Privacy and Confidentiality Policy (PHIPA-Compliant)

Purpose

This policy outlines how personal health information (PHI) is collected, used, safeguarded, disclosed, accessed, and corrected in accordance with the **Personal Health Information Protection Act, 2004 (PHIPA)** and applicable professional standards, including those of the **College of Occupational Therapists of Ontario (COTO)**.

Scope

This policy applies to all employees, contractors, students, and agents of the clinic who have access to personal health information, in both paper and electronic formats, including in-person and virtual service delivery.

Definitions

- **Personal Health Information (PHI):** Identifying information about an individual relating to their physical or mental health, health care history, or payment for health care.
- **Health Information Custodian (HIC):** The clinic or practice responsible for custody and control of PHI under PHIPA.
- **Agent:** Any individual authorized by the HIC to collect, use, disclose, or handle PHI on its behalf.
- **PHIPA:** Personal Health Information Protection Act, 2004 (Ontario).

---

1. Collection, Use, Limitation, and Disclosure of Personal Health Information

1.1 Collection

Personal health information is collected only as necessary to:

- Provide occupational therapy assessment and treatment services
- Communicate with clients, caregivers, and other health professionals involved in care
- Maintain accurate clinical records

- Meet legal, regulatory, and professional obligations

PHI is collected directly from the client or their substitute decision-maker whenever possible and with knowledgeable consent, unless otherwise permitted or required by law.

1.2 Use

Personal health information is used solely for purposes that a reasonable person would consider appropriate, including:

- Planning, delivering, and monitoring care
- Internal quality assurance and risk management
- Billing and administrative operations related to care

Use of PHI is limited to the **minimum amount necessary** to fulfill the intended purpose.

1.3 Disclosure

PHI may be disclosed:

- With the client's or substitute decision-maker's consent
- To other health care providers for the purpose of providing or assisting with health care, where permitted by PHIPA
- When required or permitted by law (e.g., risk of serious bodily harm, court orders)

Information is not disclosed to third parties (e.g., schools, insurers, or non-circle-of-care providers) without explicit consent unless legally required.

1.4 Limitations and Retention

- PHI is retained only as long as necessary to meet legal, professional, and operational requirements.
- Records are securely destroyed in accordance with applicable legislation and professional record-keeping standards.

---

2. Safeguards for Personal Health Information

The clinic employs administrative, physical, and technical safeguards to protect PHI against theft, loss, unauthorized use, disclosure, copying, modification, or disposal.

2.1 Electronic Safeguards

- Password-protected systems and role-based access controls

- Secure, encrypted electronic medical record (EMR) systems
- Two-factor authentication where available
- Secure, PHIPA-compliant virtual care platforms
- Regular software updates and security monitoring

2.2 Paper Record Safeguards

- Locked filing cabinets in secure areas
- Restricted access to authorized personnel only
- Secure transport of paper records when required
- Shredding or secure destruction of records when no longer required

2.3 Administrative Safeguards

- Privacy training for all staff and agents
- Confidentiality agreements as part of onboarding
- Clear procedures for access, use, and disclosure of PHI

---

3. Privacy Breach Management and Reporting

3.1 Definition of a Privacy Breach

A privacy breach occurs when PHI is stolen, lost, accessed, used, or disclosed without authorization, or in a manner inconsistent with PHIPA.

3.2 Immediate Response

In the event of a suspected or confirmed breach, the clinic will:

- Take immediate steps to contain the breach
- Assess the scope and impact of the breach
- Prevent further unauthorized access or disclosure

3.3 Notification and Reporting

In accordance with PHIPA, the clinic will:

- Notify the affected individual(s) at the first reasonable opportunity
- Provide information about the nature of the breach and steps taken to mitigate harm
- Report the breach to the **Information and Privacy Commissioner of Ontario (IPC)** when required
- Notify relevant regulatory bodies, including COTO, if applicable

3.4 Documentation

All privacy breaches and near-misses will be documented, investigated, and reviewed to prevent recurrence.

---

4. Access to and Correction of Personal Health Information

4.1 Right of Access

Clients or their substitute decision-makers have the right to access their personal health information, subject to limited exceptions under PHIPA.

Requests for access must:

- Be made in writing
- Be responded to within the timeframes required by PHIPA

A reasonable fee may be charged in accordance with PHIPA, and clients will be informed of any fees in advance.

4.2 Requests for Correction

Clients have the right to request correction of PHI if they believe the information is inaccurate or incomplete.

- Requests must be made in writing
- Corrections will be made where appropriate, or a statement of disagreement will be added to the record
- Responses will be provided within legislated timelines

---

5. Responsibilities

- **Health Information Custodian:** Ensures compliance with PHIPA and this policy
- **Agents and Staff:** Protect PHI and report suspected breaches immediately
- **Clinicians:** Ensure appropriate consent and confidentiality in all interactions

---

6. Policy Review

This policy is reviewed regularly and updated as required to reflect legislative, regulatory, or organizational changes.