



## **16.0 Information Management**

### **16.4 Organization and Security**

#### **16.4.2 Protection**

##### **16.4.2.1 Security of Electronic Information**

### **1.0 Introduction**

In order to fulfill its mission Vancouver Island Health Authority (VIHA) is committed to providing secure yet open electronic information access that protects the integrity and confidentiality of patient information while maintaining the accessibility required to optimize care delivery.

### **2.0 Purpose**

The purpose of this policy is to identify and communicate VIHA principles and legal obligations to guide organizational actions enabling the protection of Information.

### **3.0 Policy Statement**

VIHA is responsible for protecting the privacy, confidentiality and security of Information within its custody and/or control of accordance with the Freedom of Information and Protection of Privacy Act, industry security best practices, and standards, specifically Standard ISO/IEC 27002:2005 Information Technology – Code of Practice for Information Security Management (see [https://intranet.viha.ca/departments/imit/servicedesk/Documents/ServiceSupport/iso\\_27002.pdf](https://intranet.viha.ca/departments/imit/servicedesk/Documents/ServiceSupport/iso_27002.pdf)). VIHA is also responsible for establishing reasonable controls to mitigate the risk of unauthorized access, use of disclosure of Information and for ensuring Information is available to authorized individuals.

Access to VIHA Information must be controlled and only granted to authorized users on a need to know basis in accordance with established privacy and security best practices and procedures related to the policy. The level of control will depend on the classification of the Information and the level of risk related to loss or compromise. These controls may range in scope and complexity from extensive security installations to protect a server room, to simple measures taken to prevent unauthorized viewing of patient Information on computer monitor.

The VIHA Chief Information Officer has the delegated responsibility of establishing the required policies, standards and procedures to ensure VIHA Information is protected, available, and managed in compliance with legislation.

All Information users will receive education on the expectations, knowledge and skills related to fulfilling their responsibilities under this policy.

#### **4.0 Applies To:**

This policy applies to all Vancouver Island Health Authority employees, physicians, students, residents, researchers, contractors and affiliate agencies that have a contract relationship with VIHA.

#### **5.0 Responsibility for Security of Information**

Every individual subject to this policy has a responsibility to maintain the security of VIHA Information by ensuring that adequate security measures are followed. These measures include

- Ensuring all passwords are kept strictly confidential and adhere to VIHA standards;
- Compliance with all procedures associated with this policy;
- Ensuring ongoing awareness regarding the appropriate use of Information, and;
- Access to Information via approved equipment or processes.

The following activities are specifically prohibited under this Policy;

- Interfering with, tampering with, or disrupting the flow of Information;
- Attempting to access or accessing, Information you are not authorized to access;
- Exploiting or enabling the exploitation of Information;
- Knowingly enabling inappropriate levels of Information access by others, and;
- Disclosing any Information you do not have a right to disclose.

All VIHA employees have a responsibility to report violations of this policy without fear of reprisal. Individuals deemed responsible for violations of this policy 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.

#### **6.0 Definitions**

**Control** - of Information (contained in a record) means the power or authority to manage the record throughout its life cycle, including restricting, regulating and administering its use or disclosure.

The following are some of the factors indicating that a public body has control of a record:

- The record was created by a staff member, an officer, or a member of the public body in the course of his or her duties;
- The record was created by an outside consultant for the public body;
- The record is specified in a contract as being under the control of a public body;

- The content of the record relates to the public body's mandate and functions;
- The public body has the authority to regulate the record's use and disposition;
- The public body has relied upon the record to a substantial extent;
- The record is closely integrated with other records held by the public body; or,
- The contract permits the public body to inspect, review, possess or copy records produced, received or acquired by the contractor as a result of the contract.<sup>1</sup>

**Custody** - of Information (contained of a record) means having physical possession of a record, even though the public body does not necessarily have responsibility for the record. Physical possession normally includes responsibility for access, managing, maintaining, preserving, disposing, and providing security<sup>2</sup>.

**Information:** Any operational data or information gathered, processed transmitted or presented using a computer is defined as Information. This includes confidential personal health information and business related information.

## 7.0 Additional References:

16.4.2.2 Security of Health Records

[http://apps.viha.ca/pnp/pdf/1.5.1Privacy\\_Rights\\_and\\_Confidentiality\\_of\\_Personal\\_Information\\_vXXX2.pdf](http://apps.viha.ca/pnp/pdf/1.5.1Privacy_Rights_and_Confidentiality_of_Personal_Information_vXXX2.pdf)

[http://apps.viha.ca/pnp/pdf/1.5.2Confidential\\_Information\\_-\\_Third\\_Party\\_VIHA\\_Business\\_and\\_Other\\_Non-Personal\\_Information\\_vXXX1.pdf](http://apps.viha.ca/pnp/pdf/1.5.2Confidential_Information_-_Third_Party_VIHA_Business_and_Other_Non-Personal_Information_vXXX1.pdf)

**Standard ISO/IEC 27002:2005 Information Technology – Code of Practice for Information Security Management** (see [https://intranet.viha.ca/departments/imit/servicedesk/Documents/Service\\_Support/iso\\_27002.pdf](https://intranet.viha.ca/departments/imit/servicedesk/Documents/Service_Support/iso_27002.pdf))

Freedom of Information & Protection of Privacy Act. R.S.B.C. 1996, c. 165

[http://www.qp.gov.bc.ca/statreg/stat/F/96165\\_01.htm](http://www.qp.gov.bc.ca/statreg/stat/F/96165_01.htm)

---

<sup>1</sup> Ministry of Labour and Citizens' Services. Policy Definitions. Site accessed 13/08/09, URL: <http://www.cio.gov.bc.ca/services/privacy/manual/other/def.asp#control>

<sup>2</sup> Ministry of Labour and Citizens' Services. Policy Definitions. Site accessed 13/08/09, URL: <http://www.cio.gov.bc.ca/services/privacy/manual/other/def.asp#custody>