Information Privacy & Confidentiality Policy

Approved May 16, 2016

Effective Date	May 16, 2016
Approved By	Board of Directors
Date of Most Recent Approval	May 16, 2016
Position Responsible for Developing & Maintaining Policy	Sr. Vice President for Finance & Information Systems

1. Introduction

1.1. Description

VGH & UBC Hospital Foundation (the "Foundation") has ethical and legal obligations to protect all Personal Information it collects, uses and discloses. The Foundation may also be obliged under contract or other circumstances to protect Confidential Information.

The purpose of this Information Privacy & Confidentiality Policy ("Policy") is to establish the guiding principles and framework by which the Foundation and its Staff will comply with these obligations, demonstrate accountability for managing the collection, use, disclosure, and safekeeping of Personal Information and Confidential Information and maintain its trust-based relationship with Donors, Staff, business, health care partners and the public.

1.2. Scope

This Policy applies to Personal and Confidential Information collected, used, disclosed and retained by the Foundation.

1.3. Definitions

TERM	DEFINITION
Donors	Any individual or organization who donates funds to VGH & UBC Hospital Foundation or any prospective donors the Foundation is work with.
Confidential Information	All information that is specifically identified as confidential or is reasonably understood to be of a confidential nature, that Staff receive or have access to through the Foundation, including vendor contracts and other proprietary information that may have been received from a third party. Includes all non-public information that might be useful to competitors, or harmful to the Foundation if disclosed, and all private and non-public information about the Foundation's donors and prospective donors.

TERM	DEFINITION
Employee Personal Information	Personal Information about an individual that is collected, used or disclosed solely for the purposes reasonably required to establish, manage or terminate an employment relationship with the Foundation. It does not include Personal Information that is not about an individual's employment.
PIPA	The BC *Personal Information Protection Act*, as amended from time to time.
Personal Information	Any information about an identifiable individual, including Employee Personal Information, but not including business contact information (e.g. individual's title, business telephone number, business address, business email or facsimile number), or any work product information.
Senior Leadership	Comprised of President and CEO, Sr. VP for Philanthropy and Sr. VP for Finance and Information Systems, or a delegate chosen by Senior Leadership.
Staff	All employees (including management and leadership), students, volunteers, contractors and other service providers engaged by the Foundation.

2. Policy

2.1. Privacy Legislation and Policies

The Foundation and its Staff are governed by PIPA, the *Society Act,* and other legislation, professional codes of ethics and standards of practice.

The Foundation will comply with all applicable provisions of PIPA in relation to the collection, use, and disclosure of Personal Information. Wherever PIPA may conflict with this policy or its application, PIPA will prevail.

All Staff must ensure that their practices in collecting, accessing, using or disclosing Personal Information and Confidential Information comply with this Policy as well as applicable laws, professional codes of practice and contractual obligations. These obligations for ensuring privacy and confidentiality continue after the employment, contract or other affiliation between the Foundation and its Staff comes to an end.

2.2. Confidentiality Undertaking

All Staff must sign the Foundation's Confidentiality & Conflict of Interest Agreement annually.

2.3. Consent to Collect, Use or Disclose Personal Information

The Foundation will generally obtain consent from individuals regarding the purpose for collection, use or disclosure of personal information before, or at the time it collects the personal information as required by law. Consent may be express, deemed or implied.

Consent may be express or implied. Implied consent includes cases where an individual has, of their own initiative, provided the Foundation with Personal Information.

In some circumstances, as permitted by PIPA, the Foundation may provide notice to its employees before collecting, using or disclosing employee personal information, which is personal information reasonably necessary for establishing, managing, or concluding the employment relationship. Notice may be express, constructive or implied in the circumstances.

The Foundation will collect, use or disclose Personal Information without the required notice or consent only as permitted by law.

In determining the appropriate form of notice or consent, the Foundation will consider the sensitivity of the Personal Information and the reasonable expectations of the subject individual.

Subject to certain legal or contractual restrictions and reasonable notice, an individual may withdraw consent and the Foundation will stop collecting, using or disclosing Personal Information unless the collection, use or disclosure is permitted by law.

The Foundation may collect, use or disclose Personal Information without consent in other limited circumstances as permitted by law. For example, the Foundation may collect information without consent if doing so might defeat the purpose of collecting the information, such as in the investigation of a breach of an agreement or law. The Foundation may also disclose Personal Information without consent to a lawyer representing the Foundation to comply with a subpoena, warrant or other court order, or as may be otherwise required or authorized by law.

2.4. Collection of Personal Information

Staff may collect Personal Information as reasonably required to operate Foundation programs or activities and will not collect more Personal Information than a reasonable person would consider appropriate in the circumstances is required to fulfill those purposes.

<u>Direct Collection</u>

Where possible, the Foundation will collect Personal Information directly from the individual the information is about.

- When Staff collects Personal Information directly from an individual, the individual should be informed of: the purpose for the collection; and
- the contact person if the individual collecting the information cannot answer questions about the collection.

<u>Indirect Collection</u>

Staff may collect Personal Information indirectly (from sources other than the individual the information is about):

- with the consent of the individual, or notice to the employee;
- where another entity is authorized to disclose the Personal Information to the Foundation; or

- as otherwise permitted by PIPA.

2.5. Accuracy of Personal Information

The Foundation and its Staff will take all reasonable steps to ensure Personal Information in its possession is kept accurate and up-to-date. The Foundation will only update Personal Information if it is necessary to fulfill the purposes for which the Personal Information was collected. Staff will exercise reasonable diligence to protect against errors due to carelessness or oversight.

2.6. Use of Personal Information

Personal Information collected by the Foundation may only be used for the purpose(s) for which it was collected or as otherwise permitted by law.

Staff will only access Personal Information on a "need to know" basis, and only to the extent required to perform his or her job functions and responsibilities.

Staff must not use any Personal Information accessed in the course of their work for any other purpose than the purpose for which it was collected, unless they obtain consent, provide the required notice, or the use is otherwise permitted by law.

2.7. Disclosure of Personal Information

The Foundation may only disclose Personal Information as reasonably required in the circumstances to fulfil the purpose(s) for which it was collected or as otherwise permitted by law. All requests for disclosure will be referred to the Senior Leadership.

Disclosure with Consent
Besides the disclosures described above and other disclosures authorized by PIPA, the Foundation may disclose Personal Information with consent. Individual consent should be in writing.

Disclosure without consent to Law Enforcement
The Foundation will comply with all appropriate requests for disclosures of Personal Information to law enforcement (e.g. mandatory demands such as court orders or search warrants, requests by law enforcement or Foundation-initiated reporting to law enforcement). All disclosure requests from law enforcement will be referred to the Senior Leadership.

Requirements for Third Party Access to Personal Information
Where Personal Information is shared with, accessed or stored by a third party vendor, contractor, agency or other organization, a written agreement or other legal documentation may be required. Staff must consult with the Senior Leadership to determine what documentation is required before granting a third party access to any Personal Information in the Foundation's possession and/or control.

Examples where legal documentation which may be required are as follows:

- access by a third party organization to Foundation information systems;

- services provided by a vendor who will have access to Personal Information; and
- program that requires Personal Information to be shared with another agency.

Access to Personal Information
On written request, the Foundation will inform a person of the personal information it has in its possession and control relating to that individual. Individuals can seek access to their Personal Information. Requests will be referred to the Senior Leadership.

Except for employee personal information, the Foundation may charge a fee according to the cost required to retrieve and provide the requested information. The Foundation may provide an estimate of the fee in advance and in some cases, will require a deposit for all or part of the fee.

Access to Employee Information
Requests for employee information should be directed to the Director, Organizational Development & Human Resources.

In some cases, the Foundation may not provide access to Personal Information where the denial of access is authorized by law. Examples include information that:

(a) is work product information and/or disclosure could reveal confidential commercial or corporate information;
(b) is protected by solicitor-client privilege;
(c) relates to existing or anticipated legal proceedings against the individual making the request;
(d) is collected for purposes of an investigation or the information is the result of an arbitration or other formal dispute resolution process;
(e) would reveal personal information concerning another individual;
(f) would reveal the identity of an individual who has provided personal information concerning another individual, such as reports, assessments and reviews, and the individual providing the personal information does not consent to disclosure of his or her identity;
(g) a denial of access is necessary to protect the Foundation's rights and property or the rights and property of associated organizations, affiliates, agents, directors, or shareholders;
(h) could reasonably be expected to threaten the safety or physical or mental health of an individual; and
(i) where the request is frivolous or vexatious.

If the Foundation denies an individual's request for access to personal information, the Foundation will advise the individual of the reason for the refusal.

2.8. Safeguards

The Foundation must take reasonable security precautions to protect Personal Information and Confidential Information against unauthorized access, collection, use, disclosure or

disposal. Personal Information must be protected by appropriate safeguards according to the sensitivity of the information, regardless of the format in which it is held.

Physical Measures and Safeguards

Staff will comply with Foundation's physical security requirements and will take all reasonable steps to protect Personal Information and Confidential Information against unauthorized access, collection, use, disclosure or disposal, including:

- keeping hard copies of files and records containing Personal Information or Confidential Information in a secure location, such as locked storage rooms or locked filing cabinets, with controls over distribution of keys or lock combinations;
- protecting mobile electronic devices and storage media containing Personal Information or Confidential Information against theft, loss or unauthorized access;
- using available security systems (e.g., locking offices when not in use, activating alarm systems);
- refraining from disclosing and discussing Personal Information or Confidential Information in public areas where third parties may overhear or view records containing Personal Information or Confidential Information;
- following Foundation guidelines and procedures for the secure destruction or disposal of Personal Information or Confidential Information that is no longer required to ensure the Personal Information or Confidential Information is destroyed, erased or made anonymous; and
- prohibiting removal of records containing Personal Information or Confidential Information from Foundation premises except as necessary, and, in such cases ensuring they are kept in a secure location and not exposed to risk of loss, theft or unauthorized access.

Technical Measures and Safeguards

Staff will comply with Foundation technical security requirements and will take all reasonable steps to maintain the integrity of electronic systems, including:

- protecting the integrity of passwords, user id's and other security access measures;
- logging off computers when not in attendance; and
- using encryption and password protection for mobile electronic devices and storage media.

2.9. Privacy Impact Assessment

A Privacy Impact Assessment ("PIA") may be completed before implementing or significantly changing any program or system that requires the collection, use, disclosure or sharing of Personal Information.

Before undertaking any new initiative, program or activity that involves Personal Information, Foundation departments must contact the Senior Leadership to determine whether a PIA is required. Completion of a PIA is the responsibility of the department undertaking the program or activity, with support from the Senior Leadership.

2.10. Privacy Training

The Foundation will ensure that Staff who manage, access or use Personal Information receive privacy and information management training when initially hired and as required on an ongoing basis. The Foundation will develop privacy education programs to educate all Staff and users of Personal Information about the Foundation's privacy obligations under PIPA.

2.11. Retention and Destruction of Personal Information

The Foundation must retain for a minimum of one year Personal Information that is used to make a decision that directly affects the individual the information is about.

The Foundation must destroy documents containing Personal Information or remove the means by which it can be associated with particular individuals as soon as it is reasonable to assume that the information is no longer serving its intended purpose or retention is no longer necessary for legal or business purposes.

2.12. Whistleblower Protection

The Foundation will not dismiss, suspend, demote, discipline, harass or otherwise disadvantage a Staff member who, acting in good faith and upon a reasonable belief, has done or intends to do the following:

- make a report to the appropriate authority about a foreign demand for Personal Information;
- disclose to the BC Office of the Information and Privacy Commissioner that the Foundation or another individual has contravened PIPA;
- do something required to avoid contravention of PIPA or refuse to contravene PIPA; or
- inform the Foundation about a breach of or violation of this Policy.

The Foundation will use its best efforts to keep confidential the name and identifying information of any Staff who report an actual or suspected breach of privacy or violations of this Policy.

2.13. Challenging Compliance

The Senior Leadership will investigate all complaints concerning compliance with this Policy, and, if a complaint is found to be justified, will take appropriate measures including amending policies and procedures where required. The complainant will be informed of the outcome of the investigation regarding the complaint.

2.14. Reporting Privacy Breaches

Staff must immediately report to the Senior Leadership any actual or suspected breaches of privacy or violations of this Policy, including the theft or loss of Personal Information, devices or paper records. Privacy breaches will be dealt with in accordance with the Foundation's guidelines.

2.15. Responsibilities

2.15.1. President & Chief Executive Officer / Senior Leadership

The President & Chief Executive Officer of the Foundation is the appointed head of the Foundation for the purposes of exercising the powers of the head and ensuring the Foundation's compliance with PIPA. The authority of the head of the Foundation over matters relating to the protection of Personal Information and Confidential Information is delegated to the members of the Senior Leadership.

The Senior Leadership is responsible for:

- general oversight of privacy practices and policies within the Foundation;
- providing privacy education to Staff and promoting good privacy practices throughout the organization;
- responding to questions from Staff, Donors and members of the public concerning collection, access, use and disclosure of Personal Information; and
- investigating potential and actual breaches of this Policy brought to its attention and reporting breaches in accordance with the Foundation's breach policies.

2.15.2. Director, Organizational Development & Human Resources

The Director, Organizational Development & Human Resources is responsible for:

- in consultation with the Senior Leadership, developing and maintaining policies in respect of disciplinary actions to be taken for Staff who have been determined to have breached this Policy;
- cooperating with and assisting in Senior Leadership investigations into compliance with this Policy; and
- in consultation with the Senior Leadership, ensuring that disciplinary action for a breach of this Policy or PIPA is carried out in accordance with Foundation Human Resources policies.

2.15.3. Staff

All Staff who have access to Personal Information or Confidential Information are responsible for complying with this Policy and PIPA. Staff are required to:

- ensure that access to and disclosure of Personal Information or Confidential Information is only made by or to authorized individuals;
- ensure that reasonable measures are taken to prevent any unauthorized access, disclosure, loss or theft of information;
- comply with terms of use and security requirements for electronic systems;
- report to the Senior Leadership any actual or suspected breaches of privacy or this Policy and cooperate with the Senior Leadership and Human Resources for the purposes of any investigation.

2.16. Compliance

Failure to comply with this Policy may result in disciplinary action including, but not limited to, the termination of employment, the termination of the contractual agreement, loss of computing privileges, loss of privileges as a student placement or volunteer role, prosecution and restitution for damages.

The Foundation will not take disciplinary action against a Staff member who, acting in good faith and upon a reasonable belief, discloses Personal Information necessary to provide warning or to avert risk where immediate action is required to prevent harm to any person's health or safety.