Information Privacy & Confidentiality

1. Policy Purpose

Vancouver Coastal Health ("VCH") has ethical and legal obligations to protect Personal Information about its Clients and Staff in the custody or control of VCH.

The purpose of this Information Privacy & Confidentiality Policy ("Policy") is to establish the guiding principles and framework by which VCH and its Staff will comply with these obligations, demonstrate accountability for managing Personal Information and maintain its trust-based relationship with Clients, Staff and the public.

2. Policy Statement

2.1 Privacy legislation and Policies

VCH and its Staff are governed by the *B.C. Freedom of Information and Protection of Privacy Act* ("FIPPA"), the *E-Health (Personal Health Information Access and Protection of Privacy) Act* and other legislation, professional codes of ethics and standards of practice.

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

2.2 Governance and Accountability

The Chief Executive Officer of VCH is the appointed 'head' of VCH for the purposes of exercising the powers of the head and ensuring compliance with FIPPA. The governance and accountabilities of operational areas for implementing and complying with FIPPA are set out in Appendix A to this Policy. The Information Privacy Office is responsible for general oversight of privacy practices within VCH, maintenance of breach and compliance policies and provision of privacy education services.

2.3 Obligations of Staff

All Staff who have access to Personal Information are responsible for adhering to this Policy. Members of Staff are required to:

- ensure they are informed about this Policy and proper privacy practices;
- ensure that they comply with this Policy and FIPPA in respect of the collection, access, use, disclosure and disposal of Personal Information;
- seek the advice of the Information Privacy Office in respect of possible violation of this Policy and applicable privacy laws;
- ensure that access to Personal Information or its disclosure is only made to or by authorized individuals;
- ensure that reasonable measures are taken to prevent any unauthorized access, disclosure, loss or theft of information;
- comply with the security requirements developed for use of electronic systems;

- comply with the safe handling of Personal Information requirements set out in Section 5.7 of this Policy; and
- report to the Information Privacy Office any actual or suspected breaches of privacy or this Policy and cooperate with the Information Privacy Office and Employee Engagement for the purposes of any investigation.

Managers shall comply with this Policy and oversee compliance by Staff under their responsibility. The following Sections set out the key privacy obligations of Staff.

Confidentiality Undertakings

As a condition of employment or affiliation, all Staff must sign an approved Confidentiality Undertaking. Personal Information obtained in the course of one's employment or other affiliation with VCH must be held in confidence even after the relationship comes to an end.

2.4 Collection of Personal Information

Authority to Collect Personal Information

Under FIPPA, VCH and its Staff may only collect Personal Information for:

- purposes directly related to and necessary for an operating program or activity of VCH (e.g., the delivery of health care services or for administration or employment purposes);
- law enforcement purposes; or
- as otherwise authorized by law.

VCH may not collect more (in terms of type or amount) Personal Information than is required to fulfill the purposes for which the information is being collected.

Where possible, Staff shall collect Personal Information directly from the individual the information is about.

Informing the Client

Whenever Staff collects Personal Information directly from an individual, the individual should be informed:

- why the information is being collected;
- how it will be used or disclosed by VCH or its Staff;
- the legal authority for the collection; and
- the contact person if the individual has any questions about the collection.

VCH uses the VCH Client Notification Sign and other materials to inform Clients of the above. Notification Signs should be posted at all registration, intake and admission sites in accordance with the Notification Guidelines, including within community centers and clinics.

Indirect Collection

Personal Information should not be collected *indirectly* from other sources unless the individual agrees or there is some other legal authority for indirect collection of the

information. Where it is not possible or practical to collect Personal Information directly from the individual, Staff may only collect Personal Information indirectly from other sources authorized by FIPPA, for example:

- Staff may collect Personal Information from someone other than the Client (i.e. friends, family members) if necessary to provide medical treatment;
- Personal Information necessary for medical treatment may be collected from another Health Authority or other health care providers;
- Personal Information may be collected indirectly for the purposes of law enforcement or if Staff are authorized by other legislation to collect such information;
- Personal Information may be collected indirectly if the individual the information is about consents to such collection.

If a member of Staff has questions or concerns about the use or collection of Personal Information or if a Client expresses concerns, the matter should be referred to the Information Privacy Office.

2.5 Accuracy of Personal Information

VCH must make reasonable efforts to ensure that the Personal Information in its custody or control is accurate and complete. Staff must take all reasonable steps to ensure the accuracy and completeness of any Personal Information VCH collects or records and exercise diligence to protect against errors due to carelessness or oversight.

VCH Health Records is responsible for updating and maintaining the accuracy of health records of Clients. Staff should direct any Clients requesting correction or amendment of information in their medical records to VCH Health Records.

VCH Health Records will review and respond to such requests in accordance with appropriate practices and policies developed by VCH Health Records.

2.6 Use of Personal Information

Staff are only authorized to access and use Personal Information for legitimate purposes based upon a “need to know” in order to perform job functions and responsibilities.

Authorized Purposes

VCH may only use Personal Information for:

- the purpose(s) for which it was originally obtained or compiled by VCH (such as health care delivery or for administration or employment purposes) or for a consistent use;
- any purpose for which the individual has provided express written consent; or
- the purpose(s) for which the information was disclosed to VCH by another public body, such as another health authority.

VCH primarily collects Personal Information about Clients to provide health care services to Clients. Staff may use Personal Information for the provision of care to the Clients and for administrative and other support functions related to direct care.

Secondary Use

Staff may use Personal Information, such as health information, for purposes *related* to the provision of care ("Secondary Purposes") only if the purpose has a *reasonable and direct connection* to the provision of health care services and is required for an operating program of VCH. For example, Staff may use Client Personal Information for the following Secondary Purposes:

- program evaluation and monitoring, including quality improvement;
- system administration;
- privacy and security audits;
- medical education and training related to VCH programs.

Client identifying information is not always required where information is used for Secondary Purposes. As a general rule, Staff should only use Personal Information that is necessary to achieve the Secondary Purposes. Where possible, Personal Identifiers should be removed from records and documents, such as statistical management reports or sample electronic health records used for system usage training.

Research

Staff may only use Personal Information for purposes of research if it directly relates to the research being undertaken and the applicable Research Ethics Board has approved the research project. Staff must also comply with VCH policies and procedures related to research and any conditions attached to Research Ethics Board approval.

Access privileges are only granted to the Principal Investigator and personnel approved by the Research Ethics Board.

2.7 Disclosure of Personal Information

Under FIPPA, disclosure occurs whenever Personal Information is provided to or accessed by someone.

Internal Disclosure or Sharing

Staff may only access Personal Information or disclose Personal Information to other Staff on a "need to know" basis for the purposes of their job functions and responsibilities.

Disclosure to External Parties

VCH may disclose Personal Information to external parties only as permitted by FIPPA. Limited circumstances where VCH is authorized to disclose Personal Information include:

- where required by law (including legislation, court order, subpoena or warrant) to release Personal Information;
- where compelling circumstances exist affecting the health or safety of any individual;

- to protect the public in circumstances where there is a risk of significant harm to the environment or to the health or safety of the public or a group of people; or
- where the individual consents in writing to the information being disclosed.

Specific conditions must be satisfied before Personal Information may be disclosed under these categories. Any questions about whether a proposed or requested disclosure falls under one of these categories should be referred to Legal Services or Risk Management, as appropriate to the circumstances, before Personal Information is disclosed.

Personal Information may also be disclosed for the purposes of a common or integrated program between VCH and another public body or the Ministry of Health and for research purposes where specific legal conditions have been met. Legal Services or the Information Privacy Office must be consulted prior to use or disclosure of Personal Information in these circumstances.

Disclosures Outside of Canada

Staff shall ensure that no Personal Information is accessed, transferred or stored outside of Canada, except with the consent of the individual the information is about or as otherwise permitted by FIPPA, such as to collect a debt owing to VCH or to contact an individual's next of kin in an emergency. FIPPA generally only permits the transfer, storage of or access to Personal Information from outside Canada on a temporary basis, such as when members of Staff are traveling temporarily outside Canada. The Information Privacy Office must be consulted before any program is implemented in which Personal Information will be transferred, stored or accessed from outside of Canada.

Requirements for Accessing or Sharing Personal Information with any Third Parties

All third parties, whether a third party vendor, contractor, agency or other organization, accessing or sharing Personal Information in the custody or control of VCH must execute an Information Access Agreement, Information Sharing Agreement or agree to the terms of the VCH Privacy Schedule. Legal Services must approve the form and content of any Information Access Agreement, Information Sharing Agreement or Privacy Schedule.

Staff should take all reasonable steps to ensure no unauthorized personnel or third parties are provided with access to records containing Personal Information, except as permitted under this Policy and FIPPA. Any third party who requests access should be asked to produce identification, and confirmation that they have signed an agreement in accordance with this Policy.

Release of Information Requests

Staff shall comply with all policies, procedures and guidelines for the release of Personal Information. VCH Health Records generally administers requests to disclose Personal Information for provision of care purposes to other hospitals, primary care physicians and other care providers, if they require the information to provide health care services to the individual the information is about. Health Records also deals with Client requests or Staff requests for release of their own clinical health information records.

Staff who receive a demand, order, subpoena or request for the release of information in the possession of VCH from any court, government or other authority must immediately report the request to their manager, who shall consult with Health Records or Legal Services, and if the information relates to non-health records, with the FOI Department.

Research

The disclosure of Personal Information in the custody or control of VCH for research purposes must only be done in accordance with section 35 of FIPPA and if the project is approved by the Research Ethics Board. Wherever possible, Personal Identifiers should be removed from health information before it is disclosed and used for research purposes.

Access to Personal Information on VCH clinical systems for research purposes must adhere to applicable system access requirements, policies and procedures.

2.8 Safeguards

VCH must take "reasonable security precautions" to protect Personal Information in its custody or control 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. The safeguards and measures of protection must include (a) physical measures, (b) organizational measures, and (c) technological measures.

Physical Measures and Safeguards

Staff must protect Personal Information from unauthorized access, modification, disclosure and theft. Printed records and files containing Personal Information must be kept in a secure location, and may not be left unattended in areas vulnerable to unauthorized viewing or theft. Mobile electronic devices and storage media containing Personal Information must also be protected against theft and unauthorized access.

Examples of physical safeguards include:

- storing records containing Personal Information in locked storage rooms or locked filing cabinets, with controls over distribution of keys or lock combinations
- use of numbers or other methods to label file drawers, records storage boxes and other storage containers so as not to reveal the fact that they contain Personal Information
- restricted access to offices and data centers
- data destruction standards and procedures

Organizational Measures and Safeguards

VCH must develop and maintain appropriate procedures and management structures to ensure access to Personal Information is authorized and based on an individual's "need to know" in order to perform their job responsibilities.

Examples of procedural safeguards include:

- Appropriate management authorization is required before any user is granted access to VCH systems containing Personal Information

- Procedures to limit third party access to Personal Information to what is required, and for the shortest duration of time possible
- Where contracted services are used for storage, transportation or destruction of records, including security provisions in the service contract, contractors are required to provide a certificate of destruction.

Technical Measures and Safeguards

VCH shall ensure that VCH information systems containing Personal Information have appropriate technical and system access controls to ensure the confidentiality of Personal Information. All systems containing Personal Information must meet security standards and procedures developed by IMIS. VCH shall take all reasonable steps to implement such safeguards for all legacy systems.

Examples of technical safeguards include:

- Access controls on computer systems (i.e., passwords that allow different levels of access to various screens and differing capabilities to read, extract or change data)
- Hard disk encryption to prevent unauthorized access or disclosure of personal information stored on mobile devices

Information System Access Management and Controls

To prevent unauthorized access, modification or disclosure of Personal Information, VCH shall ensure that VCH information systems containing Personal Information have the following access management structures, policies and procedures in place:

- documented governance structure to ensure that all access to information complies with the principle of "need to know" and this Policy;
- documented policies governing decisions for the assignment of access privileges;
- documented procedures for provisioning user accounts, including appropriate authentication, authorization and assignment of access privileges;
- documented procedures for ensuring that access privileges are maintained and updated on a regular basis in accordance with an assessment of "need to know"; and
- documented procedures for de-provisioning user accounts, including a systematic, repeatable method of identifying users whose system access is no longer required and for deactivating or disabling their accounts or privileges.

VCHA shall take all reasonable steps to implement the same requirements for current legacy systems.

2.9 Privacy Impact Assessment

A Privacy Impact Assessment ("PIA") must 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, VCH departments must contact the Information Privacy Office to determine whether a Privacy Impact Assessment is required. Completion of a Privacy Impact Assessment is the responsibility of the department responsible for the new service or delivery, with support from the Information Privacy Office.

2.10 Privacy Training

VCH shall, 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. VCH will develop privacy awareness and training programs to educate all Staff and users of Personal Information about VCH's privacy obligations. Privacy education programs will be developed through the Information Privacy Office in conjunction with Employee Engagement and other operational areas to meet compliance requirements.

2.11 Obligation to Report Foreign Demand

VCH must report foreign demands for the disclosure of Personal Information to the Minister of Labour and Citizens' Services in accordance with FIPPA. "Foreign demands" include subpoenas, warrants, orders or requests from foreign courts or foreign government agencies.

Staff who receive or learn of a foreign demand or about the unauthorized disclosure of Personal Information in response to a foreign demand should report it to Legal Services.

2.12 Retention of Personal Information

FIPPA provides that Personal Information in the custody or control of VCH that is used to make a decision that directly affects the individual the information is about must be retained for a minimum of one year from the time that it is used to make the decision. However, currently VCH retains health records for longer periods to meet the requirements of the *Hospital Act* and Ministry of Health directives that have mandated indefinite retention for some records.

Staff and their respective departments are responsible for adhering to regional or departmental policies on the retention of records containing non-health-related Personal Information. Generally, Personal Information should not be retained any longer than is necessary to achieve the original purpose(s) for its collection.

2.13 Openness

VCH will make available, directly to Clients, Staff and the public, specific information about its policies and practices related to the management of Personal Information. VCH will make information about its policies and practices easy to understand, including provision of the title and address of the individual or individuals accountable for VCH compliance with this Policy, to whom inquiries or complaints may be directed and how to access to Personal Information held by VCH.

2.14 Whistle-blower Protection

VCH 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 Minister of Labour and Citizens' Services about a foreign demand for Personal Information;
- disclose to the BC Office of the Information and Privacy Commissioner that VCH or another individual has contravened FIPPA;
- do something required to avoid contravention of FIPPA or refuse to contravene FIPPA; or
- inform VCH about a breach of or violation of this Policy.

2.15 Challenging Compliance

VCH will maintain procedures for addressing and responding to all inquiries or complaints from Clients and Staff about its handling of Personal Information and will inform its Clients and Staff about the existence of these procedures.

Any individual will be able to challenge compliance with this Policy with the Information Privacy Office, which will ensure the issue is properly discussed, documented and addressed as quickly as possible.

Any individual accountable for compliance with this Policy may seek external advice where appropriate in order to provide a final response to complaints. VCH will investigate all complaints concerning compliance with this Policy, and, if a complaint is found to be justified, appropriate measures will be taken, including amending policies and procedures where required. The complainant will be informed of the outcome of the investigation regarding the complaint.

2.16 Breach of Policy

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

Staff are expected to report any actual or suspected breaches of privacy or violations of this Policy in connection with any VCH program or activity in accordance with VCH Staff Guidelines on Handling Privacy Breaches.

2.17 *E-Health (Personal Health Information Access and Protection of Privacy) Act*

VCH shall comply with all requirements of the *E-Health (Personal Health Information Access and Protection of Privacy) Act* and any ministerial orders published in respect of a designated health information bank ("HIB") in the custody or control of VCH and in respect of the collection into and use or disclosure of Personal Information in respect of an HIB in the custody or control of a Ministry or other health care bodies as defined in that Act. Staff shall also comply with VCH policies and procedures applicable to HIBs to which Staff may have access or into which Staff may disclose Personal Information.

2.18 Audit and Compliance Programs

The Information Privacy Office will investigate suspected breaches of this Policy. The Information Privacy Office and Legal Services, Employee Engagement, Managers and/or other VCH stakeholders will determine follow-up action according to the nature of the breach and parties involved.

VCH operational areas and programs must conduct appropriate reviews and audits of their systems and processes to ensure compliance in accordance with VCH policies and standards. All incidents involving theft or loss of Personal Information must be reported immediately to the Information Privacy Office, which will take steps to contain the breach, investigate and report it and advise on remedial action.

3. Policy Scope

This Policy applies to all Staff and all Personal Information regardless of format and how it is stored or recorded.

4. Policy Principles

VCH and its Staff are governed by the BC *Freedom of Information and Protection of Privacy Act* ("FIPPA"), the Health Act and other legislation, professional codes of ethics and standards of practice. VCH is committed to ensuring that personal privacy rights are respected and to maintaining a trust-based relationship with its Clients.

5. Procedures

5.1 General Inquiries

Any questions or concerns about collection, access, use or disclosure of Personal Information, reports of privacy breaches or loss of information, or the VCH privacy program should be directed to the Information Privacy Office at privacy@vch.ca.

5.2 Complaints

Clients or other members of the public who complain about a breach of their personal privacy should be directed to the Information Privacy Office at privacy@vch.ca or the VCH Client Relations department.

Any questions or concerns about the release of clinical information should be directed to VCH Health Records. Any questions or concerns for all other release of information should be directed to the FOI Department at foi@vch.ca.

5.3 Research

Requests by researchers should be directed to the Vancouver Coastal Health Research Institute.

5.4 Employee Information

Requests for employee information from legal firms, financial institutions, insurance companies, credit bureaus and police, etc. should be directed to Employee Engagement/Payroll Departments. This information may be provided upon receipt of the employee's written authorization, but the Employee Engagement/Payroll Departments may confirm dates of employment without written authorization.

5.5 Confidentiality Undertakings

The responsibilities for obtaining and holding Confidentiality Undertakings for all new Staff are as follows:

- Volunteers – Volunteer Office
- Students and Employees – Employee Engagement
- Contractors & Vendors – departments responsible for the contracted services
- Medical staff – Medical Affairs
- Research – VCH Research Institute

5.6 Requests for Information

Requests for information are to be directed to the appropriate department or agency:

- Media – Communications & Public Affairs
- Research – VCH Research Institute
- Clinical records – Health Records
- Non-clinical and corporate information – FOI Department
- Personnel information – Employee Engagement.
- Medical staff information – Medical Affairs
- Litigation or other legal documents – Legal Services or Risk Management

5.7 Safe Information Handling

Members of Staff are expected to comply with VCH security requirements developed for use of electronic systems. Staff 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
- using encryption or password protection to protect Personal Information

Staff shall ensure that access or disclosure is only made to or by authorized individuals, and that reasonable measures are taken to prevent any unauthorized access, disclosure, loss or theft of information, including:

- keeping hard copies of files and records containing Personal Information in a secure location, preferably where locked and secure against theft 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 in public areas where third parties may overhear or view records containing Personal Information;
- prohibiting removal of records containing Personal Information from VCH 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;
- immediately reporting to the Information Privacy Office any theft, loss or attempted theft of Personal Information or devices on which Personal Information may be stored;
- following VCH guidelines and procedures for the secure destruction or disposal of Personal Information that is no longer required to ensure the Personal Information is destroyed, erased or made anonymous.

6. Exceptions

There are no exceptions to this Policy.

7. Internal Tools, Forms and References

Internal Forms related to this Policy include the following:

- Confidentiality Undertaking (various forms)
- Privacy Impact Assessment
- Information Privacy Investigation Report
- Information Access Agreement
- Information Sharing Agreement
- Privacy Schedule
- Release of Information Request Forms

Refer to the VCH intranet or contact the Information Privacy Office for the latest versions of these documents.

References related to this Policy include the following:

- Memo to Staff: Faxing Personal Information
- Memo to Staff: Protecting Personal Information
- Memo to Staff: Internal Use of Email
- Memo to Staff: Protecting Personal Information Outside the Office
- Memo to Staff: Privacy in Emergency or Urgent Situations
- Need to Know Access for Staff
- Staff Brochure: Access to Clinical Information Systems
- Staff Brochure: Protecting Client Information

- Privacy Obligations and VCH Staff – Frequently Asked Questions

Refer to the VCH intranet or contact the Information Privacy Office for the latest versions of these documents.

8. Related Policies

Related VCH Policies include the following:

- Reporting Theft or Loss of Information or Information Storage Devices
- Release of Patient or Client Personal Information and Personal Belongings to Police and other Agencies
- Management of Information Privacy Incidents

For more information, refer to the VCH intranet or consult the Information Privacy Office.

9. Definitions

"Clients" means all people receiving services from VCH and includes patients and residents.

"Confidentiality" means organization's obligation to ensure that Personal Information is only accessible to those who are authorized to have access.

"FIPPA" means the BC *Freedom of Information and Protection of Privacy Act*, as amended from time to time.

"IMIS" means the Information Management Information Systems department of VCH.

"Personal Identifiers" means any recorded information that could, either by itself or in combination with other information, be used to link or associate Personal Information to a particular individual (including but not limited to name, birth date, photograph, PHN, MRN, home address, postal code, personal telephone number, social insurance number (SIN), driver's license number, employee ID number, and other identity numbers).

"Personal Information" means any information about an identifiable individual (including, but not limited to patients, clients, residents, volunteers, students, staff, physicians or members of the public), but it does not include business contact information (business contact information is information such as an individual's title, business telephone number, business address, email or facsimile number).

"Information Privacy" means the right of an individual to have some control over who has access to his or her Personal Information and under what circumstances.

"Privacy Impact Assessment" means the process to determine whether new systems, programs, initiatives, strategies or proposals meet the privacy and security requirements of the B.C. *Freedom of Information and Protection of Information Act*, other regulatory requirements and VCH policies and principles for information privacy and confidentiality.

"Reasonable security precautions" are those that a fair, rational person would think were appropriate to the sensitivity of the information and to the medium in which it is stored, transmitted, handled, or

transferred. A sliding scale of security arrangements is appropriate, depending on the sensitivity of the personal information that an organization handles.

"Staff" means all officers, directors, employees, contractors, physicians, health care professionals, students and volunteers engaged by VCH.

"VCH" means Vancouver Coastal Health Authority.

10. External References

- *B.C. Freedom of Information and Protection of Privacy Act*
- *E-Health (Personal Health Information Access and Protection of Privacy) Act*
- *Health Act*
- Office of the Information and Privacy Commissioner for British Columbia

In original copy:

Issued by:

Name: Duncan Campbell Title: CFO & VP Systems Development & Performance Date: Sept. 11, 2008

Appendix A

VCH Legal Services and the Information Privacy Office are responsible for:

1. maintaining and administering this Policy;
2. providing privacy support services and general oversight of privacy practices within VCH, including in respect of electronic health care systems, to enable compliance with FIPPA;
3. promoting good privacy practices throughout the organization, including legal services, education programs, policies and compliance tools;
4. investigating potential and actual privacy breaches brought to its attention and reporting breaches in accordance with VCH breach policies; and
5. maintaining reactive and proactive privacy audit programs for core electronic health records systems in accordance with VCH audit policies.

Information Management/Information Systems (IMIS) is responsible for:

1. development of appropriate access policies that govern access to Personal Information contained in or made accessible through VCH information systems, consulting as appropriate with the Information Privacy Office; and
2. ensuring that access controls and security measures for VCH information systems reflect organizational policies governing access to Personal Information and meet statutory requirements for the protection of Personal Information against unauthorized access, collection, use, disclosure and disposal.

Health Records is responsible for:

1. administering health information access requests in accordance with FIPPA; and
2. development of consistent policies and procedures for the administration of VCH health records.

Freedom of Information Department is responsible for:

1. receiving and responding to requests for corporate and other non-clinical information, in accordance with Part 2 of FIPPA, including ensuring that public records are not disclosed in a manner that results in an unreasonable invasion of a third party's personal privacy.

Employee Engagement is responsible for:

1. assisting with investigations into potential privacy breaches;
2. developing and maintaining policies in respect of disciplinary actions to be taken for Staff who have been determined to have committed a privacy breach;

3. ensuring that disciplinary action for privacy breaches is carried out in accordance with Employee Engagement policies;

4. administering requests for employee Personal Information.

The VCH Research Institute is responsible for:

1. establishing guidelines, in consultation with the Information Privacy Office, for use of Personal Information for the Secondary Purpose of research; and

2. in conjunction with the Information Privacy Office and Research Ethics Board, ensuring compliance with such guidelines.