AR0400 – PRIVACY AND MANAGEMENT OF CONFIDENTIAL INFORMATION

1.0 PURPOSE

This Policy is intended to provide a consistent approach for protecting the personal information and other confidential information under the custody and control of Interior Health. The Policy also ensures that staff and agents of Interior Health are aware of and acknowledge the ethical and legal obligations, and consequences of non-compliance.

2.0 DEFINITIONS

Access includes viewing information on paper or in electronic form, or through dialogue.

Clients include patients, residents, and persons in care in Interior Health facilities and programs.

Confidentiality is the duty to ensure that personal information is kept private and is accessible only to authorized persons;

Confidential Information, whether oral, written, and electronic or film, includes the following:

a) personal information about any individual that includes their:

- name, address or telephone number
- race, national or ethnic origin, colour, or religious beliefs or associations
- age, sex, sexual orientation, marital status or family status
- Personal Health Number (PHN), identification number, symbol or other particular assigned to them
- fingerprints, blood type or inheritable characteristics
- health care history, including a physical or mental disability
- information about their educational, financial, criminal or employment history
- personal views or opinions, except if they are about someone else
- and anyone else's opinions about themselves

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
- 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, 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- unpublished statistical information and internal correspondence related to organizational initiatives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

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

FIPPA Freedom of Information and Protection of Privacy Act [RSBC 1996] C. 165, as amended from time to time, is the BC legislation that prescribes obligations that all public bodies are required to meet related to the collection, use, disclosure, protection and retention of personal information.

PHIAPPA Personal Health Information Access and Protection of Privacy Act [SBC 2008] C. 38. (also known as the eHealth Act). The BC legislation that supports the introduction of electronic health records while ensuring patient privacy is protected.

Privacy is the right of an individual to determine what information about themselves may be collected, used, and shared with others.

Users includes all staff, physicians, independent contractors, students, volunteers and any other persons acting on behalf of IH.

3.0 POLICY

Interior Health has value-based, ethical and legal obligations for the custody and control of personal and confidential information.
Interior Health recognizes:

- the rights of individuals to protection of privacy regarding all aspects of their personal and business information, in keeping with the FIPPA and PHIAPPA.

- its requirement to inform individuals that there are circumstances that may override their right to privacy when personal information will be shared with authorized individuals.

3.1 Scope

The obligations outlined in this policy apply to all Interior Health (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 Interior Health, including when off-duty and extends beyond the completion of the employment or business relationship with Interior Health. While clients and visitors do not fall under the scope of this policy, it is recommended that they be made aware of the nature of the policy and encouraged to uphold its theme of privacy and confidentiality as appropriate.

3.2 Collection, Use and Disclosure of Personal or Confidential Information

Interior Health expects that users will collect, use and disclose personal or 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; and

Users are expected to comply with all Interior Health 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 patient health information is managed by the local facility where the service was provided according to standard practices;
- release of all non-health information is managed by the Leader of Policy Development & Freedom of Information; and
- release of information for research purposes must meet the standards as outlined by the Interior Health Research Ethics Board, FIPPA Section 35 and PHIAPPA Sections 14, 15 and 20.

3.3 Accessing or Sharing Personal and Confidential Information

Before personal or confidential information under the custody or control of Interior Health is shared with a third party, the appropriate data access and confidentiality acknowledgement, information sharing agreement/plan and/or a contract must be executed by the parties involved. All users must abide by the data access and confidentiality acknowledgement. The Information Privacy & Security 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 personal or 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 personal or 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 legislation. The Information Privacy & Security Office must be consulted before any program is implemented in which personal or confidential information will be transmitted, transported or stored outside of Canada.

3.4 Destruction of Personal and Confidential Information

Users are expected to follow process for the secure destruction of personal and confidential information as outlined in Security Bulletin #8 – Secure Handling of Confidential Information and AQ1800 – Surplus Equipment Disposal Policy.

3.5 Privacy Impact Assessment

A Privacy Impact Assessment ("PIA") must be completed before implementing any new initiative or significantly changing any program, system or activity that requires the collection, use, or sharing of personal and confidential information.

3.6 Compliance Monitoring, Auditing

Monitoring and audits will be performed to ensure compliance with this policy. All suspected breaches of this policy will be investigated by the Information Privacy & Security Office. Actions may be taken as identified in Section 3.7 Failure to Comply

3.7 Failure to Comply

Interior Health considers intentional viewing (accessing) of personal and 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 Ref: AR0450 Managing Privacy & Security Breaches)

3.8 Roles & Responsibilities

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 ensure that appropriate steps are taken to protect personal and confidential information at all times, as well as complying with statutory requirements and their professional codes of practice.

4.0 PROCEDURE

4.1 Users

- Review all relevant policies and complete the *Data Access & Confidentiality Acknowledgement* prior to commencing their relationship with Interior Health and on an annual basis thereafter.

- Report any breaches of this policy to a supervisor, designate, or to the Interior Health Information Privacy & Security Office without fear of reprisal. If necessary, complete an incident report in coordination with Information Privacy & Security. 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 Interior Health.
- Agree to this Policy on an annual basis.
- Follow-up on compliance audits in consultation with Human Resources, the Information Privacy and Security 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 &/or confidentiality agreements in the user's Interior Health 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 Interior Health facility.
- The person organizing the visit or tour will:
    - Ensure visitors sign a *Visitors' Confidentiality Acknowledgement form*
    - File the form with their administration for retention period as indicated on the form.

5.0. REFERENCES

1. COACH (2009): Guidelines for the Protection of Health Information
2. Freedom of Information and Protection of Privacy Act (FIPPA)
3. eHealth Act, or Personal Health Information Access and Protection of Privacy Act (PHIAPPA)
4. IHA Policy: AU0100 Standards of Conduct for IHA Employees.
5. IHA Policy: AR0100 Acceptable Use of Information Systems
6. IHA Policy and Staff Brochure: AR0450 Managing Privacy & Security Breaches
7. IHA Users' Brochure: EMR – Privacy & Security User Guide
8. IHA Client Notification Poster: Caring for Your Information
9. IHA Employee Notification Poster: Caring for Your Information
10. IHA Policy: AQ1800 Surplus Equipment Disposal
11. IHA Security Bulletin #8 - Secure Handling 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

Transporting and carrying information:

- Failing to properly secure paper files or electronic devices, when on the road

Providing access to your personal userID and password for any IH computer system:

- Sharing your password so that another user/ unauthorized person 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 personal or 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, blackberry, smartphone, PDA, or USB memory key