Assign a designated Privacy Officer responsible for oversight and compliance.

Retention and Secure Disposal

- Define retention periods for different types of records.
- Include procedures for secure disposal of electronic and paper records.
- Require documentation of disposal activities.

Consent and Patient Rights

- Clarify how consent is obtained, recorded, and withdrawn.
- Include procedures for responding to access and correction requests.
- Ensure patients are informed of their rights under PHIPA.