**AREA OF HOSPICE OPERATIONS: PRIVACY AND CONFIDENTIALITY**

| | | | |
|---|---|---|---|
| POLICY<br><br>**PR-1** | **PRIVACY, PERSONAL HEALTH INFORMATION (PHI) POLICY** | APPROVED BY | **Board Chair**<br>**Executive Director**<br>**QS&R Committee**<br>**Board of Directors** |
| PROCEDURE | | | |
| DATE ISSUED | February 2018 | REVISED | |

**PURPOSE**

It is the policy of Hospice Georgian Triangle (HGT) to be compliant with the privacy principles established by the Canadian Standards Association and to provide clear direction to Board Members, employees, physicians and volunteers in terms of privacy and confidentiality of personal health information (PHI) and personal information (PI). All information collected, used and disclosed, by the organization, its staff and affiliates shall be treated in a manner that accords with the Personal Health Information Protection Act (PHIPA), Freedom of Information and Protection of Privacy Act (FIPPA), organizational and professional obligations.

**POLICY STATEMENT**

HGT values the privacy and confidentiality of the information within its custody and control. As a health information custodian (HIC), HGT and its agents (including staff, physicians and students) are committed to protecting the PHI and/or PI of all staff and patients/clients served.

HGT's approach to privacy and access encompasses the following 10 privacy principles, adopted from the Canadian Standard Association:

**Principle 1 - Accountability:** HGT is responsible for both PHI and PI under its custody and control and has designated an individual(s) who is accountable for ensuring compliance with PHIPA and FIPPA. The designated Privacy Officer and privacy contact person for HGT is the Executive Director (ED).

While corporate accountability for the organization's compliance with the principles of PHIPA rests with the Executive Director, other individuals within HGT are responsible for the day-to-day collection, use and disclosure of PHI through delegation. HGT has implemented information practices in keeping with PHIPA and FIPPA.

The Privacy Officer and/or delegate responds to any access requests, privacy related enquiries, information transferred to a third party for processing and complaints, and Commissioner's investigations.

For the purposes of FIPPA, the Chair of the Board as the head of the institution designates a contact person under the Delegation of Authority.

**Principle 2 - Identifying Purpose(s):** HGT will make reasonable efforts to identify, in a meaningful way, the purpose for which PHI and PI is collected at or before the time of collection, to the individual and/or substitute decision maker (SDM).

The organization collects PHI and PI for the following purposes:

- for the delivery of patient/client care
- for employment
- to plan, administer and manage internal operations
- to teach and/or conduct research
- to compile statistics
- to comply with legal and regulatory requirements
- to obtain payment for patient treatment and care (from OHIP, WSIB, private insurer or others)
- to conduct risk management activities
- to conduct quality improvement activities such as patient/client satisfaction surveys
- to support fundraising for the Hospice Georgian Triangle Foundation.

HGT participates in provincial health information networks, palliative care networks and information portals designed to enhance the care provided to patients/clients.

When personal information/personal health information collected is to be used for a new purpose not previously identified, the new purpose will be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose. Persons collecting PHI must be able to explain to individuals the purposes for which the information is being collected.

**Principle 3 - Consent for Collection, Use and Disclosure:** HGT will rely on implied consent, where appropriate, or obtain express consent from the individual or SDM when collecting, using or disclosing PHI and PI unless otherwise exempted by a specific policy, data sharing agreement or legislation. Consent may be obtained verbally or in writing. To make the consent meaningful, the purpose(s) must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

To be valid, a consent must:

- be the consent of the individual or substitute decision-maker who is deemed capable
- be knowledgeable – the individual must understand
- detail the purpose for the collection, use or disclosure of the information
- relate to the information
- not be obtained through deception or coercion.

The individual understands they may provide or withhold consent.

PHI can be collected, used, or disclosed without the knowledge and consent of the individual in some circumstances, as set out under PHIPA, the Mental Health Act or any other applicable Act.

An individual may withdraw consent for the collection, use or discloser of PHI at any time, subject to legal restrictions and reasonable notice, called a Consent Directive. A Consent Directive will not have a retroactive effect. HGT will inform the individual of the implications of such withdrawal. Consent Directives will be received in writing from the individual stating that they understand the implications of withdrawal. Requests from individuals withdrawing consent must be directed to the Privacy Officer.

**Principle 4 - Limiting Collection:** HGT will not collect PHI indiscriminately and will limit the collection of personal information/personal health information to that which is necessary, for the identified purpose or for purposes that PHIPA or FIPPA permits or requires. Both the amount and the type of information will be limited to that which is necessary to fulfill the purposes identified.

HGT may collect PHI about an individual indirectly if the information is reasonably necessary to provide health care.

HGT shall take steps that are reasonable in the circumstances to ensure that PHI is not collected without authority.

**Principle 5 - Limiting Use, Disclosure, and Retention:** PHI and PI in all forms; verbal, written, electronic, printed will not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law.

Use of PHI and PI is limited to those individuals who are authorized to use or handle such information in order to perform their current role, on a need to know basis. Individuals must avoid using PHI or PI in any area where it may come to the attention of another individual who is not entitled to receive such information.

Information is retained in a secure manner and for as long as necessary to fulfill the purpose for which it was collected or as required by law. Information will be kept in accordance with HGT's retention and destruction policy/schedule and applicable legislation. Information that is no longer required will be destroyed, erased, or made anonymous in a secure manner, and in compliance with legislative requirements.

Access controls are used to prevent unauthorized or inappropriate access to PHI or PI, to ensure the protection of the organizations services, prevent unauthorized computer access, detect unauthorized or inappropriate activities and ensure information security.

The organization tracks accesses to all or part of the PHI or PI (electronic and paper) and ensures the record identifies the person who accessed the information, and the date and time of the access.

An agent of HGT who is granted access to PHI or PI as an authorized agent will have an appropriate level of authority, privacy and security training to warrant access.

**Principle 6 - Accuracy:** HGT will take reasonable steps to ensure that PHI and PI is accurate, complete, and up-to-date as is necessary to minimize the possibility that inappropriate information may be used to make a decision about an individual for the purposes for which it is used or disclosed.

**Principle 7 - Safeguards:** Appropriate technical, administrative and physical safeguards are implemented to protect PHI and PI against loss or theft, as well as unauthorized access, disclosure, copying, inappropriate use, or modification. Examples include:

- Technical - access controls including audits, use of passwords and encryption, secure computer networks.
- Administrative - limiting access on a "need to know" basis, confidentiality agreements, etc.
- Physical - locked cabinets, restricted access to offices, privacy screens on monitors.

HGT will make all individuals aware of the importance of maintaining the confidentiality of PHI and PI. As a condition of employment or affiliation, all individuals must sign a Confidentiality Agreement which will be reviewed and signed annually thereafter. This safeguard may also be facilitated through contractual provisions.

Privacy education will be provided to new employees as part of orientation to HGT. Refresher education encompassing current relevant information will be provided on an ongoing basis as required, annually at a minimum. In the event that the individual commences work prior to receiving privacy training, the Privacy Policies and Confidentiality Agreement, at minimum, will be reviewed and signed.

Program Coordinators (or designate) will ensure that any program/department specific information or procedures relating to privacy will be covered with new employees. Care and measures are used in the disposal or destruction of PHI and PI, in order to prevent unauthorized parties from gaining access to information (e.g. confidential shredding bins).

Regular, random and targeted audits are conducted on systems user activity logs in order to monitor for inappropriate activity associated with PHI or PI.

**Notifications/Reporting**

In the event that PHI is stolen or lost, used or disclosed without authority, HGT, through the Privacy Officer (ED) **must notify the individual** about the PHI that was stolen, lost, used or disclosed without authority. In addition, the individual will be made aware of their right to make a complaint to the Information and Privacy Commissioner of Ontario.

An agent within the organization must notify HGT at the first reasonable opportunity if PHI that they collected, used, disclosed, retained or disposed of on behalf of the organization is stolen or lost or if it is used or disclosed without authority.

**HGT shall notify** the appropriate professional college, within 30 days, of an agent of HGT who has been terminated, suspended or subject to disciplinary action, or has resigned as a result of, or due to, unauthorized collection, use, disclosure, retention or disposal of PHI.

**HGT shall notify** the appropriate professional college within 30 days of an agent who has had privileges at HGT revoked, suspended, restricted or that the agent has relinquished or voluntarily restricted privileges as a result of unauthorized collection, use, disclosure, retention or disposal of PHI.

HGT must report breaches to the Commissioner in seven categories described in the regulation:

**1.** Use or disclosure without authority;

**2.** Stolen information;

**3.** Further use or disclosure without authority after a breach;

**4.** Pattern of similar breaches;

**5.** Disciplinary action against a college member [related to a breach];

**6.** Disciplinary action against a non-college member [related to a breach];

**7.** Significant breach.

The categories are not mutually exclusive; more than one can apply to a single privacy breach. If at least one of the situations applies, HGT must report it.

There are significant fines which may be levied against both the organization and the person who committed the breach *(see Appendix 1).*

HGT will be required to start tracking privacy breach statistics as of January 1, 2018 and will be required to provide the Commissioner with an **Annual Report** of the previous calendar year's statistics, starting in March 2019.

**Principle 8 - Openness:** HGT makes readily available to the public, in a variety of ways, information about its policies and practices relating to the management of PHI and PI. The organization's public statements (information practices) will be in place for public viewing such as the organization's website and will include:

- A general description of the information practices;
- The name or title, and the address, of the person who is accountable for the Privacy policies and practices and to whom complaints or inquiries can be directed;
- The means of gaining access to PHI or PI held by HGT.

**Principle 9 - Individual Access to PHI or PI:** Upon request, and after providing sufficient identification, an individual will be informed of the existence, use, and disclosure of his or her PHI or PI and will be given access to that information in a manner consistent with PHIPA or FIPPA.

The individual will be able to challenge the accuracy and completeness of the information and may have it amended as appropriate. When a challenge is not resolved to the satisfaction of the individual, HGT will record the substance of the unresolved challenge. When appropriate, the existence of the unresolved challenge will be transmitted to third parties having access to the information in question.

**Principle 10 - Challenging Compliance:** An individual will be able to address concerns regarding compliance with this policy to the Privacy Officer (PO) or designated individual(s) accountable for HGT's compliance. An individual may contact the Privacy Officer (ED) at:

borgk@hospicegeorgiantriangle.com

**705-444-2555 x 7520**

Procedures are in place to receive, investigate and respond to complaints or inquiries about HGT's policies and practices relating to the handling of PHI and PI.

If a complaint is found to be justified, HGT will take appropriate measures, including, if necessary, amending its policies and practices.

Individuals may also make a complaint to the **Information and Privacy Commissioner** of Ontario at 2 Bloor St., E., Suite 1400, Toronto, Ontario M4W 1A8 or www.ipc.on.ca, or commissioner@ipc.on.ca

**Compliance:** HGT is required to provide the Information and Privacy Commissioner with annual reports regarding activities under PHIPA and FIPPA.

Nothing in this policy detracts from HGT's rights and responsibilities in respect to PHI in its possession, power and/or control as set out in any law applicable in the Province of Ontario including the Health Protection and Promotion Act, Mental Health Act and Regulated Health Professions Act and related regulations.

There may be instances where application of PHIPA or FIPPA conflicts with other legislations. In these instances, HGT may seek advice from legal counsel to determine which legislative requirement is applicable and/or appropriate.

**Definitions**

Personal Health Information Protection Act, 2004 (PHIPA) - PHIPA outlines privacy provisions for health information custodians in the province of Ontario. The purposes of the PHIPA are as follows:

- To establish regulations for the collection, use and disclosure of personal health information in a manner that protects the confidentiality of the information and the privacy of the individuals in question.
- To provide individuals with the right to access personal health information about themselves and to correct or amend such information, subject to certain exceptions.
- To provide independent review and resolution of personal health information complaints.

Freedom of Information and Protection of Privacy Act (FIPPA) - FIPPA provides the right of access to information under the control of the organization, supports the key concepts of transparency, accountability and the exercise of democracy and protects the privacy of the individuals to whom that information relates. All records created or which came into HGT's custody or control after January 1, 2007 are subject to the Act.

Personal Health Information (PHI): Recorded identifying information about an individual in oral or recorded form if the information relates the physical or mental health of the individual or related to the provision of health care to the individual. PHI includes, but is not limited to, a patient/client's name and location in the organization, and a recorded image of the individual.

Personal Information (PI): Recorded identifying information about an individual, where the information relates to an individual's race, colour, national or ethnic origin, sex, age any identifying number and/or symbol assigned to an individual. If a video surveillance system displays these characteristics of an identifiable individual or the activities in which he or she is engaged, its contents will be considered personal information.

Privacy Officer: An individual designated as the contact person to assist in meeting the organization's privacy obligations. This individual is primarily responsible for privacy compliance within the organization. The responsibilities include establishing and maintaining appropriate information practices, developing privacy policies and procedures and tools, developing access, correction, inquiry and complaint procedures, conducting privacy impact assessments and privacy audits of information use. This individual will also deal with any access requests, privacy related inquiries, complaints and Information and Privacy Commissioner investigations.

Health Information Custodian (HIC): A person or organization that has custody or control of PHI, as a result of, or in connection with, performing the person's or organization's powers or duties or work as set out under PHIPA. Examples of HICs include health professionals, long term care homes, community care access centres, and pharmacies.

Agent: A person that, with the authorization of the organization, acts for or on behalf of the organization in respect of PHI for the purposes of the organization and not the agent's own purposes, whether or not the agent has the authority to bind the custodian, whether or not the agent is employed at the organization and whether or not the agent is being remunerated.

Examples of agents include, but not limited to: employees, students, credentialed staff residents, clinicians, consultants, researchers, vendors or contractor.

Data Sharing Agreement: is a formal contract that clearly outlines the obligations of the Parties when data is being shared.

**This harmonized policy was developed in collaboration with the following organization: Collingwood General and Marine Hospital**

**References**


- Freedom of Information and Protection of Privacy Act R.S.O 1990, CHAPTER F.31, Last amendment: 2011, c.9, Schedule 15
- Personal Health Information Protection Act, 2004, CHAPTER 3 Schedule A, Last amendment: 2016, c. 30, S. 43
- Mental Health Act
- Public Hospitals Act
- Criminal Code of Canada
- Waypoint Centre for Mental Health Care Access and Privacy Policy, February 2015
- Orillia Soldiers Memorial Hospital Privacy and Access Policy, March 2012
- Muskoka Algonquin Healthcare Privacy Policy, December 2012
- Georgian Bay General Hospital, Access and Privacy Policy, December 2011
- Grey Bruce Regional Health Centre
- North Simcoe Muskoka Community Care Access Centre, Client Privacy and Confidentiality, December 2014

# APPENDIX 1:

## RECENT CHANGES TO PHIPA AFFECTING HEALTH INFORMATION CUSTODIANS

Jul 15, 2016 POSTED BY ROSEN SUNSHINE (LLB-TORONTO)

On May 18, 2016, the Ontario government passed Bill 119, the *Health Information Protection Act, 2016*, which we summarized on our blog last fall, shortly after it was introduced in the Ontario Legislature. Bill 119 makes significant amendments to the *Personal Health Information Protection Act, 2004* ("PHIPA") and related pieces of legislation relevant to the health care sector. In this post, we highlight the key provisions of Bill 119 that are now in force and which have significant impacts for health care professionals, institutions and organizations ("health information custodians" or "HICs") across the province that collect, use and maintain personal health information ("PHI").

**Amendments to PHIPA**

The key amendments to PHIPA introduced through Bill 119 that are now in force include:

- **Revised Definition of "Use":** The term "use" now means "to view, handle or otherwise deal with the information". The inclusion of the word "view" in the revised definition appears to be aimed at preventing unauthorized "snooping" into individuals' health records.
- **Increased Fines:** The maximum fines for privacy offences have doubled from $50,000 to $100,000 for individuals and from $250,000 to $500,000 for organizations. In addition, the 6 month limitation on commencing prosecutions for offences under section 72 of PHIPA has been eliminated.
- **Mandatory Reporting to the IPC:** Previously, privacy breaches only had to be reported to affected individuals. HICs are now required to report privacy breaches to the Information and Privacy Commissioner of Ontario ("IPC"), where the circumstances surrounding the theft, loss or unauthorized use or disclosure of PHI meet certain prescribed criteria. At this time, however, the government has not yet passed any regulations with respect to this amendment and therefore, the mandatory duty is not effectively in force.

- **Mandatory Reporting to Regulatory Colleges:** HICs are now required to make a report to the health regulatory colleges (or the College of Social Workers and Social Services Workers) in certain circumstances regarding privacy breaches. Specifically, HICs that employ, grant privileges to, or are otherwise affiliated with a member of one of these colleges, are required to notify the relevant regulatory within 30 days of any of the following events:
    - An employee is terminated, suspended or subject to disciplinary action as a result of a privacy breach;
    - An employee resigns, and the HIC has reasonable grounds to believe that the resignation is related to an investigation (or other action) into an alleged privacy breach;
    - An agent's privileges or affiliation with the HIC are revoked, suspended or restricted as a result of a privacy breach; or
    - An agent relinquishes or voluntarily restricts his or her privileges or affiliation with the HIC, and the HIC has reasonable grounds to believe that it is related to an investigation (or other action) into an alleged privacy breach.
- **Notice Requirements:** Prior to these amendments, HICs were required to notify affected individuals of a privacy breach at the first reasonable opportunity. This notice must now include a statement that the individual is entitled to make a complaint to the IPC.
- **Responsibilities of HICs and Agents:** HICs are granted increased authority to set conditions or restrictions over the collection, use, disclosure, retention or disposal of PHI by its agent. An agent's authority to deal with PHI is amended, such that agents are permitted to collect, use, disclose, retain or dispose of PHI only if:
    - the HIC permits it;
    - it is necessary for carrying out the agent's duties;
    - it is not contrary to PHIPA or another law;
    - any restrictions or conditions imposed by the HIC are met; and
    - any additional obligations set out in regulations are met (of which there are currently none).

Bill 119 also introduces a new Part V.1 to PHIPA to create a privacy framework for Electronic Health Records ("EHR"). EHR is the provincial electronic system that is developed and maintained by eHealth Ontario, to enable HICs to collect, use and disclose PHI for the purpose of providing or assisting in the provision of health care to the individuals whose PHI is in the EHR. eHealth Ontario will also manage and oversee the EHR, including by monitoring and logging access. The provisions of Bill 119 relating to the governance, development and maintenance of the HER are not yet in force, but once they are proclaimed will have significant implications for patients and HICs.

**New Quality of Care Information Protection Act**

Another main function of Bill 119 is to replace the existing *Quality of Care Information Protection Act, 2004* ("QCIPA") with an entirely new act of the same name. In our blog post last fall, we summarized some of the key elements of the new QCIPA. At this time, however, the provisions of Bill 119 that repeal and replace QCIPA have not been proclaimed into force. We will review the changes implemented by the new QCIPA in greater detail and discuss the implications for health facilities once the new QCIPA becomes law.

**RELATED**

- Bill 119 Health Information and Protection Act, 2016
- Personal Health Information Protection Act (PHIPA), 2004
- Freedom of Information and Protection of Privacy Act (FIPPA),

**POLICIES**

- PHI - Access, Security, Storage, Retention, Destruction
- Breach Prevention Strategies
- HGT Privacy Officer
- HGT Privacy Officer Guidelines
- Confidentiality - Staff and Volunteers
- Breach of Confidentiality - Staff and Volunteers
- Privacy Complaint and Breach Management
- Privacy Breach Protocol
- Personnel Files and Employee Information
- Privacy – Staff and Volunteers

**FORMS**

- Breach of Ethics or Code of Conduct Letter (Staff, Volunteer)
- Breach of Confidentiality Disciplinary letter (Staff)
- Breach of Confidentiality Notification Letter (Client)
- Confidentiality Agreement, Staff
- Confidentiality Agreement, Volunteers
- Release of Information sign-off