Hospice Dufferin

Privacy Policies

Applies to:	#	Policy	last reviewed	Date approved	Revision Date	Revision Date	Revision date
V,S,E	Pr-1	Breach of Personal Information	Feb 2019	Mar 2019			
V,S,E	Pr-2	Collection and Storage of Information	Feb 2019	Jan 2004			
V,S,E	Pr-3	Privacy Officer and Information Security Management	Feb 2019	Jan 2004	Jan 2019		
V,S,E	Pr-4	Privacy Safeguards	Feb 2019	Jan 2004	Jan 2019		
V,S,E	Pr-5	Security Incidents Involving Electronic Health Records					
V,S,E	Pr-6	Third Party Arrangements	Feb 2019	Feb 2019	Feb 2019		
V,S,E							
V,S,E							
V,S,E							

V - Volunteer,
S- Student Placement
E - Employee

Hospice Dufferin
Privacy Policies

Hospice Dufferin POLICY		
Title	Breach of Personal Information	Document # Pr-1
Section	Privacy	Revision #
Application	Employees, Volunteers, Students, third Party	Issue date Feb 2019
Issued By	Executive Director	Replaces Last Review: Feb 2020 Next Review: Feb 2021
Approved By	Board of Directors	**Number of pages 9**

Purpose

Protecting the privacy and confidentiality of personal information is an important aspect of the way Hospice Dufferin conducts its business. A breach of security will be taken with seriousness.

Definitions

Security safeguards

Security safeguards include the following:

- Physical measures, for example, locking filing cabinets and restricted access to offices;
- Organizational measures, for example, security clearances and limiting access on a "need-to-know" basis; and
- Technological measures, for example, the use of passwords and encryption.

Breach: the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards that are referred to in clause 4.7 of Schedule 1 of PIPEDA, or from a failure to establish those safeguards.

Personal Information (PI) Has the meaning set out in section 2 of the Freedom of Information and Protection of Privacy Act (FIPPA) as: recorded information about an identifiable individual, including, (a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual, (b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved, (c) any identifying number, symbol or other particular assigned to the individual, (d) the address, telephone number, fingerprints or blood type of the individual, (e) the personal opinions or views of the individual except where they relate to another individual, (f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence, (g) the views or opinions of another individual about the individual, and (h) the individual's name where it appears with other Personal Information relating to the individual or where the disclosure of the name would reveal other Personal Information about the individual.

Privacy Incident A privacy incident includes circumstances where there is a contravention of the privacy policies, procedures or practices implemented by Hospice Dufferin or agreements which Hospice Dufferin has entered into with external stakeholders and third party service providers, including but not limited to PHIPA agent agreements, data sharing agreements, confidentiality and non-disclosure agreements and agreements with third party service providers retained by Hospice Dufferin, where this contravention does not result in unauthorized collection, use, disclosure and destruction of PI/PHI or constitute noncompliance with applicable privacy law. A privacy incident may also be a suspected privacy breach.

Significant harm includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.

Policy

As per the Personal *Information Protection and Electronic Documents Act* (PIPEDA) regulations dated November 1, 2018, Hospice Dufferin will;

- report to the Privacy Commissioner of Canada any breaches of security safeguards involving personal information that pose a real risk of significant harm to individuals
- notify affected individuals about those breaches, and

- keep records of all breaches.

Procedures

Hospice Dufferin shall investigate all complaints concerning a breach of privacy. If a privacy breach occurs, Hospice Dufferin shall assess the situation and implement an appropriate action plan in a timely manner.

Any staff, student or volunteer that becomes aware of a privacy breach or of the possibility of a privacy breach must take immediate action as outlined below. Hospice Dufferin extends whistleblower protection to any employee, student or volunteer who reports a breach or a potential contravention of the Hospice Dufferin's Privacy Policy or of applicable legislation.

The five steps to manage a privacy breach are:
1. Report the breach or suspected breach,
2. Contain the breach,
3. Evaluate the risk associated with the breach,
4. Notify affected individuals,
5. Document, investigate and implement change.

STEP 1: Report the breach or suspected breach

1.1 Notify of possible breach

Any individual working on behalf of Hospice Dufferin who becomes aware of a privacy breach or a suspected privacy breach involving personal or health information in the custody or control of Hospice Dufferin will immediately inform their immediate supervisor and the privacy officer (Executive Director).

The following information is required when reporting the breach:

- What happened,
- When the incident occurred,
- How and when the incident was discovered,
- Type of data breached, number of people affected by the breach, and
- Whether any corrective action has already been taken.

The Chief Privacy Officer will verify the circumstances of the possible breach. The incident will be documented.

1.2 Determine if a breach has occurred

The Chief Privacy officer will assess the situation and determine if a breach has occurred.

To determine if a breach has occurred, two questions are critical to answer:
1. Is personal information involved? Identify the type of information affected by the incident in order to determine if a breach has occurred. Personal information is recorded information about an identifiable individual and includes, but is not limited to: race, nationality, religion, age, marital status, education, medical (such as a diagnosis), financial information, address, telephone number, opinions, etc.

2. Has an unauthorized disclosure occurred? Whether it is intentional, inadvertent or as a result of criminal activity, an unauthorized disclosure constitutes a privacy breach.
If the answer is yes to both questions, a privacy breach has occurred. The Chief Privacy Officer needs to follow the rest of the privacy breach response protocol outlined below.

1.3 If a breach has occurred as soon as the breach has been confirmed to have occurred, the Executive Director will inform the following:

- Person reporting the breach/possible breach
- The President of the Board of Directors and keep them updated.

This confirmation needs to occur within 24 hours of the initial report.

STEP 2: Contain the breach

When a breach of privacy has occurred, the following steps are to be followed. Some steps may be executed concurrently (i.e., notification and containment). The person who discovers the breach with support from the Executive director and other relevant individuals will immediately contain the breach in order to prevent further release of information (e.g. stop the un-authorized practice, recover records, shut down the system that was breached, revoke or change computer access codes, correct weaknesses in security, etc.).

Containment should occur simultaneously with notification (e.g., if a fax has gone to the wrong number, contact the recipient and ask that it not be read but shredded with an email to confirm).

Containment includes:

- Retrieve as much of the breached information as possible (ideally all);
- Destroy all copies of information that were collected without authorization;
- Ensure no copies of the confidential information have been made or retained by the individual who was not authorized to receive the information; obtain the individual's contact information in the event that follow-up is required;
- Ensure that further breaches cannot occur through the same means at this time.

In consultation with the Hospice Dufferin's Board president and/or legal counsel, the Chief Privacy Officer shall notify the police if the breach involves or may involve any criminal activity.

STEP 3: Evaluate the risks associated with the breach

To determine what other steps are immediately necessary, the Chief Privacy Officer will assess the risks associated with the breach.
The following factors need to be considered:

- Personal Information Involved - What data elements have been breached? Generally, the more sensitive the data, the higher the risk. Health information and financial information that could be used for identity theft are examples of sensitive personal information. - What possible use is there for the personal information? Can the information be used for fraudulent or otherwise harmful purposes?

- Cause and Extent of the Breach - What is the cause of the breach? - Is there a risk of ongoing or further exposure of the information? - What was the extent of the unauthorized collection, use or disclosure, including the number of likely recipients and the risk of further access, use or disclosure, including in mass media or online? - Is the information encrypted or otherwise not readily accessible? - What steps have already been taken to minimize the harm?
- Individuals Affected by the Breach - How many individuals are affected by the breach? - Who was affected by the breach: participants in Hospice Dufferin programs, events and services, donors, volunteers, staff, service providers, other organizations?

- Foreseeable Harm from the Breach - Is there any relationship between the unauthorized recipients and the data subject? - What harm to the individuals will result from the breach? Harm may include: security risk (e.g. physical safety), identity theft or fraud, loss of business or employment opportunities, and hurt, humiliation, damage to reputation or relationships. - What harm could result to Hospice Dufferin as a result of the breach? (e.g. loss of trust in the organization, loss of assets, and financial exposure.)

If the risk is determined to significantly impact the reputation of Hospice Dufferin, consideration will be given by the Executive Director and/ or other key individuals to activating the crisis communication plan.

If the information technology security risk is medium or high, consideration will be given to activate the IT disaster recovery plan.

STEP 4: Notify affected individuals / institutions about the privacy breach

The Chief Privacy officer will determine the need for notification using the guidelines below.

4.1 How to determine if notification of individuals / institutions is required the considerations below will help decide whether affected individuals should be notified. If either of the first two factors listed below applies, notification of the affected individuals must occur. The risk factors that follow are intended to serve as a guide. Considerations:

1. Legislation requires notification
The law requires that any breach of security safeguards involving personal information under your control if it is reasonable in the circumstances to believe that the breach of security safeguards creates a real risk of significant harm to an individual. Whether a breach of security safeguards affects one person or a 1,000, it will still need to be reported if your assessment indicates there is a real risk of significant harm resulting from the breach.

2. Contractual obligations require notification

3. Risk of identity theft • Identity theft is a concern if the breach includes unencrypted information such as names in conjunction with credit card numbers, personal health numbers, or any other information that can be used for fraud by third parties.

4. Risk of physical harm • does the loss of information place any individual at risk of physical harm, stalking, or harassment?

5. Risk of hurt, humiliation, damage to reputation • could the loss of information lead to hurt, humiliation or damage to an individual's reputation? This type of harm can occur with the loss of information such as medical records.

6. Risk of loss of business or employment opportunities

Notification should occur as soon as reasonably possible following a breach.
However, if law enforcement authorities have been contacted, it should be determined from those authorities whether notification should be delayed so as not to impede a criminal investigation.

4.2 Methods of notification

Individuals

The preferred method of notification is direct – by phone, in writing or in person – to the affected individuals. The following are considerations favouring direct notification:

- The identities of the individuals are known;
- Current contact information for the affected individuals is available;
- Individuals affected by the breach of privacy require detailed information to properly protect themselves from the harm arising from the breach;
- Individuals affected by the breach may have difficulty understanding an indirect notification (due to mental capacity, age, language, etc.). Indirect notification – website information, posted notices, advertisements or news releases – should generally be used only where direct notification could cause further harm, is prohibitive in cost, or contact information is lacking. Using multiple methods of notification in certain cases may be the most effective approach.

The following are considerations favouring indirect notification:

- A very large number of individuals are affected by the breach such that direct notification could be impractical;
- Direct notification could compound the harm to the individual resulting from the breach.

Organizations

The government will be notified by the Chief Privacy officer of a breach of security safeguards involving a real risk of significant harm must also notify any government institutions or organizations that the organization believes can reduce the risk of harm that could result from the breach or mitigate the harm.

A PIPEDA breach form can be found at:

https://www.priv.gc.ca/en/report-a-concern/report-a-privacy-breach-at-your-organization/report-a-privacy-breach-at-your-business/

The police will be notified by the Chief Privacy Officer of a breach that involves criminal activity.

The Chief privacy officer will notify any professional or regulatory bodies if required or appropriate including the college of Social Workers.

The technical supplier (i.e. Infoanywhere, eHealth) will be contacted if the breach was due to a technical failure and a recall or technical fix is required.

4.3 What to include in the notification of affected individuals

The purpose of providing notice of a privacy breach to the affected individual(s) is to provide them with sufficient information about:

- What happened and when,
- A generic description of the type(s) of personal information involved in the breach, including whether any unique identifiers of sensitive personal information were involved in the breach,
- The nature of potential or actual risks of harm,
- What action Hospice Dufferin has taken to address the situation,
- What appropriate action the individual(s) should take to protect themselves against harm (e.g. tracking credit cards, monitoring bank accounts, how to contact credit reporting agencies, etc.),
- Future steps Hospice Dufferin will take to prevent future privacy breaches,
- Hospice Dufferin contact for further information.

STEP 5: Documentation, Investigation and Remediation

5.1 Documenting the breach

All details of a privacy breach or suspected privacy breach and the containment strategy must be documented.

The Chief Privacy Officer will document the following information:

- The nature and scope of privacy breach (e.g. how many people are affected, what type of personal information is involved, the extent to which we have

contained the breach) or, if the nature and scope are not known at the time of briefing, that they are still to be determined.
- What steps have already been taken, or will be taking, to manage the privacy breach.
- The plans to notify the individuals affected by the privacy breach, and, if appropriate, other parties.
- If the breach was identified by an external source (e.g. individual, other institution, third party provider), document the information provided, including contact information for follow-ups, and any instructions given to the reporting party (e.g. asking caller to mail back the documents sent to the wrong address).
- The timetable for providing senior management with regular updates about the breach and its ongoing management.

5.2 Investigation and remediation

The Chief Privacy Officer will lead an internal investigation to:

- Identify and analyze the events that led to the privacy breach,
- Evaluate what was done to contain it,
- Recommend remedial action to help prevent future breaches.

These may include:

- Review relevant internal processes to ensure compliance with our privacy and confidentiality policy, - Amend or reinforce existing policies and practices for managing and safeguarding personal information,
- Develop and implement new security or privacy measures,
- Train staff on legislative requirements, security and privacy policies, practices and procedures,
- Test and evaluate remedial actions to determine if they have been implemented correctly and if policies and practices need to be modified.

As per legislation, records will be kept for two years.

Related Legislation

The *Personal Information Protection and Electronic Documents Act* (PIPEDA)

Related Policies

Accreditation

HPCO 00 ADM. 3 b The organization has policies and procedures in place relating to the safety and security of personal and personal health information (PHI) that align with current privacy legislation. At minimum, the P&P's must address: • Confidentiality (agreements for staff/volunteers and policy) • Breach of confidentiality (policy and process) • Collection, use, disclosure and retention of PHI (policy/procedure) • Education/Training on PHI (staff and volunteers + record of ongoing training) • Storage, retention and destruction of PHI

HPCO 00 AMD 3.c A privacy officer is appointed to manage and respond to any breaches of confidentiality.

Hospice Dufferin POLICY		
Title	Consent, Collection and Storage of Information	Document # Pr-2
Section	Privacy	Revision # Jan 24 2019
Application	Employees, Volunteers, Students, third parties	Issue date Jan 21 2004
Issued By	Executive Director	Replaces
		Next Review: Feb 2020
Approved By	Board of Directors	**Number of pages 8**

Purpose

"Personal Information", as specified in PIPEDA, is as follows: information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization.

The *Act* gives individuals the right to

- know why an organization collects, uses or discloses their personal information;
- expect an organization to collect, use or disclose their personal information reasonably and appropriately, and not use the information for any purpose other than that to which they have consented;
- know who in the organization is responsible for protecting their personal information;
- expect an organization to protect their personal information by taking appropriate security measures;
- expect the personal information an organization holds about them to be accurate, complete and up-to-date;
- obtain access to their personal information and ask for corrections if necessary; and
- complain about how an organization handles their personal information if they feel their privacy rights have not been respected.

The *Act* requires organizations to

- obtain consent when they collect, use or disclose their personal information;
- supply an individual with a product or a service even if they refuse consent for the collection, use or disclosure of your personal information unless that information is essential to the transaction;
- collect information by fair and lawful means; and
- have personal information policies that are clear, understandable and readily available.

Definitions

Personal Information Protection and Electronic Documents Act (PIPEDA) (the *Act*) is a Canadian law relating to data privacy governs how agencies collect, use and disclose personal information in the course of business.

Appropriate purpose -The purposes for which an organization collects and uses personal information must be appropriate and defined. Even with consent, privacy laws require organizations to limit collection, use and disclosure of personal information to purposes that a reasonable person would consider appropriate under the circumstances

Security safeguards – Security safeguards include the following:

- Physical measures, for example, locking filing cabinets and restricted access to offices;
- Organizational measures, for example, security clearances and limiting access on a "need-to-know" basis; and
- Technological measures, for example, the use of passwords and encryption.

Significant harm – Includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record, and damage to or loss of property

Policy

To obtain meaningful consent and meet their related obligations under Canadian privacy law, Hospice Dufferin will:

- Make privacy information readily available in complete form, while giving emphasis or bringing attention to four key elements:
    - What personal information is being collected, with sufficient precision for individuals to meaningfully understand what they are consenting to?
    - With which parties' personal information is being shared
    - For what purposes personal information is being collected, used or disclosed, in sufficient detail for individuals to meaningfully understand what they are consenting to.
    - Risks of harm and other consequences
- Provide information in manageable and easily-accessible ways.

- Make available to individuals a clear and easily accessible choice for any collection, use or disclosure that is not necessary to provide the product or service.
- Consider the perspective of your consumers, to ensure consent processes are user-friendly and generally understandable.
- Obtain consent when making significant changes to privacy practices, including use of data for new purposes or disclosures to new third parties.
- Only collect, use or disclose personal information for purposes that a reasonable person would consider appropriate, under the circumstances.
- Allow individuals to withdraw consent (subject to legal or contractual restrictions).

Procedures

Collection

1. Before collecting personal information it will be identified and documented why it is needed and how it will be used. Any changes in the collection of personal information (i.e. forms) must be reviewed by the Chief Privacy Officer. If there are any changes in the use of the information collected the individual will be informed.

2. According to the PIPEDA, Hospice Dufferin may collect information without the individual's knowledge or consent only:

   - if it is clearly in the individual's interest and consent is not available in a timely way
   - if knowledge and consent would compromise the availability or accuracy of the information and collection
   - is required to investigate a breach of an agreement or contravention of a federal or provincial law
   - for journalistic, artistic or literary purposes
   - if it is publicly available as specified in the regulations

3. All individuals receiving service are informed that they have a right to access their personal health information.

Consent

1. Hospice Dufferin will obtain informed consent from any individual whose personal information is collected, used or disclosed, as well as when a new use of their personal information is identified. Consent is first signed off in the Client agreement form. However, the employee should ask for verbal consent before sharing any information on a regular basis. This is in case; the client changes their mind. This consent should be documented in the client chart.

   Consent can be given in many ways:

   a. Express consent is given explicitly, either orally, in writing, or through a specific online action, such as clicking on "I agree". Express consent is unequivocal and does not require any inference on the part of the organization seeking consent.
   b. Implied consent arises where consent may reasonably be inferred from the action or inaction of the individual.
   c. Express, or opt-in, consent should be used whenever possible and in all cases when the personal information is considered sensitive. Relying on express consent protects both the individual and the organization.
   d. When using opt-out consent, Hospice Dufferin will establish a convenient procedure for withdrawing consent, and the opt-out should take effect immediately.

2. Employees, students and volunteers will explain how the information will be used and with whom it will be shared. This explanation should be clear, comprehensive, and easy to find.
3. We will retain proof that consent has been obtained when necessary.
4. We will not obtain consent by deceptive means.
5. We will not deny a product or service to an individual who fails to consent to the collection, use or disclosure of information beyond that required to fulfill an explicitly specified and legitimate purpose.
6. We will ensure that employees, students and volunteers collecting personal information are able to answer individuals' questions about why they are being asked for this information or if they cannot they will obtain the information for the individual.

Exceptions to the Consent Principle

List from *A Guide for Business and organizations PRIVACY TOOLKIT by the Office of the Privacy Commissioner of Canada (pg. 15) updated Dec 2015 https://www.priv.gc.ca/media/2038/guide_org_e.pdf)*

There are a number of specific exceptions to the requirements to obtain knowledge and consent for the collection, use or disclosure of personal information.

Organizations may collect personal information without the individual's knowledge or consent only:

- if it is clearly in the individual's interests and consent is not available in a timely way;
- if knowledge and consent would compromise the availability or accuracy of the information and collection is required to investigate a breach of an agreement or contravention of a federal or provincial law;
- for journalistic, artistic or literary purposes;
- if it is publicly available as specified in the regulations;
- when it is contained in a witness statement and the collection is necessary to assess, process, or settle an insurance claim;
- where it is produced by individuals in the course of their employment, business or profession–as long as the collection is consistent with the purpose for which the information was produced;
- when an individual is employed by a federal work, undertaking or business and the collection is necessary to establish, manage or terminate an employment relationship. The employer must, however, inform individuals in advance that their personal information could be collected for such purposes.

Storage of Personal Information

1. Personal information is stored securely and used only for the purposes for which it was collected, or as required by law.

- Personal information is retained only for the period of time that it is reasonably required.
- Personal information is destroyed that is no longer required using a safe, secure, and effective manner (e.g., shredding).
- All personal information collected is accurate.
- Individuals are allowed to gain access to their personal information, and make corrections as appropriate. An individual does this by contacting the Chief Privacy Officer.

- Appropriate security and safeguards are employed for the protection of personal information by all employees, students and volunteers including locking of offices, locking of filing cabinets, passwords, security keys for computer access etc.
- Access to personal information is limited to authorized personnel who have a legitimate need to access the information. Access to information is determined by the Chief Privacy Officer/Executive Director.
- Staff safeguard personal health information by use of passwords, locked cabinets, computer security keys, and by not leaving computers unattended when open
- Any removal of equipment and software must be removed by the Executive Director
- No software should be installed by employees without the approval of the Executive Director
- All computers must be protected with malware and anti- virus protection
- No personal information should be stored on removable media and devices unless approved by Executive director and ensuring that they are encrypted and protected from theft, loss and unauthorized use and disclosure. They should be locked
- Any personal information should be securely destroyed, permanently erased when no longer required.
- When accessing personal health information outside of the facility, all safeguards must be used including passwords, and computer security keys.
- No keys or passwords should be shared.
- Only people authorized by the Executive Director can repair or service computers

Sharing of Information

1. All individuals receiving service are informed that their personal health information may be shared with other members of the interdisciplinary team to facilitate efficient and effective care and that they have the right to withhold or withdraw their consent. Express consent may be required in some situations.

   Hospice Dufferin may <u>disclose</u> personal information without the individual's knowledge or consent only;
   (List from A Guide for Business and organizations PRIVACY TOOLKIT by the Office of the Privacy Commissioner of Canada (pg. 16 &17) updated Dec 2015 https://www.priv.gc.ca/media/2038/guide_org_e.pdf)

   - to a lawyer representing the organization;
   - to collect a debt, the individual owes to the organization;
   - to comply with a subpoena, a warrant or an order made by a court or other body with appropriate jurisdiction;
   - to the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) as required by the Proceeds of Crime (Money Laundering) and Terrorist Financing Act;

- to a government institution that has requested the information, identified its lawful authority to obtain the information, and indicates that disclosure is for the purpose of enforcing, carrying out an investigation, or gathering intelligence relating to any federal, provincial or foreign law; or suspects that the information relates to national 17 security, the defense of Canada or the conduct of international affairs; or is for the purpose of administering any federal or provincial law;
- to a government institution or an individual's next of kin or authorized representative when there are reasonable grounds to believe that the individual has been, is or may be the victim of financial abuse. Organizations however may make such a disclosure only for the purpose of preventing or investigating the abuse, and only if it is reasonable to expect that the disclosure with the knowledge or consent of the individual would compromise the ability to prevent or investigate the abuse;
- to another organization in instances where it is reasonable for the purposes of: o investigating a breach of an agreement or contravention of a federal or provincial law that has been, is being or is about to be committed; or o detecting or suppressing or preventing fraud that is likely to be committed. (However, it must be reasonable to expect that disclosure with the knowledge or consent of an individual would compromise the investigation of a law or agreement being broken or the ability to prevent, detect or suppress the fraud.) ᵖ in connection with a business transaction (for example, the sale or merger of a business, or the lease of a company's assets), provided certain conditions are met to, among other things, protect the information and limit its use;
- when it is contained in a witness statement, and the disclosure is necessary to assess, process, or settle an insurance claim;
- where it is produced by individuals in the course of their employment, business or profession–as long as the disclosure is consistent with the purpose for which the information was produced;
- in an emergency threatening an individual's life, health, or security (the organization must inform the individual of the disclosure);
- to a government institution, individuals' next of kin, or authorized representative if necessary to identify an individual who is injured, ill or deceased (and if alive, the individual has to be informed in writing that the disclosure took place);
- for statistical, scholarly study or research (the organization must notify the Privacy Commissioner before disclosing the information); to an archival institution;
- 20 years after the individual's death or 100 years after the record was created;
- if it is publicly available as specified in the regulations; or
- if required by law

2. Sharing of electronic personal health information through email is not guaranteed to be private. Therefore, personal health information should only be shared using the Onemail id system to identify the provider is working within the system and not in the larger internet

forum. All emails sent through Hospice Dufferin email accounts are backed up on the eHealth server and can be retrieved for evidence.

3. Sharing of personal health information through fax should be done only as a last resort. No faxes should be received to Hospice Dufferin.

4. Make sure personal information that has no relevance to the transaction is either removed or blocked out when providing copies of information to others.

Related Polices

Finance Policy – Retention of Records

Accreditation

HPCO 00 ADM 3b. The organization has policies and procedures in place relating to the safety and security of personal and personal health information (PHI) that align with current privacy legislation. At minimum, the P&P's must address: • Confidentiality (agreements for staff/volunteers and policy) • Breach of confidentiality (policy and process) • Collection, use, disclosure and retention of PHI (policy/procedure) • Education/Training on PHI (staff and volunteers + record of ongoing training) • Storage, retention and destruction of PHI

HPCO 00 ADM 3d. All individuals receiving service are informed that their personal health information may be shared with other members of the interdisciplinary team to facilitate efficient and effective care and that they have the right to withhold or withdraw their consent. Express consent may be required in some situations.

Hospice Dufferin Policy		
Title	Privacy Officer and Information Security Mgmt.	Document # Pr-2
Section	Privacy	Revision # April 2020
Application	Employees, Volunteers, Students, third parties	Issue date Jan 21 2004
Issued By	Executive Director	Replaces Next review yearly: Feb 2020
Approved By	Board of Directors	**Number of pages 4**

Purpose

To comply with the Personal Information Protection and Electronics Documents Act (PIPEDA) by appointing an individual to be responsible for implementing compliance and reporting privacy issues to the Board of Directors.

Definitions

Registration – the process of verifying the identity of applicants and proving that they are who they claim to be.

Service Enrolment – the process of providing registrants with access to services.

Legally Responsible Person (for Registration) The Legally Responsible Person (LRP) is the individual who is legally responsible for the registration process in the organization.

Policy

The Executive Director of Hospice Dufferin acts in the following capacitates;

Chief Privacy Officer - responsibility is to ensure that Hospice Dufferin is in compliance with the laws, rules, orders, regulations and by-laws regarding privacy in Ontario including PHIPA, FIPPA and orders made by the Information and Privacy Commissioner/ Ontario and stakeholder expectations. The Chief Privacy Officer's will ensure that appropriate training is provided throughout the agency.

Legally Responsible Person (for registration) – responsible for the registration process in the organization.

Local Registration Authority - responsible for communicating registrations and revocations, identity proofing, etc... A LRA is required for eHealth registrations including oneid (emails).

Procedures

Chief Privacy Officer

1. The Executive Director is designated the Chief Privacy Officer by the Board of Directors.

2. The name or the title of the Chief Privacy Officer will be communicated both internally and externally including the Hospice Dufferin website and Client agreements.

3. The Chief Privacy Officer will audit and analyze information handling practices, using the following checklist to ensure that Hospice Dufferin meets fair information practices:
   - What personal information do we collect?
   - Why do we collect it?
   - How do we collect it?
   - What do we use it for?
   - How to obtain consent for collecting and use?
   - How to ensure accuracy?
   - Where do we keep it?
   - How is it secured?
   - Who has access to or uses it?
   -To whom it is disclosed?
   -When is it disposed of?

4. The Chief Privacy Officer will report as part of the regular Board of Directors report any concerns, complaints or actions taken in regards to PIPEDA, or privacy of personal information

5. The Chief Privacy Officer will ensure that staff/volunteers are trained on privacy policies and procedures.
   They will be informed so they can answer the following questions:
   - How do I respond to public inquiries regarding Hospice Dufferin's privacy policies?
   - What is consent? When and how is it obtained?
   - How do I recognize and process requests for access to personal information?
   - To whom should I refer complaints about privacy matters?
   - What are the ongoing activities and new initiates relating to the protection of personal information at our organization?

6. The Privacy Officer will review access logs, at a minimum of a quarterly basis, activities of a subsets of users accessing Health information and a record of the audit is maintained. This includes the outside agencies that have this in their agreement. (e.g. LHIN, OHT)

Local Registration Authority

Your responsibilities include:

- Adhering to all compliance and auditing requirements established by the provincial government, the Ministry of Health and Long-Term Care, Hospice Dufferin, LHIN and eHealth Ontario.
- Adhering to and communicating the Privacy and Security practices
- Establishing and communicating discretionary guidelines.
- Notifying registrants of all relevant information pertaining to their rights and obligations.
- Being accountable for transactions performed as an LRA.
- Validating the identity of individuals with documents and appropriate background checks. A record is maintained that names the documents provided and the date these were verified.
- Creating "@ONEID.ON.CA" accounts for individuals
- Adding service enrolments to authorized accounts including Coordinated care plans
- Liaising with eHealth Ontario or other third party organization on registration issues.
- Responding to eHealth Ontario requests for assistance in validating the identity of individuals.

Where can an LRA do?	Where	How
Register new user and/or enroll first time user		• Complete the new user registration tasks • Enroll the new user
Revoke enrolment	Log into the One Id system	Revoke the user's enrollment when they no longer need this service (i.e. retired, no longer with the organization)
Suspend enrolment		Suspend enrolment due to an extended leave (i.e. medical, sabbatical, parental etc.)e
Re-instate enrolment		Reinstate a user when they return from an extended leave
Request access to an existing one mail direct mailbox	Email One mail info box	Complete and submit all section of the Account Access Request form

Accreditation

HPCO ADM 3b. The organization has policies and procedures in place relating to the safety and security of personal and personal health information (PHI) that align with current privacy legislation. At minimum, the P&P's must address: • Confidentiality (agreements for staff/volunteers and policy) • Breach of confidentiality (policy and process) • Collection, use, disclosure and retention of PHI (policy/procedure) • Education/Training on PHI (staff and volunteers + record of ongoing training) • Storage, retention and destruction of PHI

HPCO 00 ADM 3c. A privacy officer is appointed to manage and respond to any breaches of confidentiality.

Title	Privacy Safeguards	Document # Pr-4
Section	Privacy	Revision # April 2020
Application	Employees, Volunteers, Students, third parties	Issue date Jan 21 2004
Issued By	Executive Director	Replaces Next Review Yearly: Feb 2020
Approved By	Board of Directors	**Number of pages 3**

Purpose

The purpose of privacy safeguards includes:

- Protect personal information against loss or theft.
- Safeguard the information from unauthorized access, disclosure, copying, use or modification.
- Protect personal information regardless of the format in which it is held.

Definitions

telework: a flexible work arrangement whereby employees have approval to carry out some or all of their work duties from a telework place

Policy

Privacy Safeguards will be in place to ensure privacy of information and will be reviewed by the Chief Privacy officer on a yearly basis or as required when new systems are put in place.

Procedures

1. Appropriate security safeguards will be used and monitored to provide necessary protection including
    - physical measures (locked filing cabinets, restricting access to offices, alarm systems)
    - technological tools (passwords, encryption, firewalls)
    - organizational controls (security clearances, limiting access on a “need-to-know” basis, staff training, agreements)
    - all users of electron health information systems are assigned a unique identifier

2. The Chief Privacy Officer will review security safeguards to ensure they are up-to-date and known vulnerabilities have been addressed. A list of safeguards will be maintained by the Chief Privacy Officer. Any new systems will be reviewed for security.

   The following factors will be considered in selecting appropriate safeguards;
   - sensitivity of the information
   - amount of information
   - extent of distribution
   - format of the information (electronic, paper, etc.)
   - type of storage

3. Employees, students and volunteers will receive training on confidentiality and privacy at orientation. They will sign a confidentiality agreement on a yearly basis. Employees that have access to Health records accounts will be kept updated and immediately upon termination will be removed from the system.

4. Hospice Dufferin will ensure there is a contractual arrangement in place with any third-party processor of information to address compliance with the breach provisions set out in PIPEDA including notification and record-keeping obligations.

5. Upon termination of an employee, student or volunteers, Hospice Dufferin should terminate the access privileges of each registered user connected to health information. Additionally, access to systems should be reviewed on a quarterly basis and access removed or modified as appropriate. A record of audits and changes should be maintained.

Teleworking

1. When working from a remote location, a 2 factor authentication must be used to connect to personal health information files. Internet connections should be through a secure network and not a public network. Teleworking should be done in a private not a public space.

Insurance Coverage

1. Hospice Dufferin will ensure that they maintain appropriate insurance coverage (cyber insurance).

Related Policies

Finance Policy – Retention of Records
Privacy Policy – Collection and Storage of information, Third Party Agreements

Accreditation

HPCO ADM 3a. All personnel (I.e. staff, volunteers, contracted service providers, students) are informed of their responsibility to protect the security of personal and personal health information*. This includes any information about individuals receiving service that is obtained, heard or seen during their work. All personnel receive education on privacy and confidentiality and sign a confidentiality agreement. The education and agreement is renewed annually.

HPCO ADM 3b. The organization has policies and procedures in place relating to the safety and security of personal and personal health information (PHI) that align with current privacy legislation. At minimum, the P&P's must address: • Confidentiality (agreements for staff/volunteers and policy) • Breach of confidentiality (policy and process) • Collection, use, disclosure and retention of PHI (policy/procedure) • Education/Training on PHI (staff and volunteers + record of ongoing training) • Storage, retention and destruction of PHI

HPCO ADM 3g. If health information is stored electronically, the organization has appropriate insurance coverage (cyber-insurance)

	Hospice Dufferin Policy	
Title	Security Incidents Involving Electronic Health Records	Document # Pr-2
Section	Privacy	Revision # Jan 24 2019
Application	Employees, Volunteers, Students, third parties	Issue date Jan 21 2004
Issued By	Executive Director	Replaces Next review year: Feb 2020
Approved By	Board of Directors	**Number of pages 4**

Purpose

The aim of this policy is to ensure that Hospice Dufferin reacts appropriately to any actual or suspected security incidents relating to information systems and data.
Examples of the most common Information Security Incidents are listed below. It should be noted that this list is not exhaustive.

Malicious

- Giving information to someone who should not have access to it - verbally, in writing or electronically.
- Computer infected by a Virus or other malware.
- Sending a sensitive e-mail to 'all staff' by mistake.
- Receiving unsolicited mail of an offensive nature.
- Receiving unsolicited mail which requires you to enter personal data.
- Finding data that has been changed by an unauthorized person.
- Receiving and forwarding chain letters – including virus warnings, scam warnings and other emails which encourage the recipient to forward onto others.
- Unknown people asking for information which could gain them access to council data (e.g. a password or details of a third party).

Misuse

- Use of unapproved or unlicensed software on Hospice Dufferin equipment.
- Accessing a computer database using someone else's authorization (e.g. someone else's user id and password).
- Writing down your password and leaving it on display / somewhere easy to find.
- Printing or copying confidential information and not storing it correctly or confidentially.

Theft / Loss

- Theft / loss of a hard copy file.

- Theft / loss of any Hospice Dufferin computer equipment.

Definitions

An Information Security Incident includes, but is not restricted to, the following:

- The loss or theft of data or information.
- The transfer of data or information to those who are not entitled to receive that information.
- Attempts (either failed or successful) to gain unauthorized access to data or information storage or a computer system.
- Changes to information or data or system hardware, firmware, or software characteristics without the Council's knowledge, instruction, or consent.
- Unwanted disruption or denial of service to a system.
- The unauthorized use of a system for the processing or storage of data by any person.

Policy

Hospice Dufferin will ensure that it reacts appropriately to any actual or suspected incidents relating to information systems and information within the custody of the agency.

Procedures

1.0 Reporting Information Security Events

Security events, for example a virus infection, could quickly spread and cause data loss across the organization. All users must understand, and be able to identify that any unexpected or unusual behavior on the workstation could potentially be a software malfunction. If an event is detected users **must**:

- Note the symptoms and any error messages on screen.
- Not use any removable media (for example USB memory sticks) that may also have been infected.

All suspected security events should be reported immediately to the Executive Director.
If the Information Security event is in relation to paper or hard copy information, for example personal information files that may have been stolen from a filing cabinet, this must be reported to Executive Director for the impact to be assessed.

The following information will be collected

- Contact name and number of person reporting the incident.
- The type of data, information or equipment involved.
- Whether the loss of the data puts any person or other data at risk.
- Location of the incident.
- Inventory numbers of any equipment affected.

- Date and time the security incident occurred.
- Location of data or equipment affected.
- Type and circumstances of the incident.

In the event that the personal information is shared between two organizations, the Executive Director is to contact the other organization to report an incident. An example is OACCAC Prism team or the hospital It.

2.0 Reporting Information Security Weaknesses

Security weaknesses, for example a software malfunction, must be reported through the same process as security events. Users must not attempt to prove a security weakness as such an action may be considered to be misuse.

Audits on a yearly basis should be conducted by the Executive Director on all systems with Personal Health information.

3.0 Learning from Information Security Incidents

To learn from incidents and improve the response process incidents must be recorded and a Post Incident Review conducted. The following details must be retained:

- Types of incidents.
- Volumes of incidents and malfunctions.
- Costs incurred during the incidents.

Type of Impact	Reputational Media and Member Damages	Reputational Loss within Government and / or Failure to Meet Statutory / Regulatory Obligations	Contractual Loss	Failure to meet Legal Obligations	Disruption to Activities	Personal Privacy Infringement
Low	None	None	None	None	None	None
	Contained internally within HD Unfavorable response	Internal investigation or disciplinary involving one individual	Minor contractual problems / minimal SLA failures	Civil lawsuit / small fine -	Minor disruption to service activities that can be recovered	Personal details revealed or compromised
Medium	Unfavorable local media interest	Government authorized investigation by national Privacy commission	Significant client dissatisfaction.	Damages and fine	Disruption to service that can be recovered with an intermediate	Personal details revealed or compromised internally

					level of difficulty	within authority. Harm mental or physical to clients or staff
High	Sustained local media coverage, extending to national media coverage in the short term	Government intervention leading to significant business change.	Failure to retain funding at the point of renewal Or assess to other systems	Greater than $100,000 fine	Major disruption to service which is very difficult to recover from. Two or more systems not being backed up for two or more days	Severe embarrassment to individual(s)
	Sustained unfavorable national media coverage	Service or product outsourced through Government intervention	Client contract(s) cancelled	Over $1M damages and / or fine	Catastrophic disruption - service activities can no longer be continued	Detrimental effect on personal & professional life OR large scale compromise affecting many people. Harm mental or physical to two or more members of staff or public

Related Policies

Accreditation

Hospice Dufferin POLICY		
Title	Third Party Agreements	Document # Pr-5
Section	Privacy	Revision #
Application	Employees, Volunteers, Students, Third Parties	Issue date Feb 2019
Issued By	Executive Director	Replaces Next review: Feb 2020
Approved By	Board of Directors	**Number of pages 4**

Purpose

The privacy laws recognize that personal information transferred to a third party for processing (e.g. outsourcing; service provision) is *not* disclosed to that party, but remains, under the relevant privacy law, the responsibility of the transferring organization (the "data collector"). The laws also mandate the data collector to ensure that the service provider organization applies the same level of protection to that data while within its custody or control as the data collector is obliged to provide under its relevant law.

Definitions

Third party A third party can be any outside individual (such as a consultant), a business or an organization that provides a service to, or acts of behalf of, an institution.

A third party arrangement may include:

a) outsources management or controls of all or some part of Hospice Dufferin's solution;
b) uses third-party facilities management for access to their systems; or
c) permits access to their systems by third parties.

Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F. 31 (FIPPA) A provincial privacy statute that provides a right to access information under the control of institutions in accordance with the principles that information should be available to the public; necessary exemptions from the right of access should be limited and specific; and decisions on the disclosure of government information should be reviewed independently of government. FIPPA also protects the privacy of personal information of individuals held by institutions. It provides individuals with a right of access to, and correction of, that information.

Personal Health Information Protection Act, 2004, S.O. 2004, c. 3. (PHIPA) A provincial health privacy statute that establishes rules for the management of PHI and protection of the

confidentiality of that information, while facilitating the effective delivery of healthcare services.

Policy

Hospice Dufferin will have third party contracts containing all necessary security requirements including:

- an acknowledgement that the service provider holds personal information on behalf of and (as applicable, e.g. under PHIPA) as agent for the data collector;
- an obligation on the service provider to protect the personal information from unauthorized disclosure or loss including meeting stipulated objective or recognized standards;
- an obligation of the service provider to refer all requests for access to personal information to the data collector
- an obligation of the service provider not to use or disclose to third parties' personal information except is authorized by the data collector;
- an obligation of the service provider to return to the data collector and delete or destroy personal information at any time as directed by the data collector or in any event at the end of the agreement term;
- an audit right for the data collector to inspect the service provider's procedures and facilities;
- (as applicable) a restriction or procedural requirement in connection with any cross-border transfer or data storage and a requirement of the service provider to notify immediately the data collector in the event of any court, law enforcement or national security authority access to personal information;
- an obligation of the service provider to notify immediately the data collector in the event of any unauthorized use/disclosure, loss or other security breach and to provide full cooperation to the data collector in responding to such incident;
- an obligation of the service provider to comply with applicable privacy laws and to conduct itself in a manner that does not cause the data collector to breach such laws.

Procedures

1.0 Written Agreement

The written agreement should include:

Collection

Where a third party is collecting personal information on behalf of Hospice Dufferin, they must comply with the provisions regarding the authority to collect, the manner of collection and notice of collection. The requirements are in sections 38, 39(1) and 39(2) of the provincial Act.

Retention
The third party must adhere to the minimum retention periods for personal information in accordance with section 5 of R.R.O. 1990, Reg. 460 under the provincial Act.

Use and Disclosure
Regardless of how the third party receives the personal information, the third party must use it in accordance with Ontario's access and privacy legislation. Specifically, sections 41 and 42 of the provincial Act.

Disposal
A clause should be included in the agreement to outline approved procedures and methods to dispose of personal information in the custody of the third party.

Security
Third parties must implement the necessary precautions to ensure that personal information can be reproduced if the original information is accidentally lost or destroyed. (This is for basic security and to ensure the minimum retention period.) After the personal information has been returned to the government institution, the institution must be assured that the third party cannot reproduce it. Security procedures must meet the requirements outlined in section 4 of R.R.O. 1990, Reg. 460 under the provincial Act and section 3 of R.R.O. 1990, Reg. 823 under the municipal Act.

Out of Province third part contracts
If an institution hires a consultant who resides outside the province or country, personal information may be transferred to another jurisdiction. Privacy breaches could occur if this jurisdiction does not have privacy legislation to protect personal information, or if the third party is not sensitive to privacy issues. Therefore, this will be a consideration when developing a relationship with the third party.

2. **Logging and Document Retention**

The Chief Privacy Officer shall maintain standard content about privacy for agreements with third party providers. The CPO shall periodically review and update the standard content to ensure it is up-to-date and accurate.

Legislation

Personal Health Information Protection Act, 2004 (PHIPA) and its regulation: under section 6.2 of Ontario Regulation (O. Reg.) 329/04, section 6 of O. Reg. 329/04

Section 6 and section 6.2 of the O.Reg. 329/04 to PHIPA requires eHealth Ontario to ensure that any third party it retains to assist it in providing services related to its roles under PHIPA agrees to comply with the restrictions and conditions that are necessary to enable eHealth Ontario to comply with all these requirements.

Related Policies

Accreditation

HPCO AMD 3 f If health information is stored electronically, the organization ensures that the vendor storing the health information abides by relevant legislation (PHIPA).

Appendices

HPCO Privacy Standards

OO.ADM.3 – Information Privacy
As Health Information Custodians (HIC) under PHIPA, organizations providing hospice palliative care services abide by the legal and ethical responsibility to maintain the confidentiality and privacy of personal and personal health information* whether in written or electronic form, in accordance with current legislation, best practice and professional standards.
Criteria

a. All personnel (I.e. staff, volunteers, contracted service providers, students) are informed of their responsibility to protect the security of personal and personal health information*. This includes any information about individuals receiving service that is obtained, heard or seen during their work. All personnel receive education on privacy and confidentiality and sign a confidentiality agreement. The education and agreement is renewed annually.

b. The organization has policies and procedures in place relating to the safety and security of personal and personal health information (PHI) that align with current privacy legislation. At minimum, the P&P's must address: • Confidentiality (agreements for staff/volunteers and policy) • Breach of confidentiality (policy and process) • Collection, use, disclosure and retention of PHI (policy/procedure) • Education/Training on PHI (staff and volunteers + record of ongoing training) • Storage, retention and destruction of PHI

c. A privacy officer is appointed to manage and respond to any breaches of confidentiality.

d. All individuals receiving service are informed that their personal health information may be shared with other members of the interdisciplinary team to facilitate efficient and effective care and that they have the right to withhold or withdraw their consent. Express consent may be required in some situations. (define in glossary)

e. All individuals receiving service are informed that they have a right to access their personal health information. In some circumstances, access may be refused. (define in glossary)

f. If health information is stored electronically, the organization ensures that the vendor storing the health information abides by relevant legislation (PHIPA).

g. If health information is stored electronically, the organization has appropriate insurance coverage (cyber-insurance)