AR0400 – PRIVACY AND MANAGEMENT OF CONFIDENTIAL INFORMATION

T Interior Health would like to recognize and acknowledge the traditional, ancestral, and unceded territories of the Dãkelh Dené, Ktunaxa, Nlaka'pamux, Secwépemc, St'át'imc, Syilx, and Tŝilhqot'in Nations, where we live, learn, collaborate and work together.

Interior Health recognizes that diversity in the workplace shapes values, attitudes, expectations, perception of self and others and in turn impacts behaviors in the workplace. The dimensions of a diverse workplace includes the protected characteristics under the human rights code of: race, color, ancestry, place of origin, political belief, religion, marital status, family status, physical disability, mental disability, sex, sexual orientation, gender identity or expression, age, criminal or summary conviction unrelated to employment.

1.0 PURPOSE

Provide a consistent approach for protecting Confidential Information under Interior Health's (IH) custody and control. The Policy also ensures that IH staff and agents are aware of, and acknowledge, the ethical and legal obligations and consequences of non-compliance.

2.0 DEFINITIONS

TERM	DEFINITION
Access	*Viewing information on paper or in electronic form, or through dialogue.*
Clients	*Patients and persons in care in IH facilities and programs.*
Confidentiality	*The duty to ensure that personal information is kept private and is accessible only to authorized persons.*
Confidential Information	*Whether oral, written, electronic or film, includes the following:* *a) Personal Information (see also definition below);* *b) business information collected or created by Interior Health that exists regardless of form and includes, but is not limited to:* • *information provided to Interior Health by an external vendor or service provider which, if disclosed, would harm the business interests of the third party;* • *financial information provided by Clients and Users including but not limited to bank account information, Social Insurance Number (SIN), credit card information, and Canada Revenue Agency (CRA) account information;*

	• *information prepared as part of 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;* • *in-camera deliberations of Interior Health where such topics as budget strategies, personnel, labor relations, land acquisitions or litigation may be discussed;* • *unpublished statistical information and internal correspondence related to organizational initiatives; and* • *information supplied in confidence to a mediator or arbitrator to resolve or investigate a labor relations dispute.* c) *all information that, if disclosed without authorization, could be prejudicial to the interests of Interior Health and associated individuals or agencies; and* d) *organizational business information that would harm Interior Health's financial interests and/or information that relates to the management of Interior Health that has not yet been implemented or made public; such as information that identifies the security architecture and infrastructure of the organizations' information systems.*
E-Health Act	*E-Health (Personal Health Information Access and Protection of Privacy) Act. The B.C. legislation that supports the introduction of electronic health records while ensuring patient privacy is protected.*
FIPPA	*Freedom of Information and Protection of Privacy Act, as amended from time to time, is the B.C. legislation that prescribes obligations that all public bodies are required to meet related to the collection, use, disclosure, protection and retention of personal information.*
Personal Information	*Includes any information which may be associated with or identifies an individual except business contact information. Personally identifiable information includes things such as a person's name, social insurance number, account number, health care number, employment*

	history or medical information. Personal information does not include business contact information, such as a person's title, business telephone number, business address, email or facsimile number. References to "personal information" within this policy apply to any documents or records (whether in hard copy or electronic form) on which personal information is recorded and all verbal comments or conversations in which personal information is mentioned or discussed.
Privacy	*The right of an individual to determine what information about themselves may be collected, used, and shared with others.*
Users	*All staff, medical staff, independent contractors, students, volunteers and any other persons acting on behalf of IH.*

3.0 POLICY

IH has value-based, ethical and legal obligations for the custody and control of Confidential Information.

IH recognizes:

- The rights of individuals to protection of privacy regarding all aspects of their Confidential Information, in keeping with the FIPPA and the E-Health Act; and
- Its requirement to inform individuals that there are circumstances that may override their right to privacy when Confidential Information will be shared with authorized individuals.

3.1 Scope

The obligations outlined in this policy apply to all IH (services, programs and agencies) Users and information in any format, including but not limited to, conversational, paper, or electronic. This policy applies while in the course of working and conducting business for or on behalf of IH, including when off-duty and extends beyond the completion of the employment or business relationship with IH. While this policy does not apply to Clients, it is recommended that Users make Clients aware of the nature of the policy and encourage them to uphold the themes of privacy and confidentiality as appropriate.

3.2 Collection, Use and Disclosure of Confidential Information

IH expects Users to collect, use and disclose Confidential Information:

- for purposes directly related to the delivery of health care services or for administration or employment purposes and limit the collection to what is needed to fulfill the purposes identified;
- for any purpose where the individual has explicitly consented to the use of their information.

Users are expected to comply with all IH policies, procedures and guidelines for the release of Confidential Information. This includes information for education, teaching, research, quality improvement, or other secondary purposes, coordinated as follows:

- release of Client health information is managed by the local facility where the service was provided according to standard practices;
- release of all corporate information is managed by the Freedom of Information office; and
- release of information for research purposes must meet the standards as outlined by the Interior Health Research Ethics Board, FIPPA Section 33(3)(h) and E-Health Act Sections 14, 19 and 20.

3.3 Accessing or Sharing Confidential Information

- Before Confidential Information under the custody or control of IH is shared with a third party, the appropriate data access and confidentiality acknowledgement, information sharing agreement/plan or a contract must be executed by the parties involved. All Users must abide by the data access and confidentiality acknowledgement. The Information Privacy Office must review all information access agreements for third parties, information sharing agreements/plans and/or privacy schedules.
- Users should take all reasonable steps to ensure no unauthorized personnel or third parties are provided with Access to records containing Confidential Information. Any third party requests for Access should be asked to produce identification and their legal authority to Access the requested information.
- Users are responsible for ensuring that no Confidential Information is accessed, transferred or stored outside of Canada except with the explicit consent of the individual the information is about or where otherwise permitted by FIPPA. Contact the Information Privacy Office before you implement any program that transmits, transport or stores Confidential Information outside of Canada.

3.4 Destruction of Confidential Information

Users must follow the process outlined in Security Bulletin #8 – Secure Handling of Confidential Information and AQ1800 – Surplus Equipment Disposal Policy to securely destroy Confidential Information.

3.5 Privacy Impact Assessment

Users must complete a Privacy Impact Assessment ("PIA") before implementing any new initiative or significantly changing any program, system or activity that requires the collection, use, or sharing of Confidential Information.

3.6 Compliance Monitoring and Auditing

Monitoring and audits will be performed to ensure compliance with this policy. IH Information Privacy office investigates all suspected breaches of this policy. Actions may be taken as identified in Section 3.7.

3.7 Accessing or Sharing Confidential Information

IH considers intentional viewing (accessing) of Confidential Information that is not required to carry out work-related responsibilities or the misuse of such information to be a breach of policy (for examples of breaches, see Appendix A). Failure to comply with this policy may lead to termination of Access, termination of employment, termination of contract, withdrawal of privileges and/or professional sanctions (Policy Reference: AR0450 Managing Privacy & Security Breaches).

3.8 Roles and Responsibilities

- ***Information Privacy Office*** – Information Privacy staff provide general oversight of privacy practices within IH, as well as delivery of privacy education and promotion of good privacy practices. Information Privacy responds to questions from Users, Clients, and members of the public concerning collection, access, use, and disclosure of Confidential Information. Information Privacy investigates potential and actual breaches of this policy brought to its attention and in accordance with IH breach policies.

- ***Managers*** – management staff have a responsibility to oversee compliance with this policy by Users within their area(s) of responsibility.

- ***Users*** – all have a responsibility to take appropriate steps to protect Confidential Information at all times, as well as complying with statutory requirements and their professional codes of practice.

AR0400 – PRIVACY AND MANAGEMENT OF CONFIDENTIAL INFORMATION

4.0 PROCEDURES

4.1 Users

- Review all relevant policies and complete the *Data Access & Confidentiality Acknowledgement* in iSite prior to commencing their relationship with IH.
- Agree to this Policy on an annual basis.
- Report any breaches of this policy to a supervisor, designate, or to the IH Privacy office without fear of reprisal. If necessary, complete an incident report in coordination with the Privacy office. All reported breaches are kept strictly confidential.

4.2 Manager / Chief of Staff

- Ensure Users review all relevant policies and complete the appropriate data access and confidentiality acknowledgement prior to commencing their relationship with IH,
- Agree to this Policy on an annual basis, and
- Follow-up on compliance audits in consultation with Human Resources, the Information Privacy Office and/or Executive Medical Directors, and taking appropriate action when required.

4.3 Human Resources / Volunteer Services / Medical Administration / Purchasing / Contract Managers

- Retain any signed hardcopy of applicable data access and/or confidentiality agreements in a User's IH file, or as indicated on the specific form.

4.4 Visitors

- Must sign a separate *Visitors' Confidentiality Acknowledgement Form* prior to commencing a visit or tour within an IH facility.
- The person organizing the visit or tour will:
  - Ensure visitors sign a *Visitors' Confidentiality Acknowledgement form*, and
  - File the form with their administration for retention period as indicated on the form.

5.0 REFERENCES

1. Freedom of Information and Protection of Privacy Act (FIPPA)
2. E-Health (Personal Health Information Access and Protection of Privacy) Act
3. IH Policy: AU0100 Standards of Conduct for IHA Employees
4. IH Policy: AR0100 Acceptable Use of Information Systems
5. IH Policy: AF0100 Transparency and Freedom of Information
6. IH Policy: RA0700 Confidentiality of Information
7. IH Policy: AR0450 Managing Privacy & Security Breaches
8. IH Users' Brochure: EMR – Privacy & Security User Guide
9. IH Client Notification Poster: Caring for Your Information
10. IH Employee Notification Poster: Caring for Your Information
11. IH Policy: AQ1800 Surplus Equipment Disposal
12. IH Security Bulletin #8 - Secure Handling of Confidential Information

AR0400 – PRIVACY AND MANAGEMENT OF CONFIDENTIAL INFORMATION

APPENDIX A - Examples of Breaches of Access, Privacy and Confidentiality

Accessing information that you do not need to know to do your job:
- Unauthorized reading of a Client's chart when not involved in the direct care of the Client as part of your role at Interior Health
- Accessing your own health information, children, family, friends or co-workers

Sharing, copying or changing information without proper authorization:
- Unauthorized release of health information for educational or teaching purposes
- Disclosing Client information without prior severing or anonymizing Client identifiers.
- Disclosing or discussing Client or other Confidential Information on a social networking website such as Facebook
- Discussing Confidential Information in a public area such as a waiting room or elevator
- Conducting private and confidential Interior Health business in a non-confidential Flexible Work Location space

Transporting and carrying information:
- Failing to properly secure paper files or electronic devices, when on the road and when working at a Flexible Work Location

Providing access to your personal userID and password for any IH computer system:
- Sharing your password so that a coworker can log onto an IH computer
- Allowing an unauthorized user, (i.e. member of the public), to use an IH computer

Leaving a password-protected Interior Health application unattended while signed on:
- Being away from your desk while you are logged into a computer
- Allowing a co-worker to use your application for which he/she does not have access after you have logged in

Using another person's personal userID and password:
- Using a co-worker's password to log onto a computer system
- Using a co-worker's application for which you do not have rights after he/she is logged in

Providing or gaining unauthorized access to physical locations, which contain or store Confidential Information:
- Lending out your keys or facility/office access swipe card to someone OR using another's keys/swipe card for the same purpose
- Leaving secure storage areas unlocked

Failing to report a breach of privacy, confidentiality or security:
- 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
- Not reporting that your mobile computing device you use for work has been lost or stolen, e.g. laptop computer, smartphone, or USB memory key