Information Privacy & Confidentiality

1. Introduction

Description

Vancouver Coastal Health Authority ("VCH") has ethical and legal obligations to protect Personal Information about its Clients and Staff. VCH 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 VCH and its Staff will comply with these obligations, demonstrate accountability for managing Personal Information and Confidential Information and maintain its trust-based relationship with Clients, Staff, business and healthcare partners (including Lower Mainland Consolidation parties) and the public.

Scope

This Policy applies to all Staff and all Personal Information and Confidential Information in the custody or control of VCH regardless of format and how it is stored or recorded.

2. Policy

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.

VCH will comply with FIPPA when collecting, using and disclosing Personal Information.

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 VCH and its Staff comes to an end.

2.2. Confidentiality Undertaking

All Staff must complete the VCH Confidentiality Undertaking and Information Privacy Online course as required by the *Mandatory Education* Policy.

2.3. Collection of Personal Information

Staff may collect Personal Information as needed to operate VCH programs or activities and will not collect more Personal Information than is required to fulfill those purposes.

2.4. Direct Collection

Where possible, VCH 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;
- 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, including community centers and clinics.

2.5. Indirect Collection

Staff may collect Personal Information indirectly (from sources other than the Client):

- with the consent of the Client;
- where the information is required to provide health care and it is not possible to collect the information directly from the Client (Client consent is not required);
- where another public body is authorized to disclose the information to VCH; or
- as otherwise permitted by FIPPA

For example, where the Client is incapable of providing information or does not have the information, Staff may collect Personal Information necessary to provide care from another Health Authority, other health care providers, family members or friends.

2.6. Accuracy of Personal Information

VCH and its Staff will take all reasonable steps to ensure the accuracy and completeness of any Personal Information VCH collects or records. Staff will exercise diligence to protect against errors due to carelessness or oversight.

Health Information Management (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 Health Information Management.

2.7. Use of Personal Information

Staff may only access and use Personal Information for legitimate purposes based on a "need to know" in order to perform job functions and responsibilities.

Primary Use

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 Clients and for administrative and other support functions related to direct care.

Secondary Use

Staff may use Personal 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 planning, evaluation and monitoring, including quality improvement;
- system administration;
- privacy and security audits;
- medical education and training related to VCH programs;
- analysis, management and control of disease outbreaks and population health; and
- as otherwise authorized by FIPPA.

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 (eg. name, birth date, photograph, PHN, MRN, home address, postal code, personal telephone number, social insurance number, driver's license number, employee ID number, and other identity numbers) 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 use Personal Information for research only in compliance with VCH policies and procedures related to research, including approval from the VCH Research Institute and the Information Privacy Office, and any Research Ethics Board conditions.

2.8. Disclosure of Personal Information

Set out below are examples where Personal Information may be disclosed. Staff may consult with the Information Privacy Office for questions about disclosure.

Disclosure for Continuity of Care

Staff may disclose Personal Information on a "need-to-know" basis to other health care providers or members of the care team, both within and outside VCH, including to family members who are providing care (i.e., within the "circle of care" or for "continuity of care"). Disclosures within the circle of care do not require consent, although Staff may wish to discuss such disclosures with the Client.

Disclosure for Safety Purposes

Staff may, without requiring Client consent, disclose Personal Information necessary to provide warning or to avert the risk:

- where compelling circumstances exist that affect the health or safety any person;

- 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
- to reduce the risk that anyone will be a victim of domestic violence, if Staff believe that domestic violence is reasonably likely to occur.

Staff should seek approval from a Staff member in charge, supervisor or manager. If in doubt Staff should consult with the Information Privacy Office or Client Relations and Risk Management in deciding whether to disclose information. Examples of compelling circumstances include:

- an intent expressed by the Client, which Staff believe, to cause serious harm to self or others, such as specific threats of assault or death; and
- a Client who is incapable of driving and indicates intention to drive.

Good-faith decision-making

VCH will not dismiss, suspend, demote, discipline or otherwise disadvantage 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.

Disclosure to Law Enforcement

For disclosures of Personal Information to law enforcement (e.g., mandatory demands such as court orders or search warrants, requests by law enforcement, or VCH-initiated reporting to law enforcement) see the *Release of Information or Belongings to Law Enforcement* Policy.

Disclosure with Consent

Besides the disclosures described above and other disclosures authorized by FIPPA, Staff may disclose Personal Information with Client consent. Client consent should be in writing or may be documented by Staff on the health record.

Disclosures Outside of Canada

Staff will not access, transfer or store Personal Information outside of Canada, except with the consent of the individual the information is about or as otherwise permitted by FIPPA (eg. while temporarily travelling outside Canada, or temporary access for systems support). Staff will consult the Information Privacy Office before implementing a program where Personal Information will be transferred, stored or accessed from outside of Canada.

Obligation to Report Foreign Demand

Staff who receive or learn of a foreign demand for the disclosure of Personal Information or about the unauthorized disclosure of Personal Information in response to a foreign demand must report it to Legal Services. "Foreign demands" include subpoenas, warrants, orders or requests from courts or agencies outside Canada.

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 Legal Services or the Information Privacy Office to determine what documentation is required. Examples where legal documentation may be required are as follows:

- access by a third party organization to VCH clinical information systems
- services provided by a vendor who will have access to Personal Information
- program that requires Personal Information to be shared with another agency

Personal Information may be disclosed to third parties for research only in compliance with VCH policies and procedures related to research, including approval from the VCH Research Institute and the Information Privacy Office, the requirement to sign an Information Sharing Agreement and Research Ethics Board approval.

Release of Information Requests

Health Records: Staff may provide Client with a copy of a document if it was completed with the Client present (e.g. client assessment, care plan). Staff may also provide Client with a copy of a single lab or radiology report if they request. If Client requests a copy of their entire health record or health records narrative in nature (e.g. progress notes, transcribed reports), please direct the request to Health Information Management (Health Records Department).

Corporate/Non-Health Records: Refer requests to the Freedom of Information Office.

Employee Information

Requests for employee information from legal firms, financial institutions, insurance companies, credit bureaus, etc. should be directed to Employee Engagement/Payroll.

2.9. Safeguards

VCH 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 VCH 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 VCH 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;
- prohibiting removal of records containing Personal Information or Confidential 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.

Technical Measures and Safeguards

Staff will comply with VCH 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;
- using encryption and password protection for mobile electronic devices and storage media.

2.10. 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 PIA is required. Completion of a PIA is the responsibility of the department undertaking the program or activity, with support from the Information Privacy Office.

2.11. Privacy Training

VCH 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 Information Privacy Office will develop privacy education programs in conjunction with Employee Engagement and other operational areas to educate all Staff and users of Personal Information about VCH's privacy obligations.

2.12. Retention of Personal Information

VCH 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. Currently, VCH retains health records for longer periods to comply with Ministry of Health directives.

Staff and their respective departments must adhere to regional or departmental policies on the retention of records containing non-health-related Personal Information.

2.13. Whistleblower 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 appropriate authority 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.

2.14. Challenging Compliance

The Information Privacy Office 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.

2.15. Reporting Privacy Breaches

Staff must immediately report to the Information Privacy Office 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 *Reporting and Management of Information Privacy Breaches* Policy.

2.16. Responsibilities

2.16.1. Chief Executive Officer / Senior Executive Team / Chief Privacy Officer

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 authority of the head is delegated to the members of the Senior Executive Team and to the Chief Privacy Officer.

2.16.2. Information Privacy Office / Legal Services

The Information Privacy Office / Legal Services is responsible for:

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

2.16.3. Employee Engagement

Employee Engagement is responsible for:

- in consultation with the Information Privacy Office, 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 Information Privacy Office investigations into compliance with this Policy; and
- in consultation with the Information Privacy Office, ensuring that disciplinary action for a breach of this Policy or FIPPA is carried out in accordance with Employee Engagement policies.

2.16.4. Staff

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

2.17. 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.

VCH 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.

3. References

Tools, Forms and Guidelines

The Information Privacy Office webpage has a complete list of privacy-related policies, tools, forms and guidelines.

Keywords

Privacy, Breach, Confidentiality, Personal Information, Confidential Information, Freedom of Information and Protection of Privacy Act, FIPPA, Security, Lower Mainland Consolidation

Definitions

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

"**Confidential Information**" means all information, other than Personal 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 VCH or through other Lower Mainland Consolidation parties, including vendor contracts and other proprietary information that a Lower Mainland Consolidation party may have received from a third party.

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

"**Lower Mainland Consolidation**" means the consolidation of certain corporate and clinical support functions amongst Vancouver Coastal Health Authority, Fraser Health Authority, Provincial Health Services Authority and Providence Health Care Society as more fully set out in a Master Services Agreement amongst the parties dated January 1, 2011.

"**Personal Information**" means any information about an identifiable individual, but does not include business contact information (eg. individual's title, business telephone number, business address, business email or facsimile number).

"**Staff**" means all employees (including management and leadership), Medical Staff Members (including physicians, midwives, dentists and Nurse Practitioners), residents, fellows and trainees, health care professionals, students, volunteers, contractors and other service providers engaged by VCH.

Questions

Contact: Information Privacy Office at privacy@vch.ca

Issued by:

Name: **Glen Copping** Title: CFO & VP, Systems Development & Performance Date: March 7, 2014

Signature of issuing official