

Appendix B

Privacy Impact Assessment Template and Guide for Treasury Board, Executive Council Office, Office of Policy and Priorities, and the Chief Information Office (“the Offices”)

Note: Attach supporting documentation as necessary

1. Introduction

- a) Name of Program or Service
- b) Name of Department, Branch and Program Area
- c) Name of Program or Service Representative
- d) Key Program or Service Dates

2. Description

- a) Summary of the New Program or Service or the Change
 - i. General Description
 - ii. Purposes, Goals and Objectives
 - iii. The Need
- b) The Intended Scope
- c) Conceptual Technical Architecture
- d) Description of Information Flow (include text and diagram)

3. Collection, Use and Disclosure of Personal Information

- a) Authority for the Collection, Use and Disclosure of Personal Information
- b) List of Personal Information to be Collected, Used and/or Disclosed and the Rationale for each
- c) The Sources and Accuracy of the Personal Information
- d) The Location of the Personal Information
- e) The Retention Schedule and Method of Destruction or De-identification for Personal Information
- f) Identification of Consent Issues
- g) Users of Personal Information

4. Access Rights for Individuals to their Personal Information

5. Privacy Standards: Concerns and Security Measures

- a) Security Safeguards
 - i. Administrative Safeguards
 - ii. Basic Technical Safeguards
 - iii. Auditing

b) Methods for Avoidance of Unintentional Disclosure

6. Compliance with Personal Information International Disclosure Protection Act

7. Conclusions

- a) An Assessment of the Impact on Privacy, Confidentiality and Security of Personal Information as a Result of the New Program or Service or Change
- b) Strategy for Mitigation of Privacy Risks, if any
- c) Additional Comments

Completed by:

Program/Service Representative

Date

Reviewed by:

Privacy Lead for "the Offices"

Date

Recommended by

Senior IM Management Position

Date

Approved by:

Deputy Minister

Date

Guide for the use of the Privacy Impact Assessment Template

Notes:

- ▶ This Guide is intended to assist you with the completion of the Privacy Impact Assessment. When completing the Assessment, keep in mind that not all questions will be relevant to your project at this time.
- ▶ If a question is not applicable, answer “Not applicable,” but do not delete the question from the Assessment.
- ▶ Add additional questions and/or explanations as required by your project.
- ▶ Attach any relevant documents.
- ▶ Where appropriate, provide information on both the current plan, and future intentions for the program/service.
- ▶ “Change” means a change to a program or service that affects the collection, use, disclosure or retention of personal information and includes the implementation of an information system.
- ▶ It is important to remember your audience for this assessment. It is not intended to be an assessment of the technical architecture of the system, but an assessment of privacy issues arising from a change. Make an effort to keep information straightforward and understandable by a reader who does not have expertise in information system technology, law, or the background to the system.
- ▶ Avoid jargon and acronyms unless they are explained.
- ▶ Explain any terms, positions and organizations that are not commonly understood.
- ▶ Although information must be comprehensive, make an effort not to include information that is not necessary to the reader’s understanding of the change and its impacts.

1. Introduction

- 1. Name of Program or Service**
- 2. Name of Department, Branch and Program Area**
- 3. Name of Program or Service Representative**
- 4. Key Program or Service Dates**
 - a) This may include program or service initiation date, implementation date(s), project completion date, and other key milestones, if applicable.

2. Description

- a) Summary of the New Program or Service or Change**
 - a) General Description
 1. Provide a brief explanation of the new program or service or change and include a brief explanation of the existing program, service or change.
 - b) Purposes, Goals and Objectives
 - a) What are you trying to accomplish with this new program or service or change? For example:
 - improve client services
 - make a program more efficient, save time and other resources
 - improve protection of privacy
 - standardize a program component
 - track incidence of a specific event/action
 - obtain sufficient information to administer the program
 - c) The Need
 - Why are you making this new program or service or change?
 - is it required by law, policy or standards?
 - is it to fulfill a governmental/departmental commitment or mandate?

b) The Intended Scope

a) Outline both the planned and anticipated scope of the program or service. The “scope” may include:

- Conversion from a paper-based information system to an electronic information system.

- Who is able to use the system? (e.g. in the current plan, only Department of XXX staff will have access to the system. In future, it is anticipated that other Departments will have access.) Note that the identification of specific users (e.g. clerks) will be covered in question 3(g).

- Linkages with other systems or programs (e.g. an example of anticipated linkage is a plan to “link data-collection system X with billing-system Y by 2007.”)

- The type of information collected (e.g. in the first year the system will collect only name, address and contact information; by year three the system will include additional identifiable financial information).

- Future enhancements to the system (e.g. remote access).

- Future uses of the information (e.g. secondary use of data research or analysis).

c) Conceptual Technical Architecture (if applicable)

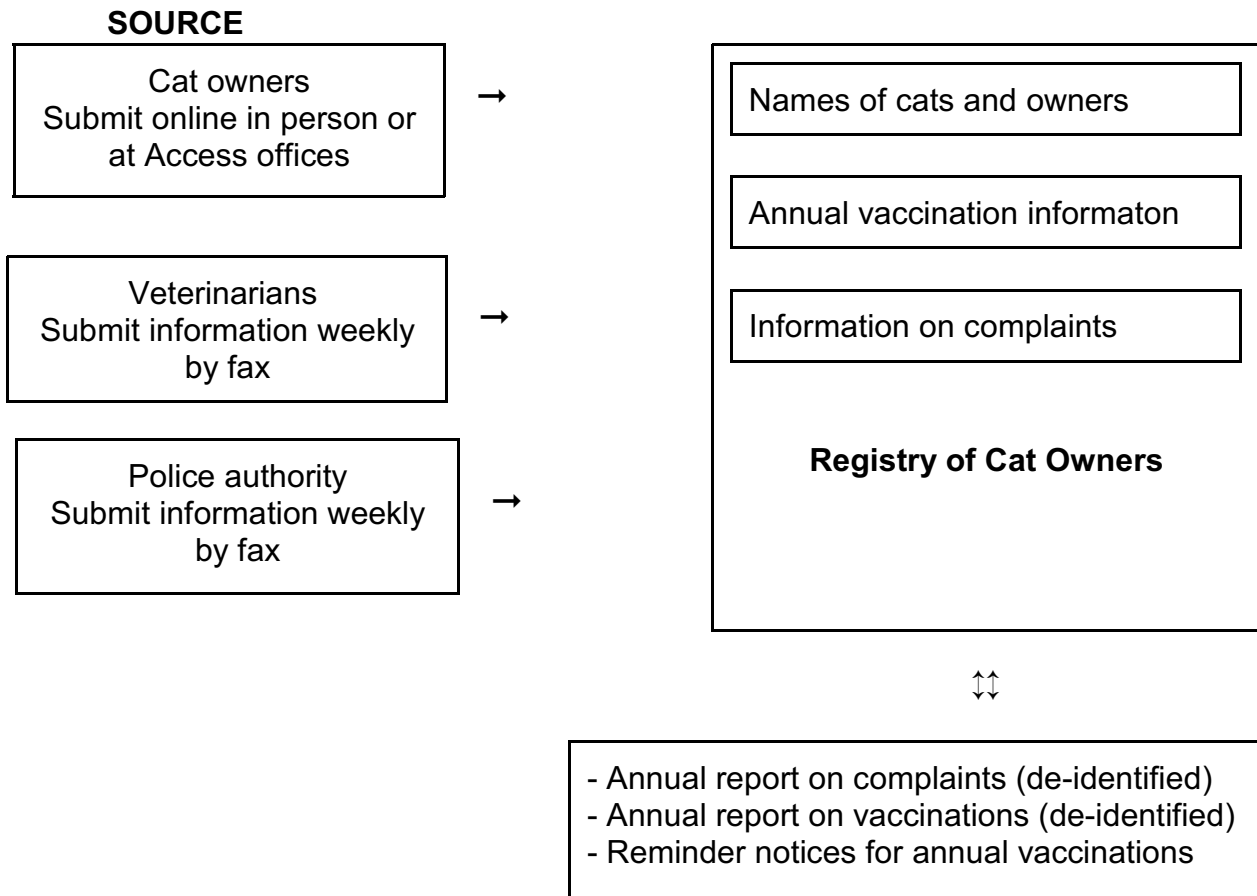
- Identify and describe the types of applications, platforms, and external entities involved in the information flow. Describe their interfaces, services, and the context within which the entities interoperate.

- This document is not intended to assess the technical security aspects of an electronic system. This section should be brief and clear to all readers. It is not intended to be or to replace a Threat Risk Assessment if one is required.

d) **Description of Information Flow (include text and diagram to describe flow as necessary)**

This section should include a diagram, but also requires a written description of any manual procedures and an identification of the staff who will be users of the system or who will receive information from the system.

Mock example: Information Flow for a Registry of Cat Owners



Note: Cat owners will be informed of the registry through notices and advertisements, but registration is voluntary.

Veterinarians will obtain consent to provide vaccination information to Registry.

3. Collection, Use and Disclosure of Personal Information

NOTE: Tables would be helpful to organize the answers to (a), (b), (c), and (d)

a) Authority for the Collection, Use and Disclosure of Personal Information

- ✓ Is there a law, regulation or authorized policy that allows you to **collect** the personal information as outlined in the new service or program or change?
- ✓ Is there a law, regulation or authorized policy that allows you to **use** the personal information as outlined in the new program or service or change?
- ✓ Is there a law, regulation or authorized policy that allows you to **disclose** the personal information as outlined in the new program or service or change?

b) List of Personal Information to be Collected, Used and/or Disclosed, the Method of Collection and Disclosure, and the Rationale for each.

There must be a reason or intended use for each item of personal information.

- ✓ List each item or field to be collected, and the reason or intended use for the collection.

For example:

Telephone number	To contact clients to update them on program changes
Financial information	To verify income

- ✓ In general, good privacy principles mandate that the minimum amount of information necessary for the purpose is collected, used and disclosed. Is it necessary to collect each item of personal information to fulfill your purposes?

For example, do you need date of birth or would month and year of birth or age in years be sufficient?

- ✓ In some cases it may be necessary to include information which may not appear to the writer to be “personal information”. This can be discussed with the reader; there may be information that in combination with other information would be categorized as “personal information”.
- ✓ Do not exclude data elements on the basis that you think there are no privacy issues with the data elements. The data, in combination with other data held on this system or others may raise privacy issues.

Example of a table for this section:

Data Element	Rationale for Collection, Use and/or Disclosure	Method of Collection and Disclosure	Comments
Name	Collected to identify clients	Provided by client on application form	Disclosed by e-mail to approved vendors

c) The Sources and Accuracy of the Personal Information

- ✓ Who is providing the information – the individual or another source (e.g. another government department, a family member)?
- ✓ Is the information as accurate and up to date as is necessary for the purposes for which it would be used and disclosed?
- ✓ Are there any data-quality issues that are linked to user and system performance?

d) The Location of the Personal Information

- ✓ Is the information on servers or in a data repository? Will it be recorded on paper only and maintained in files?
- ✓ Where will the information be located? List all locations.
- ✓ Will the information be stored in multiple locations? For example, will users be permitted to store information on other devices (.e.g. laptops) or produce information from system (e.g. print and store in files)? If “Yes”, do you have a policy on protection of information held on electronic devices?
- ✓ Will the data be interfaced with data from other systems?
- ✓ If there is a data repository, give the name, description and geographical location of the repository.
- ✓ Additional questions related to the *Personal Information International Disclosure Protection Act* are in Section 6.

e) The Retention Schedule and Method of Destruction or De-identification for Personal Information

- ✓ Is there a retention schedule or timetable for keeping the information in its identifiable form (e.g. hospital retention schedules)? If “Yes”, please include or attach schedule, and provide a link between the data elements and the retention schedule.
- ✓ Is retention monitored for compliance to the schedule?
- ✓ What is the plan and method of destruction (if any)?

f) Identification of Consent Issues

- ✓ Are you required by law, regulation or policy to obtain consent for the collection, use or disclosure of personal information?

For example:

Sections 26 and 27 of the *FOIPOP Act* outline the circumstances under which a public body may use and disclose personal information with and without consent. Do either of these sections apply?

Please note that consent is not always required for collection, use and disclosure. It is important for you to confirm whether or not consent is required.

- ✓ Has the individual consented to the collection, use and disclosure anticipated in the new program or service or change? If “Yes”, what is the method of requesting consent? Attach any consent form(s), and outline the process for obtaining consent.
- ✓ If consent has not been collected, have the subject individuals been notified (either specifically or generally) of the new program or service or change?

g) Users of Personal Information

- ✓ List the users (positions, not names) who will have access to the information. If it is a generic category of user (e.g. nurses) be as specific as you can be (e.g. nurses employed by District Health Authority XX who provide care to patients in the XYZ Clinic).
- ✓ Describe the level of access each user group will have to personal information.
- ✓ Include a brief rationale for each user’s need to access the information.
A table would be very helpful for completion of this section:

User Group	Level of Access	Rationale	Comments
Clerical Staff	Demographic information only (Name, Address, HCN, DOB)	To address reimbursement forms to clients	
Research and Statistical Officers, Public Health Program	Access to all data elements except identifiers (Name, Address, HCN). Clients will be identified by a Program Number.	RSOs do not need to know the names of the clients to conduct their analyses.	The system has been customized to automatically replace the identifiers with a Program Number.

4. Access Rights for Individuals to their Personal Information

- ✓ Will individuals have access to their personal information on the system? Sections 2(a)(ii) and 2(c) of the *FOIPOP Act* require public bodies to provide individuals with a right of access to their personal information.
- ✓ If “Yes”:
 - ✓ describe your process for allowing access to their personal information; and
 - ✓ indicate if individuals will be informed of the following:
 - the information source(s) of their personal information
 - the uses and disclosures of their personal information

Note: In the case of this example, of information held by the Department of Health and/or the Department fo Health Promotion and Protection, individuals would request their personal information by application to the Department’s Administrator, Information Access and Privacy.

5. Privacy Standards: Concerns and Security Measures

a) Security Safeguards

i. Administrative Safeguards

- ✓ Do contracts with external service providers contain privacy provisions, which meet or exceed the privacy standards of the *Freedom of Information and Protection of Privacy Act*?
- ✓ Have all users signed confidentiality agreements? If not, are they subject to a Code of Conduct that includes the requirement for confidentiality?
- ✓ Has staff received training on privacy and confidentiality policies and practices?
- ✓ Is access to the personal information restricted on a “need to know” basis? How is this determined?
- ✓ What controls are in place to prevent and monitor misuse of the personal information?
- ✓ Is there a process in place for access or role changes for system users (e.g. users who leave employment or change jobs)?
- ✓ Describe the process in case of a breach of privacy.

ii. Basic Technical Safeguards

Note: This section is intended to capture information related to basic technical safeguards (e.g. passwords, security that is related to the location of the information (e.g. locked filing cabinets). It is not intended to capture and assess the security elements of an information system that more properly would be assessed in a Threat/Risk Assessment.

- ✓ How is the personal information collected and transferred from the individual to the system/program?

For example, electronic, paper, fax, and courier
- ✓ If the information is transmitted in electronic format, is it being transmitted within a secured server, is it encrypted?
- ✓ Is all access to the system password-protected?

- ✓ Are all users trained on best password practices?
- ✓ Is there an automatic prompt for users to change their passwords? If “Yes”, how often are they asked to change the password?
- ✓ Is remote access to the information permitted? If “Yes”, what is the method for access? Is the information secure on transfer?
- ✓ Will the system be tested to ensure privacy controls are functioning?
- ✓ Are fax machines located in a secure, private area?
- ✓ Are paper files secured in a locked area with controlled access?

iii. Auditing

- ✓ Does the level of sensitivity of the information require that use of this system be audited? If “No”, why not?
- ✓ Does the system have the capability to audit access and/or view to the system?
- ✓ What is the level of information that audit can produce (e.g. can it identify individual patients/clients, pieces of information etc. that the user viewed)?
- ✓ Does the audit always run, or is it a system that must be switched on and off?
- ✓ Is there a limit to the time that audit information can be kept?
- ✓ Will an auditing plan be developed?
- ✓ Are resources being committed to the auditing and follow-up function?

b) Avoidance of Unintentional Disclosure

- ✓ Is the information reviewed prior to disclosure to prevent unintentional disclosure of personal information?
- ✓ When statistical information about a small group of individuals is disclosed outside the Department, there is a risk that these individuals could be identified. As a general guideline, do not disclose statistical information about groups (cells) containing fewer than five individuals.
- ✓ Are small cell sizes (e.g. cells of fewer than five) disclosed?
- ✓ If small cell sizes are to be disclosed, what is the rationale for doing so?

6. Compliance with the *Personal Information International Disclosure Protection Act*

- ✓ Will any person transport the information in a computer, a cell phone or another mobile electronic device outside of Canada?
- ✓ If “Yes”, provide the rationale for the head of your public body to give permission to do so.
- ✓ Will any personal information be:
 - a) accessed from
 - b) stored in, or
 - c) disclosed toa person or organization outside Canada?
- ✓ If “Yes”, provide details, including the rationale for any access, storage and disclosure outside Canada.
- ✓ If “Unknown”, provide as much detail as possible, and indicate what steps will be taken to confirm the information.
- ✓ Who is the vendor(s), and does the vendor(s) have any foreign affiliation, subcontractors, parent company(s), or sites?
- ✓ What is the commitment date of the contract(s)?
- ✓ What is the renewal date of the contract(s)?

7. Conclusions

- a) **An Assessment of the Impact on Privacy, Confidentiality and Security of Personal Information as a Result of the New Program or Service or Change**
- ✓ Assess the privacy, confidentiality and security impact on personal information as a result of:
 - the new program or service
 - changes to the current program or service
 - anticipated future changes to the program or service.
- ✓ Discuss both negative and positive impacts.

b) Strategy for Mitigation of Privacy Risks

- ✓ Outline any plans or proposals for reducing or eliminating any negative impacts on privacy.

c) Additional Comments

- ✓ Make any additional comments related to the privacy impact(s).

Completed by:

Program/Service Representative Date

Reviewed by:

Privacy Lead for "the Offices" Date

Recommended by:

Senior IM Management Position Date

Approved by:

Deputy Minister Date

Reference:

FOIPOP Definition of Personal Information

Does the access, storage or disclosure involve personal information? Personal information is defined as recorded information about an identifiable individual, including:

- (i) the individual's name, address or telephone number
- (ii) the individual's race, national or ethnic origin, colour, or religious or political beliefs or associations
- (iii) the individual's age, sex, sexual orientation, marital status or family status
- (iv) an identifying number, symbol or other particular assigned to the individual
- (v) the individual's fingerprints, blood type or inheritable characteristics
- (vi) information about the individual's health-care history, including a physical or mental disability
- (vii) information about the individual's educational, financial, criminal or employment history
- (viii) anyone else's opinions about the individual, and
- (ix) the individual's personal views or opinions, except if they are about someone else.

FOIPOP Sections on Collection, Use and Disclosure

Does Section 24(1) of the *FOIPOP Act* authorize you to collect the personal information:

- a) Is the collection of that information expressly authorized by or pursuant to an enactment?
- b) Is that information collected for the purpose of law enforcement?
- c) Does that information relate directly to and is necessary for an operating program or activity of the public body?

Does Section 26 of the *FOIPOP Act* authorize you to use the personal information:

- a) For the purpose for which it was obtained or compiled or for a use compatible with that purpose?
- b) Has the individual the personal information is about identified the information and consented to its use?

- c) If the personal information was disclosed to the public body under Sections 27 to 30 of the *FOIPOP Act*, is the information being used for that same purpose?

Does Section 27 of the *FOIPOP Act* authorize you to disclose the personal information:

- a) in accordance with this Act or as provided pursuant to any other enactment
- b) if the individual the information is about has identified the information and consented in writing to its disclosure
- c) for the purpose for which it was obtained or compiled, or a use compatible with that purpose
- d) for the purpose of complying with an enactment or with a treaty, arrangement or agreement made pursuant to an enactment
- e) for the purpose of complying with a subpoena warrant, summons or order issued or made by a court, person or body with jurisdiction to compel the production of information
- f) to an officer or employee of a public body or to a minister, if the information is necessary for the performance of the duties of, or for the protection of the health or safety of the officer, employee or minister
- g) to a public body to meet the necessary requirements of government operation
- h) for the purpose of
 - (i) collecting a debt or fine owing by an individual to Her Majesty in right of the Province or by a public body to an individual
 - (ii) making a payment owing by Her Majesty in right of the Province or by a public body to an individual
- i) to the Auditor General or any other prescribed person or body for audit purposes
- j) to a member of the House of Assembly who has been requested by the individual, whom the information is about, to assist in resolving a problem
- k) to a representative of the bargaining agent who has been authorized in writing by the employee, whom the information is about, to make an inquiry
- l) to the Public Archives of Nova Scotia, or the archives of a public body, for archival purposes
- m) to a public body or a law-enforcement agency in Canada to assist in an investigation
 - (i) undertaken with a view to a law-enforcement proceeding, or
 - (ii) from which a law-enforcement proceeding is likely to result
- n) if the public body is a law-enforcement agency and the information is disclosed
 - (i) to another law-enforcement agency in Canada or
 - (ii) to a law-enforcement agency in a foreign country under an arrangement, written agreement, treaty or legislative authority
- o) if the head of the public body determines that compelling circumstances exist that affect anyone's health or safety
- p) so that the next of kin or a friend of an injured, ill or deceased individual may be contacted, or
- q) in accordance with sections 29 or 30. **PIIDPA Definition of Personal Information**

The PIIDPA definition is the same as that found in FOIPOP, see page 13 of this document.

PIIDPA sections on Access, Storage and Disclosure

5(1) A public body shall ensure that personal information in its custody or under its control and a service provider or associate of a service provider shall ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada, unless:

- (a) Where the individual the information is about has identified the information and has consented, in the manner prescribed by the regulations, to it being stored in or accessed from, as the case may be, outside Canada
- (b) Where it is stored in or accessed from outside Canada for the purpose of disclosure allowed under this *Act*, or
- (c) The head of the public body has allowed storage or access outside Canada pursuant to subsection (2).

(2) The head of a public body may allow storage or access outside Canada of personal information in its custody or under its control, subject to any restrictions or conditions the head considers advisable, if the head considers the storage or access is to meet the necessary requirements of the public body's operation.

(3) Where the head of a public body makes a decision pursuant to subsection (2) in any year allowing storage or access outside Canada, the head shall, within ninety days after the end of that year, report to the Minister all such decisions made during that year, together with the reasons therefor.

(4) In providing storage, access or disclosure of personal information outside Canada, a service provider shall only collect and use such personal information that is necessary to fulfill its obligation as a service provider, and shall at all times make reasonable security arrangements to protect any personal information that it collects or uses by or on behalf of a public body.

Do you have the authority under PIIDPA to disclose personal information outside of Canada

8 A person referred to in Section 3 (essentially an employee of a public body) who has access, whether authorized or unauthorized, to personal information in the custody or under the control of a public body, shall not disclose that information except as authorized pursuant to this *Act*.

9(1) A public body shall ensure that personal information in its custody or under its control and a service provider or associate of a service provider shall ensure that personal information in its custody or under its control is disclosed outside Canada only as permitted pursuant to this Section.

(2) A public body, service provider or associate of a service provider may disclose outside Canada personal information in its custody or under its control

- (a) in accordance with this Act
- (b) where the individual the information is about has identified the information and consented, in writing, to its disclosure inside or outside Canada, as the case may be
- (c) in accordance with an enactment of the Province, the Government of Canada or the Parliament of Canada that authorizes or requires its disclosure
- (d) in accordance with a provision of a treaty, arrangement or agreement that
 - (i) authorizes or requires its disclosure, and
 - (ii) is made under an enactment of the Province, the Government of Canada or the Parliament of Canada
- (e) to the head of the public body, if the information is immediately necessary for the performance of the duties of the head
- (f) to a director, officer or employee of the public body or to the head of the public body, if the information is immediately necessary for the protection of the health or safety of the director, officer, employee or head
- (g) to the Attorney General or legal counsel for the public body, for use in civil proceedings involving the Government of the Province or the public body
- (h) for the purpose of
 - (i) collecting moneys owing by an individual to Her Majesty in right of the Province or to a public body, or
 - (ii) making a payment owing by Her Majesty in right of the Province or by a public body to an individual
- (i) for the purpose of
 - (i) licensing or registration of motor vehicles or drivers, or
 - (ii) verification of motor vehicle insurance, motor vehicle registration or drivers' licences

- (j) where the head of the public body determines that compelling circumstances exist that affect anyone's health or safety
- (k) so that the next of kin or a friend of an injured, ill or deceased individual may be contacted, or
- (l) in accordance with Section 10 or 11.

(3) In addition to the authority pursuant to this Section, a public body that is a law-enforcement agency may disclose personal information in its custody or under its control to

- (a) another law-enforcement agency in Canada, or
- (b) a law-enforcement agency in a foreign country under an arrangement, a written agreement, a treaty or an enactment of the Province, the Government of Canada or the Parliament of Canada.

Do you have authorization to transport personal information outside of Canada?

9(4) The head of a public body may allow a director, officer or employee of the public body to transport personal information outside Canada temporarily if the head considers it is necessary for the performance of the duties of the director, officer or employee to transport the information in a computer, a cell phone or another mobile electronic device.