



## 1.0 General Administrative

### 1.5 Legal/Ethical

#### 1.5.2 Confidential Information – Third Party, VIHA Business and Other Non-Personal Information Policy

### 1.0 Introduction/Purpose

The Vancouver Island Health Authority (VIHA) is responsible to protect business information under its custody and control, which, if disclosed, would harm the business interests of VIHA and/or a third party.

Business information may exist in an aggregated form relating to several third parties. VIHA also holds business information that directly relates to VIHA activities and not specifically attached to a third party business (e.g. Draft Service Plans; Draft Communication Plans etc). In all circumstances, VIHA values business information as an asset that must be created, collected, used, protected and disclosed in accordance with supporting legislation and/or policies (e.g. Freedom of Information and Protection of Privacy Act (FOIPPA); VIHA Policies and Procedures).

The purpose of this policy is to provide a framework for the consistent management of third party and VIHA business information created, collected, used, disclosed and protected by the VIHA in accordance with the principles and requirements of various legislative and common law rules, including but not limited to the Evidence Act, Ombudsman Act, Workers Compensation Act, FOIPPA of BC and various professional bylaws (e.g. medical practitioner bylaws), Codes of Ethics and Standards of Practice. **This policy incorporates but does not go beyond the existing requirements for confidentiality under the Freedom of Information and Protection of Privacy Act.**

## 2.0 Policy

### 2.1 Responsibility for Confidentiality

Business information obtained in the course of an agent's affiliation with VIHA must be held in confidence. All reasonable measures must be taken to ensure that business information is collected, used and disclosed only in circumstances necessary and authorized in the conduct of the business of the organization and in accordance with the appropriate legislative authority (e.g. FOIPPA) and/or VIHA policy.

Intentionally viewing confidential information that is not necessary to perform an individual's role is considered a breach of confidentiality even if that information is not disclosed to another party. Confidential information must not be discussed in any physical location where others, not entitled to receive that information, are present and likely to overhear, unless required to fulfil one's professional role, by law or with permission from an authorized individual.

Third party and organizational business information may be subject to copyright. Section 27(2)(i) and 27(2)(j) of the Copyright Act (R.S.C. 1985) c.C-42 set out actions that do not constitute an infringement of copyright. In some cases, disclosure of copyrighted records may cause financial harm to third parties, the public body or the government as a whole.

Some information may be protected by statute (e.g., Evidence Act) while other information may be confidential due to the nature of the relationship between VIHA and the provider of the information and the circumstances of the communication (for example, witness statements in an investigation are protected). Confidential information may also include third parties (e.g. contractors) who have supplied information about private sector enterprises to VIHA or information regarding internal organizational business plans (e.g. in camera meeting of a Health Board). Business information that was supplied in confidence\*\*, that would reveal third party trade secrets, commercial, financial, labour relations, scientific or technical information must be kept confidential and should not be disclosed without consent of the third party or by a legislative requirement (e.g. FOIPPA). In addition, organizational business information that would harm VIHA's financial interests and/or relates to the management of VIHA that has not yet been implemented or made public will not be disclosed without the proper legislative authority (e.g. FOIPPA).

\*\*This policy does not override the provisions of section 21 of the FOIPPA.

## **2.2 Access to Confidential Business Information**

Individuals may formally request access to business information of either a third party and/or VIHA by submitting a written request to the Regional Office, Information and Privacy. All business information will be reviewed subject to the provisions of the Freedom of Information and Protection of Privacy Act.

## **2.3 Confidentiality Acknowledgement**

A signed Confidentiality Acknowledgement is a requirement of employment for all VIHA employees and for the establishment of a relationship between the VIHA and all designated VIHA agents.

All VIHA employees and designated VIHA agents are required to be familiar with and abide by the Confidential Information - Third Party, VIHA Business and Other Non-Personal Information Policy during the course of their involvement with the VIHA.

## **2.4 Breach of Confidentiality**

Individuals will be held accountable for breaches of confidentiality.

Breaches of confidentiality include intentional and unauthorized access to, use and/or disclosure of, confidential information.

All VIHA employees and designated VIHA agents have a responsibility to report breaches of confidentiality without fear of reprisal.

If it is established that a breach of confidentiality has occurred, those individuals deemed responsible may be subject to penalty or sanction up to and including termination of employment, cancellation of contract or services, termination of the relationship with VIHA, withdrawal of privileges and/or legal action.

## **2.5 Reviews**

Reviews may be performed to ensure compliance to this policy. With respect to electronic records, automated audit systems have the capability to monitor and record all access made to documents performed by an employee or agent of the VIHA. The frequency of audits and designation of individuals or system auditor(s) will be the responsibility of the program or area manager. Involvement of Information systems personnel, consultative bodies and other specifics of the review process are the responsibility of each program area.

## **3.0 Scope**

This policy applies to:

1. All VIHA employees.
2. All designated VIHA agents.
3. Any individual either directly or indirectly associated with the VIHA.
4. Business information in any format including, but not limited to, paper, electronic, film, verbal discourse.
5. Information as noted in #4 that is provided to, obtained from, or as a result of a relationship with the VIHA, regardless of where that information may be subsequently stored or used.

All such information in the custody and control of the VIHA is covered by this policy and the associated legislative and common law rules.

Research shown to be conducted by a VIHA employee and/or designated agent under the auspices of VIHA's affiliation with a post-secondary educational body is outside the scope of the FOIPPA as per s. 3(1)(e).

#### 4.0 Examples of Breaches (What you should NOT do)

These are examples only. They do not include all possible breaches of confidentiality covered by the Confidential Information - Third Party, VIHA Business and Other Non-Personal Information Policy and the Confidentiality agreement.

<p><b>Accessing and/or using information that you do not need to do your job:</b></p> <ul style="list-style-type: none"><li>• Unauthorized reading of business information pertaining to a third party</li><li>• Showing, telling, copying, selling, changing, or disposing of confidential information that is not pertinent to your role or care activity.</li><li>• Showing telling, copying, selling, changing or disclosing confidential third party or VIHA business information to another third party</li><li>• Showing, copying, selling, changing, disclosing or disposing of confidential VIHA business without proper authority</li><li>• Discussing confidential information in a public area such as a waiting room or elevator.</li></ul>	<p><b>Providing or gaining unauthorized access to physical locations (e.g. file cabinets) which contain confidential information</b></p> <ul style="list-style-type: none"><li>• Lending out your keys to an unauthorized person to access file cabinets, file storage areas or other areas where confidential information is stored, OR using another's keys for the same purpose</li><li>• Leaving file storage areas unlocked when they should be locked.</li></ul> <p><b>Failing to report a breach of confidentiality</b></p> <ul style="list-style-type: none"><li>• Being aware of a breach of confidentiality, but not reporting the breach to your supervisor or other designated individual.</li><li>• Not reporting that your password to a computer system has been compromised or that you have lost keys to a storage location for confidential information.</li></ul>
--	--

## 5.0 Definitions

### Confidential Business Information

Business information is information provided to, collected or created by the VIHA that exists regardless of form and includes, but is not limited to the following:

- Information provided to VIHA by an external vendor which, if disclosed would harm the business interests of the external vendor (e.g. Proposal documents, contracts, unit prices, vendor proprietary advice or information, vendor proprietary technology).
- Information (staff statements, legal advice, investigators' reports, incident reports) prepared as part of a pending or ongoing litigation, law enforcement investigation, quality assurance review, Workers Compensation Board or Ombudsman investigation.
- Information related to credentialing, discipline, privilege, quality assurance reviews and external review of quality of care. Note that both business and personal information may be found within these records.
- In camera deliberations of VIHA where such topics as personnel, labour relations, land acquisitions or litigation may be discussed,
- Unpublished statistical information and internal correspondence related to organizational initiatives.
- Information supplied in confidence to a mediator or arbitrator to resolve or investigate a labour relations dispute.

### Confidentiality

Confidentiality refers to the responsibility or obligation of an individual or organization to ensure that third party and VIHA business information is kept secure and is created, collected, accessed, used and disclosed appropriately.

### Other Related Definitions

**“Commercial”** – means concerning the sale, purchase or exchange of goods or services. This includes information that is, in itself, a commercial product.

**“Labour Relations”** – information relates to the management of a third party's personnel, whether or not the personnel are organized into bargaining units.

**“Scientific”** – means according to rules laid down in exact science for performing observations and testing the soundness of conclusions; systematic, accurate; used in, engaged in, or relating to science (OED 9<sup>th</sup>)

**“Supplied in confidence”** - applies to information that one person provides or furnishes voluntarily or by law and entrusts to another in circumstances where there is an implicit or explicit expectation that confidentiality will be maintained and the public body will not disclose. It would also include information provided orally and recorded by an employee of the public body. Information created by a public body about a third party is not “supplied”

(for example, supplied information that is changed as a result of subsequent negotiations may not be considered “supplied in confidence”). \*\*

**“Technical information”** – means information relating to a particular subject, craft or profession or its techniques.

**“Third party”** – in relation to a request for access to a record, means any person, group of persons or organization other than the person who made the request or a public body.

**“Trade secret”** – information including a formula, pattern, compilation, program, device, product, method, technique or process that is used, or may be used, in business for any commercial advantage; derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure and/or which would result in harm or improper benefit.

\*\*This policy does not override the provisions of section 21 of the FOIPPA.

### **Designated VIHA Agents**

Designated VIHA agents are individuals or organizations who have a business relationship with the VIHA and, at the discretion of the VIHA, are deemed to have the potential to access, intentionally or inadvertently, all forms of VIHA confidential information by virtue of their relationship to the VIHA.

Examples of designated VIHA agents may include, but are not limited to: Physicians, other health care providers, researchers, volunteers, students, contractors, sub-contractors, vendors/suppliers or any individual directly/indirectly associated with the VIHA.

### **Authorized Individual**

An individual who has the authority under law or policy to access specific forms of confidential information.

### **Supporting and Related Policies and Procedures**

- Freedom of Information and Protection of Privacy Act, S.B.C. 1992, Chapter 61, as amended by S.B.C. 1993, Chapter 46.
- Policy 1.5.1 Confidential Information - Privacy Rights of Personal Information
- Freedom of Information Policy and Procedures Manual - section 17  
[http://www.mser.gov.bc.ca/foi\\_pop/manual/toc.htm](http://www.mser.gov.bc.ca/foi_pop/manual/toc.htm)
- Freedom of Information Policy and Procedures Manual – section 21  
[http://www.mser.gov.bc.ca/foi\\_pop/manual/toc.htm](http://www.mser.gov.bc.ca/foi_pop/manual/toc.htm)
- Workers Compensation Act
- Ombudsman Act
- Evidence Act (in particular s.51)