# Privacy Policy

## Office of the Premier

### Policy Statement

It is the policy of the Office of the Premier that adherence to the privacy protection provisions of the *Freedom of Information and Protection of Privacy Act* (FOIPOP), the *Personal Information International Disclosure Protection Act* (PIIDPA), the Government Privacy Policy, the *Privacy Review Officer Act*, and other applicable legislation will be ensured. The Office of the Premier will uphold the principles of transparency, custodianship and shared responsibility established in the Government Privacy Policy, as it relates to the collection, use and disclosure of personal information.

### Definitions

For the purposes of this policy, the following definitions shall apply:

#### Employee(s)

An individual in the employ of, seconded to, or under personal service contract to the Office of the Premier, and its volunteers, students, and interns who have access to records.

#### FOIPOP

*Freedom of Information and Protection of Privacy Act*

#### Personal Information

As defined in clause 3 (i)(i) of the *FOIPOP Act*, "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, color, 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.

### Privacy Breach

The event of unauthorized collection, access, use, disclosure, or alteration of personal information.

### Privacy Impact Assessment

A Privacy Impact Assessment (PIA) is a due diligence exercise which identifies and addresses potential privacy risks that may occur in the course of the operations of a public body.

### Record

As defined in clause 3(l)(k) of the *FOIPOP Act*, includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or any other mechanism that produces records.

## Policy Objectives

The policy is designed to ensure that government meets its legislated obligations in the management of personal information throughout its life cycle. This includes ensuring the protection of personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

## Application

This policy applies to:

- All employees
- All personal information in the custody and control of the Office of the Premier.

## Policy Directives

- The Office of the Premier shall collect, access, store, use, disclose and dispose of personal information only where authorized by law or agreement with another public body that is authorized by law.
- The deputy head of the Office of the Premier shall identify those individuals with designated or delegated responsibilities for making reasonable security arrangements for personal information in keeping with the provisions of applicable legislation.
- The Office of the Premier shall have a privacy breach protocol, per the template maintained by the NS Information and Access Privacy Office (See Appendix A, “Privacy Breach Protocol and Privacy Complaint Protocol.”)
- The Office of the Premier shall complete a privacy impact assessment for any new program or service or for a significant change to a program or service, as per the template maintained by the NS Information Access and Privacy Office (See Appendix B, “Privacy Impact Assessment Template and Guide.”)
- All employees shall be advised of the policy coming into force.
- This policy shall be made readily available and will be posted on the Premier’s website.

- Requests for correction of personal information or to express concern regarding compliance shall be directed to IAPServices@novascotia.ca, attention: IAP Administrator.

## Policy Guidelines

To support the policy in securing Personal Information, the Office of the Premier will establish specific procedures that will include the following:

- Personal Information will be used, disclosed, or shared only for the purpose for which it was obtained or compiled, or for a use compatible with that purpose [pursuant to Sections 24-30, *FOIPOP Act*; also see Appendix B, "Privacy Impact Assessment Template and Guide."
- Access to files containing Personal Information will be limited to access needed for operational requirements / performance of duties, pursuant to Section 27, *FOIPOP Act*.
- Databases containing Personal Information will be password-protected.
- Directories containing Personal Information will be password-protected.
- Passwords will be issued on a need-to-know basis, as determined by operational requirements, pursuant to Section 27, *FOIPOP Act*.
- Filing cabinets containing Personal Information will be locked.
- Personal Information will not be stored on thumb drives, unless they are password protected.
- Files containing Personal Information will not be removed from the Office of the Premier or left unattended, except with the approval of the Supervisor.
- Blackberries will be password-protected and emails sent and received using Outlook will be encrypted by the Government Blackberry Enterprise Server.
- Approval is required from the head of a public body to take Blackberries and other electronic devices outside the country, pursuant to Section 9 (4) of the *Personal Information International Disclosure Protect Act* (PIIDPA). See also Appendix B, "Privacy Impact Assessment Template and Guide."
- When sending emails to more than one private individual at a time, when those individuals are known to the sender but unknown to each other, ensure that the individuals are blind copied. This will ensure that their email addresses are not inappropriately disclosed to all the other third parties in the email, and will therefore prevent a privacy breach from occurring.
- When the Office of the Premier receives a request from a third party to assist in resolving a problem with another third party, ensure compliance with s. 27 of the act (i.e., ensure that the office has the permission of the first third party, in writing, to share his/her Personal Information with the second third party).
- If this authority cannot be obtained, where possible the office will provide the contact information for the first third party to contact the second third party directly.

- Disposal of both transitory and master records containing Personal Information will be carried out only using secure methods, such as shredding (including shred boxes used for on-site confidential shredding).
- Training and awareness will be provided to all staff on the privacy protection of Personal Information.
- The Office of the Premier shall ensure that all new employees receive a copy of this policy in an orientation package, and that the IAP Administrator will provide training on proper procedures regarding the privacy of Personal Information.
- The Office of the Premier will provide a process for expressing concerns about compliance with its privacy policy.
- If the Office of the Premier receives a concern or complaint regarding this policy, they must immediately notify the IAP Administrator to ensure appropriate response, as well as the time frame in which the individual can expect to receive a response.

## Accountability & Security

1. The deputy head of the Office of the Premier shall be accountable for compliance with this policy.
2. Each employee is responsible for complying with this policy and the privacy policy of the Government of Nova Scotia.

## Monitoring

The IAP Administrator assigned to the Office of the Premier will be responsible for monitoring compliance with this policy.

## References

- *Freedom of Information and Protection of Privacy Act* and regulations
- *Personal Information International Disclosure Protection Act*
- *Government Records Act*
- *Privacy Review Officer Act*
- 4.7 Website Privacy Policy (Corporate Administrative Policy Manuals: Manual 300, Common Services, Chapter 4)
- 4.11 Privacy Policy (Corporate Administrative Policy Manuals: Manual 300, Common Services, Chapter 4)
- 1.2 Corporate Administrative Policy Manuals Policy (Corporate Administrative Policy Manuals: Manual 100, Management Guide, Chapter 1)
- Privacy Impact Assessment
- Privacy Breach Protocol
- Canadian Standards Association Model Code 10 Principles

## Enquiries

Corporate IAP/FOIPOP Administrator
Office of the Premier
(902) 424-4879 (direct)
(902) 424-5150 (general)
(902) 424-0667 (fax)

Approval Date: March 19, 2009
Effective Date: April 1, 2009
Administrative Update: February 1, 2016

## Approved by:

Deputy Minister, Office of the Premier

# Appendix A

## Privacy Breach Protocol and Privacy Complaint Protocol for the Office of the Premier

A Privacy Breach may be discovered through a variety of means. It may be uncovered expectantly in the course of normal business activity. It might be very obvious as soon as it happens. Or there could be a complaint from someone whose information way involved, or from a third party. Regardless, there must be a clear set of instructions on how to proceed once a privacy breach is suspected or discovered.

Part 1 of this protocol is for responding to a breach or suspicion of a breach, however it occurred.

Part 2 of this protocol is for responding to an actual complaint about an alleged privacy breach, which requires additional steps to be considered.

# Part 1
## Privacy Breach Protocol for the Office of the Premier

1. **Identify the privacy breach**
   Once the potential of a privacy breach has been identified, establish the date, time, location, length, type and extent of the breach.

2. **Immediate remedial action**
   Identify what action is to be taken to contain/stop the breach. For consideration:
   - Were hard copies of any faxed personal information retrieved or was there confirmation that the recipient(s) securely disposed of the fax?
   - Was the Government email (Outlook) recipient(s) who had opened the email contacted to request the email be deleted and hard copies securely destroyed?
   - Regarding a recipient(s) not on the Government email system (Outlook), did you contact the recipient(s) to request deletion of the email and secure disposal of any hard copies?
   - Will the breach allow access to any other personal information, and if so, were steps taken to avoid this potential additional breach?
   - If an electronic device and/or paper records containing personal information was stolen, did you immediately contact security (if within a public body facility) or the police (if outside a public body facility)?

3. **Internal notification**
   Provide instructions on who needs to be notified internal to your organization. Note: In all cases, notify your supervisor and the IAP Administrator, who will consult with the Communications Director/Advisor. Also recommended:
   - If the breach involves a website, the Department of Internal Services will be contacted.
   - If the breach is serious or could be potentially serious, the Deputy Minister and Legal Counsel need to be contacted.

4. **Investigation and documentation**
   Determine the detail of what/whose personal information is involved, and what is the extent/scope of the breach. Example questions:
   - Were the immediate remedial actions effective?
   - Is there enough documented evidence about the incident to determine the series of events that led to the breach?

5. **External documentation**
   When personal privacy is breached, it is necessary to determine which stakeholders (e.g., public bodies or municipalities, general public, individuals, etc.) should be notified, under what circumstances, and when. Outline external notification requirements. For consideration:
   - After the IAP Administrator consults with the Deputy Minister and Legal Counsel, one or more of the following may need to be notified:
     - Individual(s) whose privacy has been breached,

- Chief Information Officer, Province of Nova Scotia,
- Communications Nova Scotia (through your Communications Director),
- Security Authority, and/or
- Other individuals who may have been affected by the breach.

**6. Follow-up and long-term remedial action**

Determine what follow-up and long term remedial action there will be to prevent the breach from occurring again (e.g., analysis of incident to identify future preventive measures). Example questions include:

- Was the privacy breach protocol followed?
- Are new or amended policies, procedures, and/or training required to prevent re-occurrence of the breach?
- What plans have to be developed to lessen the likelihood or eliminate the possibility of another breach?

# Part 2
# Privacy Complaint Protocol for the Office of the Premier

1. **Receive and document the complaint.**
   When a complaint is received, discuss the details of the alleged breach with the complainant and document what the complainant believes has happened. This is a critical first step and should be completed in writing so that it can form part of the record of the response to the complaint. It is recommended that a consistent format be used for this purpose. The Information Access and Privacy Office will be developing a template for use by government entities in the near future. In the meantime, the following structure is recommended.

2. **Follow Steps 2 through 6 of the Privacy Breach Protocol.**
   At this point, all of the steps required for a self-identified or suspected privacy breach are the same as described in the previous template. Containment, internal and external notifications, full investigation and follow-up are all required.

3. **Complainant communication.**
   A complaint obviously differs from an internal discovery to the extent that there is an external complainant. Communication throughout the process and at the end of the process with the complainant(s) is a unique requirement in this regard.

   Governed by the complexity of the breach scenario and the duration of the ensuing investigation, the following steps should be incorporated into the Office of the Premier's complaint procedure:

   3.1 Send written acknowledgment to the complainant, re-stating the details presented by the complainant to the Office of the Premier, and an indication of who is accountable internally for the investigation (first formal correspondence).

   3.2 Send written update of progress of the investigation (stage of investigation, follow-up activities, expected or updated time frames, etc.) This step should be triggered by the time that has elapsed since initial acknowledgment of the complaint. A written update is required no later than two months from the acknowledgment. Updates continue on a schedule set out in the Office of the Premier's procedure.

   3.3 Generate a report of the results of the investigation. At a minimum, the report is to include:

   - verification of the breach
   - mitigating activities
   - other follow-up activities

   3.3 Share the de-identified details of the breach investigation with the Information Access and Privacy Office for incorporation into training and communication.

# Appendix B

## Privacy Impact Assessment Template for the Office of the Premier

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 Safety 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 Office of the Premier Date

**Recommended by**

Senior IM Management Position Date

**Approved by:**

Deputy Minister Date

# Appendix B

## Privacy Impact Assessment Template Guide for the Office of the Premier

### 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**
    a. Name of Program or Services
    b. Name of Department, Branch and Program Area
    c. Name of Program or Service Representative
    d. Key Program or Service Dates
        i. This may include program or service initiation date, implementation date(s), projection completion date, and other key milestones, if applicable.

2. **Description**
    **a. Summary of the New Program or Service or Change**
        **i. General Description**
            ✓ Provide a brief explanation of the new program or service or change and include a brief explanation of the existing program, service or change.
        **ii. Purposes, Goals and Objections**
            ✓ 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
        **iii. 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**
        i. 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.")

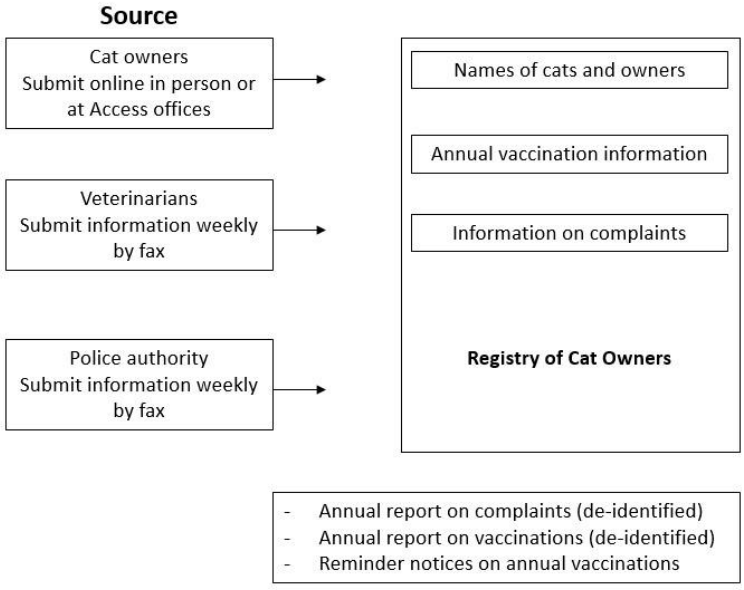
- ✓ The type of information collected (e.g., in the first year the system will collect only name, address and contact information; by year three the system will include additional identifiable financial information).
- ✓ Future enhancements to the system (e.g., remote access).
- ✓ Future uses of the information (e.g., secondary use of date research or analysis).

c. **Conceptual Technical Architecture** (if applicable)
   i. 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 inter-operate.
   ii. 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 email 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 the 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**

i. 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 XXX who provide care to patients in the XYZ Clinic).

ii. Describe the level of access each user group will have to personal information.

iii. Include a brief rationale for each user's need to access the information.

A table will 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 analysis. | 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 Wellness, individuals would request their personal information by application to the Department's Information Access and Privacy (IAP) Administrator.

**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, 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:
  - accessed from
  - stored in, or
  - disclosed to

  a 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 Office of the Premier 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, color, 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 program body?

Does Section 26 of the FOIPOP Act authorize you to use 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 Section 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 if 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 Nova Scotia Archives, 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
    a) undertaken with a view to a law-enforcement proceeding, or
    b) 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
    a) to another law-enforcement agency in Canada or
    b) 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 22 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 therefore.

(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.

**<u>Do you have the authority under PIIDPA to disclose personal information outside of Canada</u>**

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 monies owing by an individual to Her Majesty in right of the Province or to a pubic 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.