POLICY #	POLICY	SECTION	SUB-SECTION	APPROVAL DATE	REVIEW DATE	REVIEW FREQUENCY
IM-PC-PL-001	Privacy, Confidentiality and PHIPA Compliance Policy	Information Management & Privacy	Privacy & Confidentiality	October 2021	January 2025	Annual

1. Purpose

To protect the privacy and confidentiality of all client information in accordance with the **Personal Health Information Protection Act (PHIPA), 2004**, and to define CareHop's responsibilities for the collection, use, disclosure, storage, and safeguarding of personal health information (PHI).

2. Scope

This policy applies to all employees, contractors, students, and volunteers who have access to personal or health information at CareHop Nursing & Home Care Services.

3. Policy Statement

CareHop is committed to maintaining the privacy and confidentiality of all personal health information in its custody. Staff must handle all PHI in a manner that respects client rights and complies with applicable legislation and professional standards.

4. Definitions

- **Personal Health Information (PHI):** Identifying information about an individual in oral, written, or electronic form related to their physical or mental health, health services, or health number.
- **Confidentiality:** The obligation to protect personal information from unauthorized access or disclosure.
- **Privacy Breach:** Unauthorized collection, use, disclosure, or loss of PHI.

5. Collection, Use and Disclosure of PHI

- PHI is only collected as needed to provide or support client care. CareHop uses AlayaCare, a secure cloud-based health care platform, to collect, store, and manage client personal health information (PHI) in accordance with PHIPA. Microsoft 365 is used primarily as a supplemental administrative and communication tool and is not used to manage client care plans or core PHI storage.
- Use of PHI is restricted to the minimum necessary for the intended purpose. CareHop maintains contractual and data sharing agreements with all third-party Technology Service Providers (e.g., AlayaCare, Microsoft 365, BlueBird IT Solutions) that include provisions for PHI protection and mandatory reporting of security incidents within 24 hours.

- Disclosure to third parties (e.g., caregivers, specialists) must be authorized by the client or their Substitute Decision-Maker (SDM), unless permitted or required by law.

6. Client Rights Under PHIPA

- Right to access and request correction of their health records
- Right to be informed about how their PHI is used
- Right to provide or withhold consent for disclosure
- Right to file a complaint with the **Information and Privacy Commissioner of Ontario (IPC)**

7. Staff Responsibilities

- Maintain strict confidentiality of client information
- Use only authorized systems and secure methods to share PHI
- Avoid discussing client information in public or unsecured settings
- Report any suspected or confirmed privacy breaches immediately to the CEO or designated Privacy Lead

8. Security and Safeguards

- Electronic records must be stored on encrypted and password-protected systems
- Paper records must be kept in locked cabinets or restricted-access rooms. AlayaCare is CareHop's primary electronic health record (EHR) and care management platform. Access to AlayaCare is permission-based, and only authorized personnel with valid credentials may access client PHI. All AlayaCare data is encrypted and stored in compliance with Canadian data residency and health privacy requirements. Microsoft 365 is used to handle only limited administrative materials, and access to such documents is restricted and secured according to organizational protocols.
- PHI must not be stored on personal devices
- Access to client information is granted based on role and need-to-know. Electronic systems that store or transmit PHI include audit logging, which is retained and monitored for a minimum of 3 months. Logs are protected from unauthorized modification or deletion.

9. Breach Reporting and Response

- All privacy breaches must be reported immediately to the CEO or Privacy Lead
- An investigation will be conducted within 2 business days
- Affected clients will be notified, and if required, a report will be filed with the IPC
- All breaches are logged and reviewed during privacy audits. CareHop maintains incident response playbooks, conducts periodic incident response exercises, and ensures staff are trained to recognize and report cybersecurity threats. Impacted third parties, including Ontario Health at Home, are notified within 24 hours where applicable.

10. Training and Acknowledgment

- All staff must complete annual PHIPA training
- Staff must sign confidentiality agreements upon hire and as part of policy renewals

11. Oversight and Review

- The CEO oversees policy implementation and compliance
- Privacy practices are reviewed annually and as required by regulation or breach investigation findings. The use and configuration of AlayaCare are also reviewed as part of the annual privacy and security audit.

12. Related Policies

- Information Security and Data Breach Incident Reporting Policy
- Whistle Blower Protection Policy
- Client Rights and Responsibilities Policy
- Consent to Treatment and Services Policy

13. References

- Personal Health Information Protection Act, 2004 (PHIPA)
- Information and Privacy Commissioner of Ontario Guidelines
- Ontario Regulation 187/22 – Patient Bill of Rights
- Accreditation Canada: Privacy and Information Management Standards

Policy Approval

Approved by: 

Chief Executive Officer