1.0 General Administrative

1.5 Corporate – Legal/Ethical

1.5.1 Confidential Information - Privacy Rights of Personal Information Policy

1.0 Introduction/Purpose

The Vancouver Island Health Authority (VIHA) is responsible to protect our clients' and VIHA agents' (see 5.4 and 5.5 for definitions) legal right to privacy of their personal information under our custody and control. VIHA further recognizes that we have an obligation to inform our clients and VIHA agents that there are specific circumstances that override an individual's right to privacy when personal information will be shared with individuals with an authorized requirement for that information. In all circumstances, VIHA recognizes the value of an individual's personal information, which must be collected, used, disclosed and protected appropriately.

The purpose of this policy is to provide a framework for the consistent management of personal information collected, used, disclosed and protected by the VIHA in accordance with the principles and requirements of various legislative Acts, including but not limited to BC's Freedom of Information and Protection of Privacy Act (FOIPPA), Evidence Act, Coroners Act, Ombudsman Act, Health Authority Act, Community Care Facility Act and various professional bylaws, privacy codes and standards of practice.

2.0 Policy

2.1 Privacy Right and Access to Personal Information

The right of privacy includes an individual's right to determine with whom he or she will share information and to know of and exercise control over collection, use, disclosure, access and retention concerning any information collected about him or

her. The right of privacy and consent are essential to the trust and integrity of the client care or service provider relationship.

While caregivers are expected to be open in their communication with patients with respect to their day-to-day care practices, it is also recognized that clients and other individuals may make formal written information requests to the VIHA in accordance with the provisions of FOIPPA.

Information rights include the right of access to records, with limited exception and the right to request correction of personal information about oneself. Individuals may formally request access to or correction of personal information by following proper procedures as outlined in the access to and release of information policies (referred to in 'Supporting and Related Policies and Procedures, pg. 8), subject to the exceptions for disclosure under FOIPPA.

2.2 Responsibility for Confidentiality

Personal 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 personal information is collected, used and disclosed only in circumstances necessary and authorized for client care, research, education, or as necessary in the conduct of the business of the organization. Use, sharing or disclosure of information must be 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 in order to fulfill one's professional role, by law or with permission from an authorized individual.

Client information in VIHA is collected and used for the provision of care or a healthcare related service. Disclosure of client information for other than that purpose, or as authorized by the appropriate legislative Act (e.g. FOIPPA), **without** informed client consent is a breach of client privacy and confidentiality.

Projects or initiatives concerning the collection, use or disclosure of personal information must have appropriate privacy protections in place. Specifically, all Information Systems Projects, Partnership arrangements and all other projects that collect, use or disclose personal information must complete a Privacy Impact Assessment (PIA), in consultation with the VIHA Regional Information and Privacy Office and Information Systems Security Office, PRIOR TO implementation of the

project. The PIA is a standardized process conducted to identify and address any impacts on privacy that may result from the implementation of new systems, projects or programs. A PIA must be completed at the outset of the initiative to aid in the design of privacy protections and ensure compliance with the privacy provisions of the *Act*.

Research involving human subjects may require completion of a PIA (to be determined by the VIHA Regional Research and Ethics Committee) and must be approved by the VIHA Regional Research and Ethics Committee.

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 VIHA Confidential Information - Privacy Rights of 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 Audits

Audits will be performed to ensure compliance to this policy. With respect to electronic records, automated audit systems can capture 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 audit process are the responsibility of each program area to outline in a corresponding procedure to this policy.

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. Personal 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.

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 VIHA Confidential Information - Privacy Rights of Personal Information Policy and the Confidentiality agreement.

Accessing information that you do not need to know to do your job:

- Unauthorized reading of a patient's chart.
- Accessing information on yourself, children, family, friends or co-workers.
- Asking co-workers for information that you do not need to do your job.
- Showing, telling, copying, selling, changing, or disposing of confidential information that is not pertinent to your role or care activity.

Providing access to your sign-on code and password for computer systems:

- Telling a co-worker your password so that he or she can log in to a computer system.
- Telling an unauthorized person the access codes for employee files or patient information.
- Leaving your password in plain view so that others may know it.

Providing or gaining unauthorized access to physical locations (e.g. file cabinets) which contain confidential information

- Lending out your keys to someone else to access file cabinets, file storage areas or other areas where confidential information is stored, OR using another's keys for the same purpose
- Leaving file storage areas unlocked when they should be locked.

Leaving a password protected application unattended while signed on:

- Being away from your desk while you are logged into an application.
- Allowing a co-worker to use your application for which he/she does not have access after you have logged in.

Sharing, copying or changing information without proper authorization:

- Making unauthorized marks on a patient's chart.
- Making unauthorized changes to an employee file.
- Discussing confidential information in a public area such as a waiting room or elevator.

Using another person's sign-on code and password:

- Using a co-worker's password to log in to a VIHA computer system.
- Unauthorized use of a log-in code to access employee files or patient accounts.
- Using a co-worker's application for which you do not have rights after he/she is logged in.

Failing to report a breach of confidentiality

- Being aware of a breach of confidentiality, but not reporting the breach to your supervisor or other designated individual.
- 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.

5.0 Definitions

5.1 Personal and Confidential Information[1]

Personal and confidential 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:

Personal information about an identifiable individual [e.g. client) including:

- The individual's name, address or telephone number,
- The individual's race, national or ethnic origin, colour, or religious or political beliefs or associations,
- The individual's age, sex, sexual orientation, marital status or family status,
- An identifying number, symbol or other particular assigned to the individual,
- The individual's fingerprints, blood type or inheritable characteristics,
- Information about the individual's health care history, including a physical or mental disability,
- Information about the individual's education, financial, criminal or employment history,
- Anyone else's opinions about the individual, and
- The individual's personal views or opinions, except if they are about someone else;

Confidential Information related to an identifiable individual under the custody and control of the VIHA including:

- Information (staff statements, legal advice, investigators' reports, incident reports) prepared as part of a pending or ongoing litigation, law enforcement investigation, quality assurance review or Coroner, Ombudsman or Human Rights investigation.
- Information related to credentialing, discipline, privilege, quality assurance reviews and external reviews of quality of care.

5.2 Information Privacy[2]

Information privacy refers to the right of an individual or data subject to determine with whom their personal information is shared, under what circumstances and to know of and exercise control over use, disclosure and access concerning any personally identifiable information collected about him or her.

5.3 Confidentiality

Confidentiality refers to the responsibility or obligation of an individual or organization to ensure that personal and confidential information is kept secure and is collected, accessed, used and disclosed appropriately.

5.4 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

5.5 Client

The term client includes patients, clients, residents, and customers.

5.6 Authorized Individual

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

Supporting and Related Policies and Procedures

[1] Freedom of Information and Protection of Privacy Act, S.B.C. 1992, Chapter 61, as amended by S.B.C. 1993, Chapter 46.
[2] Guidelines for the Protection of Health Data; COACH Security and Privacy Committee (2001)
CMA Health Information Privacy Code (1998)
CSA Standard CAN/CSA-Q830-96, Model Code for the Protection of Personal Information (R-2001).
Draft Privacy Charter and Guide; Ministry for Children and Families (1999)
VIHA Draft Policy Release of Personal Information from the Client Record (2002)
GVHS Policy V.a.45 Patient Access to Health Records (1993)
GVHS Policy V.c.10 Retention of Hospital Records (Revised Nov.1993.)
CHR Media Guidelines
CHR IS Policy and Procedures - Chapter 4.4 and Appendix S – Internet Policy
CHR IS Policy and Procedures - Chapter 4.0, Messaging – E-Mail usage
VIHA Policy and Procedure - Privacy Impact Assessments (pending 2002)
VIHA Policy 1.5.2. Confidentiality Information - Third Party, VIHA Business and Other Non-Personal Information (2002)
College of Physicians and Surgeons of British Columbia: Policy: Maintenance of Confidentiality of Patients' medical Records – Policy Manual – M –10 February 2000 – http://www.cpsbc.bc.ca/policymanual/m/m10.htm
http://www.cpsbc.bc.ca/policymanual/m/m10.htm
Privacy Code for Private Physicians' Offices in British Columbia
http://www.cpsbc.bc.ca/policymanual/p/p5.htm
http://www.cpsbc.bc.ca/policymanual/p/p5.htm

VANCOUVER ISLAND HEALTH AUTHORITY

CONFIDENTIALITY ACKNOWLEDGEMENT

Please use a pen to complete

I (print name) _____hereby acknowledge that I have read and understand the Vancouver Island Health Authority's (hereinafter called "VIHA") policies *1.5.1 and **1.5.2 regarding privacy and confidentiality. These policies outline my responsibilities regarding information obtained during the course of my employment, affiliation[1] or assignment[2] at the VIHA. I further acknowledge that I have read and understand the consequences for breach of these policies.

RELATIONSHIP WITH VIHA:

- Employee (provide Employee number)

_____

- Physician (provide Medical Billing number)

_____

- Other[3] (specify affiliation and name of VIHA contact)

_____

Signature: _____ Date_____/_____/_____
Day Month Year

* 1.5.1 Privacy Rights and Confidentiality of Personal Information
** 1.5.2 Confidentiality of Third Party, VIHA Business and other Non-Personal Information

[1]Affiliation: Connected to as a member or branch of an organization
[2]Assignment: Task or mission
[3]Other VIHA Agents: Volunteers, Researchers, Contractors, Sub-contractors, Vendors/suppliers or any individual directly or indirectly associated with VIHA.