Category: Information Access and Privacy	
Title: Privacy and Confidentiality Policy	**Reference Number:** IA_020
Approved by: PHSA Senior Executive Team	Last approved: Oct 24, 2016 Last reviewed: Oct 24, 2016

1. PURPOSE

The Provincial Health Services Authority (PHSA) is responsible for the management of all Personal Information and Other Confidential Information, within its possession (custody) and control. Due to the Lower Mainland Consolidation and other provincial activities PHSA its Staff and Agents have access to Personal Information and Other Confidential Information under the custody or control of any other Health Authority in British Columbia or its affiliates (the "Health Organization") in the delivery of a common or integrated programs. PHSA is responsible for managing all its own Personal Information and those of the other Health Organizations in accordance with the *Freedom of Information and Protection of Privacy Act* of British Columbia *(FIPPA)* and the *E-Health (Personal Health Information Access and Protection of Privacy) Act.* The PHSA also wishes to ensure that all Personal Information in its custody or control is kept secure and accessed in accordance with established access protocols.

The purpose of this Privacy and Confidentiality Policy ("Policy") is to:

a) establish the guiding principles and framework by which PHSA its Staff and Agents will comply with the obligations regarding the protection and management of Personal Information set out in FIPPA, the *E Health Act*, and other applicable legislation; and
b) set out obligations for Staff and Agents regarding maintaining the confidentiality of Other Confidential Information they may have access to during the course of their work at PHSA.

2. SCOPE

The obligations in this policy apply to all Staff and Agents relating to Personal Information and Other Confidential Information in any format including paper, electronic, film, and verbal discourse.

3. BACKGROUND

PHSA is governed by FIPPA, the *E-Health Act*, other legislation and standards of practice regarding protecting personal information. FIPPA in particular provides a framework for upholding privacy and confidentiality of Personal Information. There are privacy protection offences for individuals and organizations who commit an unauthorized disclosure under FIPPA and/or the E Health Act.

4. POLICY STATEMENT

4.1 Accountability

a. Accountability and Governance

The Chair of PHSA, or the Board of PHSA, as appropriate, are responsible for ensuring compliance with FIPPA. In accordance with FIPPA, accountability for compliance is delegated by the Chair of PHSA, or designated by the Board of PHSA as appropriate, to senior management roles within PHSA.

The PHSA Chief Privacy Officer is accountable for maintaining this policy and for providing general oversight of the PHSA privacy management program.

The Information Access and Privacy (IAP) Office is responsible for:

- advising PHSA departments and agencies on privacy compliance issues;
- advising PHSA departments and agencies on the interpretation and application of this policy;
- managing Privacy Impact Assessments;
- managing privacy breaches and suspected privacy breaches in accordance with the Managing Privacy Breaches Policy and ensuring that investigations are completed;
- managing privacy awareness and education programs;
- reviewing amendments to privacy legislation and making recommendations for policy changes;
- proactive monitoring of user activity in selected electronic systems containing Personal Information;
- acting as the point of contact for the Office of the Information and Privacy Commissioner of British Columbia (OIPCBC) when complaints are received about PHSA's compliance with FIPPA; and
- receiving notification of potential non-compliance with FIPPA.

PHSA will establish other policies and procedures to support compliance with FIPPA and the E Health Act.

b. Accountability and General Obligations of Staff and Agents

Staff and Agents must only collect, access, use, or disclose Personal Information and Other Confidential Information of PHSA or any other Health Organization as necessary to fulfill the terms and requirements of their duties and as authorized by this policy and the Standards of Business Conduct Policy AB 610 and the Code of Ethics Policy AB 600. and Agents must not collect, access, use, or disclose Personal Information and Other Confidential Information for personal use or gain, or for any purpose not expressly authorized by PHSA or a Health Organization.

All Staff and Agents must comply with the PHSA IMITS policies and security requirements developed for the use of electronic systems.

The obligations for ensuring privacy and confidentiality set out in this policy apply while on or off duty and continue after the employment, contract or other affiliation between PHSA its Staff and Agents ends.

c. Acknowledgement

All Staff and Agents must formally acknowledge their understanding of and commitment to upholding confidentiality by signing an acknowledgement of policy and/or PHSA Privacy Schedule or other agreement as deemed applicable by PHSA.

d. Mandatory Privacy Training

All Staff must complete the E learning privacy training every two years. Staff must complete any additional privacy training that is required by the professional regulatory association that they are affiliated with or that PHSA requires for their role.

e. Mandatory Privacy Reviews

PHSA departments and agencies must complete a Privacy Compliance Review or Privacy Impact Assessment (PIA) prior to undertaking any new initiative, program or activity that involves Personal Information. PHSA departments and agencies are accountable for addressing the compliance gaps identified in the review for their initiative, program or activity.

PHSA departments and agencies planning to undertake any new initiative, program or activity that involves Personal Information must consult with the IAP Office to determine whether a Privacy Compliance Review or PIA is required. Completion of the review is the responsibility of the department or agency implementing the new initiative, program or activity. The IAP Office provides advice to assist in the completion of the review. PHSA departments and agencies should refer to the Privacy Compliance Review User Guidelines.

Prior to PHSA undertaking any common or integrated program or activity with another public body or agency, as "common or integrated program or activity" is defined in FIPPA, PHSA must:

- Notify the Office of the Information and Privacy Commissioner (the "Commissioner") at any early stage of development; and
- Complete a PIA and submit it to the Commissioner for review.

A PHSA department or agency considering implementing a common or integrated program or activity must consult with the IAP Office and Legal Services.

f. Obligations to Report Foreign Demand

PHSA must report foreign demands for the disclosure of Personal Information to the Minister of Labour and Citizens' Services in accordance with *FIPPA.* "Foreign demands" include subpoenas, warrants, orders or requests from foreign courts or foreign government agencies.

Staff who receive a foreign demand, know about a PHSA service provider who has received a foreign demand, or know about the unauthorized disclosure of Personal Information in response to a foreign demand, must immediately inform Legal Services.

g. Consequences of Breach of Policy

Failure to comply with this Policy may result in disciplinary action including, but not limited to, the termination of employment, loss of computing privileges, loss of privileges as a student placement or volunteer, prosecution and restitution for damages.

h. Reporting Actual or Suspected Policy Breach

Staff must report any actual or suspected violations of this Policy to the IAP Office, or if they wish to report anonymously, must follow the process set out in the Whistleblower Policy AB 620 . Staff must report any actual or suspected Privacy Breach to the IAP Office

and to other PHSA Departments, as required by the process set out in the Managing Privacy Breaches Policy.

4.2 Collection of Personal Information

a. Purpose for Collection

Staff must have specific management authorization to collect personal information. Personal Information must only be collected for the following purposes:

- a purpose directly related to and necessary for a program or activity of PHSA (e.g. the delivery of health care services or for the purposes of managing the employment relationship);
- where the information is necessary for the purposes of planning or evaluating a program or activity of PHSA; or
- where the collection of the information is expressly authorized by legislation.

Staff not certain about whether the collection of Personal Information they propose to undertake is authorized, must consult with their immediate supervisor or the IAP Office.

b. Informing the Information Subject

Whenever Staff collect Personal Information directly from an individual, the individual must be informed:

- why the information is being collected;
- how it will be used or disclosed by PHSA;
- the legal authority for the collection; and
- the title, business address and business telephone number of an officer or an employee of PHSA who can answer the individual's questions about the collection.

c. Indirect Collection

In most cases, Personal Information must be collected directly from the information subject. Staff must not indirectly collect Personal Information unless such collection is authorized under FIPPA. Examples of the limited circumstances in which indirect collection is authorized:

- Personal Information may be collected indirectly if the information subject expressly consents to such collection;
- Staff may collect Personal Information from someone other than the information subject, such as friends or family members, if this collection is necessary to provide medical treatment and it is not possible to obtain the information subject's consent;
- Staff may collect Personal Information from other Health Authorities or health care providers if such collection is necessary to facilitate ongoing medical treatment;

Staff with questions about the collection of Personal Information should consult the IAP Office.

d. Limiting Collection

Staff members must not collect more Personal Information than is required to fulfill the specific purpose for which the information is collected.

4.3 Use of Personal Information

All access to and use of Personal Information by Staff and Agents must be exercised on a "need to know" basis and for purposes that are necessary for the performance of an individual's job functions and responsibilities. Staff and Agents must only access and use personal information for the following purposes, as authorized by FIPPA:

- the purpose(s) for which it was originally collected by PHSA (such as health care delivery or for administration or employment purposes;);
- for a purpose which is reasonably and directly related to the original purpose for collection and the use is necessary for a program or activity of PHSA;
- any purpose for which the individual has provided express written consent in the form required by FIPPA; or
- the purpose(s) for which the information was disclosed to PHSA by another public body such as another health authority.

4.4 Disclosure of Personal Information

Under FIPPA, disclosure occurs whenever Personal Information is provided to or accessed by someone.

a. Internal Disclosure or Sharing

Staff must only share or disclose Personal Information to other Staff members or Agents if those persons require the information in order to perform their job functions.

b. Disclosure to External Parties – General Requirements

The disclosure of Personal Information to persons or parties other than Staff must be made only where such disclosure is permitted by FIPPA and authorized by PHSA. PHSA is authorized under FIPPA to disclose Personal Information in the following circumstances:

- where specifically required or authorized by legislation to release Personal Information;
- where required by the terms of a court order, subpoena or warrant;
- where compelling circumstances exist affecting the health or safety of any individual;
- where the individual consents in writing to the information being disclosed;
- to a service provider for PHSA where the service provider is obligated by legal agreement to abide by FIPPA, and the conditions under "Sharing Personal Information With Third Parties" are met;
- to protect the public in circumstances where there is a risk of significant harm to the environment or to the health or safety of the public or a group of people.

Specific conditions must be satisfied before Personal Information may be disclosed under these categories. Before disclosing Personal Information to an external party, Staff must consult with their supervisor, the IAP Office, or Risk Management Department of PHSA, as appropriate to the circumstances.

Personal Information may also be disclosed for the purpose of a common or integrated program between PHSA and another public body or the Ministry of Health only if a written agreement describing services, Personal Information sharing, and other specific legal conditions has been signed. Staff must consult the IAP Office in the preparation of the required written agreement.

c. Disclosure to External Parties – Contractual Safeguards

All Agents and other third parties, accessing or sharing Personal Information in the custody or control of PHSA must execute an agreement in which that party agrees to abide by the terms of the PHSA Privacy Schedule. Legal Services must approve the form and content of the agreement.

Staff should take all reasonable steps to ensure no Agents or third parties are provided with access to records containing Personal Information, except as permitted under this Policy and FIPPA. Any Agent or other third party who requests access should be asked to produce identification, and confirmation that they have signed an agreement in accordance with this Policy.

d. No Disclosure Outside of Canada

All Staff must ensure that no Personal Information is accessed, transferred or stored outside of Canada, except with the written consent of the individual the information is about or as otherwise permitted by FIPPA, such as to collect a debt owing to PHSA or to contact an individual's next of kin in an emergency.

Staff must consult with the IAP Office prior to implementing any program or other initiative in which Personal Information will be transferred, stored or accessed outside of Canada.

e. Disclosure For Research Purposes

The disclosure of Personal Information for research purposes must be done in accordance with section 35 of *FIPPA,* after approval from the applicable Research Ethics Board, and in accordance with the processes required by the applicable PHSA agency.

Access privileges must only be granted to the Principal Investigator and personnel approved by the applicable Research Ethics Board.

Access to Personal Information on PHSA clinical systems for research purposes must adhere to applicable IMITS system access requirements, policies and procedures.

4.5 Accuracy of Personal Information and Handling Requests for Correction of Personal Information

PHSA Departments and agencies must make every reasonable effort to ensure that Personal Information they collect or cause to be collected is accurate and complete.

PHSA Departments and agencies must fully document and keep current the processes they use to make a decision affecting an individual.

An information subject who believes that there is an error on his or her Personal Information may request correction of this information. PHSA Departments and agencies in control of the Personal Information at issue must consider any request to correct the Personal Information. Where the information subject successfully demonstrates that the Personal Information is inaccurate, the record must be corrected. If no correction or addition is made, the record must be annotated with the correction that was requested but not made.

4.6 Retention of Personal Information

Personal Information in the custody or control of PHSA that is used to make a decision that directly affects the individual the information is about must be retained for a minimum of one

year from the time that it is used to make the decision, but all Staff are required to abide by the PHSA Records Retention Policy.

4.7 Protecting Personal Information

All Staff and Agents must take all reasonable steps to ensure that the security of Personal Information is at all times protected against unauthorized access, use, collection, disclosure, storage, retention, duplication, loss, theft and disposal.

Staff and Agents are expected to be familiar with, maintain and enforce the security arrangements applicable to their own program areas. All program areas must adhere to the IMITS Policies.

4.8 Responding to Access Requests From the Public, Clients, Staff, and Governmental Authorities

Under FIPPA, members of the public have the right to request access to records within the custody or control of PHSA. The law also recognizes that, subject to certain limited exceptions, individuals have the right to access their own information, including medical information. PHSA has various policies and procedures dealing with processing such access requests.

Staff members receiving such access requests should refer the requests to the appropriate department, as follows:

- Health Care/Medical Records - Requests by Clients for access to their medical information should be referred to Health Information Management.
- Employment Files. - Requests for access to employment, payroll or human resources files received from employees, legal firms, financial institutions, insurance companies, credit bureaus, the Canada Revenue Agency and police should be directed to Human Resources.
- Non Medical Records – Formal requests under Part 2 of FIPPA for access to non clinical records should be directed to the IAP Department in accordance with the Freedom of Information Policy.

4.9 Audit and Compliance Programs

Suspected breaches of this Policy will be managed in accordance with the Managing Privacy Breaches Policy. PHSA operational areas and programs must conduct appropriate reviews and audits of their systems and processes to ensure compliance in accordance with PHSA policies and standards. If a review or audit uncovers the suspected or confirmed theft or loss of Personal Information or the unauthorized collection, use, disclosure, storage, or disposal of Personal Information the PHSA Managing Privacy Breaches Policy will apply.

4.10 E-Health Act and Health Information Banks

PHSA shall comply with all requirements of the *E-Health (Personal Health Information Access and Protection of Privacy) Act* and any ministerial orders published in respect of a designated health information bank ("HIB") in the custody or control of PHSA and in respect of the collection into and use or disclosure of Personal Information in respect of a HIB in the custody or control of a Ministry or other health care bodies as defined in that Act.

Staff and Agents must comply with PHSA policies and procedures applicable to HIBs to which Staff or Agents may have access or into which Staff or Agents may disclose Personal Information.

4.11 Challenging Compliance

PHSA will investigate all complaints concerning compliance with this Policy, and, if a complaint is found to be justified appropriate measures will be taken, including amending policies and procedures where required. The complainant will be informed of the outcome of the investigation regarding the complaint, if permitted by law and PHSA policy.

5. PROCEDURES

Procedures are to be developed by the IAP Office and be available on POD.

6. EXCEPTIONS

There are no exceptions to this Policy.

7. RELATED POLICIES

Listed below are the related PHSA policies:

- Code of Ethics Policy AB 600
- Freedom of Information Policy IA_010
- Managing Privacy Breaches IA_100
- Record Retention Policy IA_200
- Standards of Business Conduct Policy AB 610
- Theft, Fraud, Corruption and Non-Compliant Activities policy AB 630
- Whistleblower Policy AB 620
- All IMITS policies developed for the security of personal and confidential information

For further information, please refer to Information Access and Privacy Office.

8. DEFINITIONS

Agents may include but are not limited to: fee for service physicians, other health care providers, researchers, contractors, sub-contractors, vendors/suppliers, or any other third party individual directly/indirectly associated with the PHSA in a business relationship.

Clients means all persons receiving services from PHSA and includes patients or their authorized or legal representative.

Collaboration Organization means any Health Organization with which PHSA is engaged in the delivery of a common or integrated program or activity.

Confidentiality is the responsibility and obligation of an employee or agent of PHSA to ensure that Personal Information or Other Confidential Information is kept secure and is collected, accessed, used, disclosed, stored and disposed of only for purposes necessary and authorized by PHSA or a Collaboration Organization to conduct its business.

FIPPA means the *Freedom of Information and Protection of Privacy Act* [RSBC] Chapter 165.

Health Organization means any Health Authority in British Columbia or its affiliates.

IAP Office means the Information Access and Privacy Office of PHSA. For further information, please refer to http://pod/phsa/foi/pages/Default.aspx

IMITS means the consolidated Information Management/Information Technology Services department of PHSA, Vancouver Coastal Health Authority, and Providence Health Care.

Other Confidential Information is the information provided to, collected or created by the PHSA or a Collaboration Organization, which may or may not contain information on an identifiable individual, in the course of the business operations of the PHSA or such Collaboration Organization.

Other Confidential Information includes:

- information provided to PHSA or a Collaboration Organization 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, intellectual property, information or technology
- information prepared as part of a pending or ongoing litigation, law enforcement or Internal Audit investigation, quality assurance review or Coroner, Workers Compensation, Ombudsman or Human Rights investigation
- information related to credentialing, discipline, privilege, or external reviews of quality of care
- in camera deliberations of the PHSA or a Collaboration Organization where such topics as personnel, labour relations, land acquisitions or litigation may be discussed • unpublished statistical, scientific, technological or other intellectual property information, or internal correspondence related to organizational initiatives
- information supplied in confidence to a mediator or arbitrator to resolve or investigate a labour relations dispute.

Personal Information means any information about an identifiable individual, but it does not include business contact information (business contact information is information such as a person's title, business telephone number, business address, email or facsimile number).

PHSA means the Provincial Health Services Authority, its programs, divisions, services and branch societies.

Privacy Breaches are the loss, theft, intentional or inadvertent unauthorized collection, use, disclosure, storage or disposal of personal information in the custody or control of the PHSA or Collaboration Organization. Such activity is "unauthorized" if it occurs in contravention of Part 3 of the *Freedom of Information and Protection of Privacy Act* or this policy.

Privacy Impact Assessment ("PIA") is an assessment of a current or proposed initiative (a system, enactment, project, program, or activity) to evaluate privacy impacts, including evaluating compliance with this Policy and with PHSA's privacy responsibilities under FIPPA.

Staff means, officers, directors, employees, physicians, health care professionals, students, volunteers and researchers engaged by PHSA or organizations with which PHSA has concluded a services agreement.