POLICY/PROCEDURE NAME: Privacy and Confidentiality at Hospice Peterborough	**NUMBER:** 1b-0001 (formerly policy 3-210)
MANUAL (SECTION): 1. Governance, Organization & Finance (b. Organization)	**POLICY OWNER:** Chair, Governance Committee
OTHER RELEVANT P&P'S: 1b-0006 Privacy and Security Governance & Accountability 1b-0003 Concerns, Complaints and Compliments 1b-0009 Integrated Quality and Safety Framework 3-320 Risk Management 1b-0007 Privacy Audit 2a-0001 Consent to the Collection, Use and Disclosure of Personal Health Information 2a-0002 Access, Corrections and Disclosure of Personal Health Information 3a-0001 Storage, Retention, Transfer and Disposal of Client and Organizational Records 3a-0003 Information Security	**HOW OFTEN REVIEWED:** Every two years unless there is legislated or significant practice changes.
DATE OF ORIGINAL: November 2003	**APPROVED BY:** Board of Directors
DATES REVISED: July 2010; February 28, 2019, June 2021	**LAST REVIEWED:** June 2021
Any physical copies of this document are considered reference only and may not be current if not checked against the electronic copy. Obsolete documents must not be used.	

POLICY

Statement

Hospice Peterborough (HP) is committed to maintaining the privacy and confidentiality of personal, organizational and health information regardless of the medium (verbal/written/electronic) in accordance with our mission, Ontario's Personal Health Information Protection Act (PHIPA Bill 31), public expectations for privacy and internationally accepted information principles.

Section 12(1) of PHIPA requires health information custodians to take steps that are reasonable in the circumstances to ensure personal health information in their custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that records containing personal health information are protected against unauthorized copying, modification or disposal.

Objectives

HP is committed to protecting the privacy of the personal, organizational and health information of our clients, employees, volunteers, donors and other stakeholders through policy and practice. This is inclusive of the collection, use and disclosure of personal health information and the storage, retention, transfer and disposal of client and organizational records.

During the course of our various programs and services, we frequently gather and use personal and health information. This information will be carefully protected. Utilization or sharing of this information will be limited to relevant health care providers and individuals the client identifies through express or implied consent.

HP is also committed to the protection of printed or written confidential information belonging to the organization, such as financial and statistical data, cost information and staff salaries.

Privacy practices
HP takes measures to ensure the integrity of personal and health information is maintained. HP retains personal and health information for the time period required to fulfil the purposes for which the information was collected, or as authorized or required by PHIPA and as defined in the Storage, Retention, Transfer and Disposal of Client and Organizational Records policy.

Privacy policies are reviewed every two years unless there is legislated or significant practice changes.

Privacy training is provided to all staff, volunteers and students in accordance with legislative and professional practice standards. All staff, volunteers and students sign an agreement annually that they will uphold HP's privacy and confidentiality policies and for the containment, resolution and investigation of privacy and security incidents within the organization.

With regard to its privacy and confidentiality practices, HP will respond in a timely manner to potential breaches, and inquiries and complaints (as defined in the Complaints and Unusual Incidents policy).

DEFINITIONS

Clients: Inclusive of individuals participating in any HP programs and services.

Express Consent: Consent that is given either verbally or in writing, to a custodian to collect, use or disclose an individual's personal health information.[1]

Implied Consent: Consent that one concludes has been given based on what an individual does or does not do in the circumstances.[2]

Personal Information: Information about an identifiable individual that is recorded in any form including, but not limited to: Information relating to the race, national or ethnic origin, colour, religion, age or marital status of the individual; information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved; the address, fingerprints or blood type of the individual; any identifying number, symbol or other particular assigned to the individual; the views or opinions of another individual about the individual.[3]

[1] Accessed November 7, 2018: https://www.ipc.on.ca/health/consent-and-your-personal-health-information/
[2] Ibid.
[3] Taken from Section 3 of Canada's *Privacy Act.*

Personal health information: Identifying information about an individual in oral or recorded form, if the information relates to:

a) The physical or mental health of the individual, including information that consists of the health history of the individual's family;

b) The providing of health care to the individual, including the identification of a person as a provider of health care to the individual;

c) An individual's plan of care and service within the meaning of the Home Care and Community Services Act, 1994 for the individual;

d) Payments or eligibility for health care, or eligibility for coverage for health care, in respect of the individual;

e) The donation of any body part or bodily substance of the individual, or is derived from the testing or examination of such body part or bodily substance;

f) An individual's health number;

g) An individual's substitute decision-maker.[4]

Organizational information includes, but is not limited to:

- Financial information that is not contained in a public budget or in a public report;
- Non-public information about HP's operation, its staff, its plans; aspects of the relationship between HP and other agencies, etc.;
- Reports or information received or discussed in a closed meeting.

Privacy Breach/Breach of Confidentiality: a privacy breach occurs when personal information is collected, retained, used, disclosed, or disposed of in ways that do not comply with Ontario's privacy laws.

PROCEDURE

All HP staff, volunteers and students will participate in privacy and confidentiality training and indicate comprehension and agreement by signing the Commitment and Agreement to Privacy and Confidentiality Form upon commencement of work and on an annual basis.

With regard to its privacy and confidentiality practices, all staff, volunteers and students will respond an appropriate manner to potential breaches, inquiries and complaints (as defined in the Concerns, Complaints and Compliments policy).

All staff, volunteers and students who facilitate groups at HP will remind participants to respect the privacy and confidentiality of fellow participants. In addition, group facilitators will:

- Establish guidelines for each group which includes 'privacy & confidentiality' amongst group members;
- Stress that "What is said at Hospice, stays at Hospice";

[4] Definitions a) through g) quoted from Section 4 (1) of the *Personal Health Information Protection Act (*PHIPA)

- Inform participants how to proceed should they have concerns about privacy and confidentiality;
- Ensure that group participants indicate comprehension and agreement by signing the Confidentiality Agreement for Group Participants Form.

BREACH OF PRIVACY/CONFIDENTIALITY PROCEDURE:

1. **Contain the breach and notify affected individuals**
    - Alert all relevant staff of the breach, including HP's privacy officer, and determine who else within the organization should be involved in addressing the breach.
    - Identify the nature and scope of the breach and the action needed to take to contain it
    - Determine what personal information is involved
    - Take corrective action:
        - ensure that no personal information has been retained by an unauthorized recipient.
        - obtain their contact information in case follow-up is required
        - ensure that the breach does not allow unauthorized access to any other personal information by taking appropriate action (for example, changing passwords or identification numbers, or temporarily shutting down a system)
        - in a case of unauthorized access by staff, consider suspending their access rights
        - retrieve hard copies of any personal information that has been disclosed
2. **Notify those affected by the breach**
    - Notify those affected as soon as reasonably possible if HP determines that the breach poses a real risk of significant harm to the individual, taking into consideration the sensitivity of the information and whether it is likely to be misused.
    - If law enforcement is involved, ensure that notification will not interfere with any investigations.
    - Notification should be direct, such as by telephone, letter, email or in person. Indirect notification can be used in situations where direct notification is not possible or reasonably practical, for instance, when contact information is unknown or the breach affects a large number of people.
    - Notification to affected individuals should include details of the extent of the breach and the specifics of the breach.

3. **Investigate**
    - Identify and analyse the events that led to the breach
    - Review HP policies and practices in protecting personal information, privacy breach response plans and staff training to determine whether changes are needed
    - Determine whether the breach was a result of a systemic issue and if so, review HP program-wide or institution-wide procedures
    - Take corrective action to prevent similar breaches in the future and ensure HP staff are adequately trained
    - If the Information and Privacy Commissionaire is contacted, advise them of the findings and remedial measures, and cooperate with any further investigation IPC may undertake into the incident

4. **Notify the Information and Privacy Commissionaire (IPC)**
    - The IPC will be notified of significant breaches, such as those that may involve sensitive personal information or large numbers of individuals, or when you are having difficulties containing the breach. In these situations, you should notify the IPC as soon as reasonably possible.
    - In situations where HP will be notifying a large number of individuals, it is important to contact the IPC before beginning the notification process. The IPC can assist HP with your breach response plan.

5. **Reduce the risk of future breaches**
    - Educate HP staff about Ontario's privacy laws and the organization's policies and practices governing the collection, retention, use, security, disclosure and disposal of personal information
    - Conduct privacy impact assessments before introducing or changing technologies, information systems, and processes to ensure privacy risks are identified and addressed
    - Seek input from appropriate parties such as HP legal counsel and security units, freedom of information and privacy coordinator, the Ontario ministry responsible for information and privacy matters, and IPC as necessary.

FORMS, TOOLS & PROTOCOLS

- Privacy and Confidentiality Policies Map (Guide)
- Commitment and Agreement to Privacy and Confidentiality Form
- Confidentiality Agreement for Group Participants Form
- Privacy & Confidentiality @ Hospice Peterborough Primer (Guide)

POLICY COMMUNICATION PLAN

This policy is included in orientation for all, staff, volunteers, and students in annual refresher training and signing of the Commitment and Agreement to Privacy and Confidentiality Form.

This policy and contact information for the Privacy Officer is posted on the HP website and available in other accessible formats as needed.

REFERENCES (e.g. research, legislation, organizations)

Information and Privacy Commissioner of Ontario

Information and Privacy Commissioner of Ontario - Privacy Breaches Guidelines for Public sector organizations.

Personal Health Information Protection Act, 2004

Privacy Act, 2013

Summary of Privacy Laws in Canada

POLICY REVIEW DETAILS

To ensure compliance and to identify any needed revisions, the Policy Manual Owner or designate will review this policy every two years unless there is legislated or significant practice changes.