4.1.1 Access and Privacy Policy

Introduction

1. All business at the Board shall be conducted in compliance with the provisions of the *Freedom of Information and Protection of Privacy Act*[1], *Personal Information International Disclosure Protection Act*[2], and *Privacy Review Officer Act*[3]. These laws regulate the public's access to information collected or controlled by the Board and the Board's responsibilities to protect personal information that is maintained in Board's records from unauthorized disclosure.

2. The Board affirms the importance of access to information and an obligation to conduct its operation in ways that are open to public scrutiny. The right to access, however, is balanced by the need to protect personal privacy.

Policy Statement

3. The Board will uphold the principles of transparency, custodianship and shared responsibility as it relates to the collection, use, disclosure and disposal of personal information.

Definitions

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

    a. **"application"**, includes any matter or thing which the Board can determine within those statutes setting out the Board's mandate with respect to applications, including a complaint.

    b. **"appeal"** means any proceeding, matter or thing that the Board can determine within those statutes setting out the Board's mandate with respect to appeals.

    c. **"Board"** means the Nova Scotia Regulatory and Appeals Board as an organization created under the *Energy and Regulatory Boards Act.*

    d. **"Chair"** means the Chair of the Board.

    e. **"employee"** for ease of writing, the term "employee" includes both Members and staff of the Board. For greater clarity, this also includes an individual in the employ of, seconded to, appointed to, or under personal service contract to the Board.

    f. **"*FOIPOP Act*"** means the Nova Scotia *Freedom of Information and Protection of Privacy Act*.

[1] Link to *Freedom of Information and Protection of Privacy Act*
[2] Link to *Personal Information International Disclosure Protection Act*
[3] Link to *Privacy Review Office Act*

g. **"personal information"** is as defined in clause 3(1)(i) of the *FOIPOP Act* which is "recorded information about an identifiable individual." In particular:

(1) the individual's name, address or telephone number,

(2) the individual's race, national or ethnic origin, colour, or religious or political beliefs or associations,

(3) the individual's age, sex, sexual orientation, marital status or family status,

(4) an identifying number, symbol or other particular assigned to the individual,

(5) the individual's fingerprints, blood type or inheritable characteristics,

(6) information about the individual's health-care history, including a physical or mental disability,

(7) information about the individual's educational, financial, criminal or employment history,

(8) anyone else's opinions about the individual, and

(9) the individual's personal views or opinions, except if they are about someone else.

h. **"privacy breach"** means the event of unauthorized collection, access, use, disclosure, or alteration of personal information.

i. **"PIA"** means a Privacy Impact Assessment that is a due diligence exercise which identifies and addresses potential privacy risks that may occur in the course of the operations of the Board.

j. **"record"** has the meaning as defined in clause 3(1)(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.

k. **"third party"** in relation to a request for access to a record or for correction of personal information, means any person, group of persons or organization other than the person who made the request; or the Board.

Policy Objectives

5. This policy is designed to ensure that all employees of the Board are aware of the terms of the applicable legislation and conduct business accordingly.

Application

6. This policy applies to:

a. all employees of the Board.

b. all personal information in the custody and control of the Board.

Policy Directives

7. The Board shall, as required by law[4] and subject to the procedures set out in the *FOIPOP Act*:

   a. provide the public with the right to access records that the Board has custody of or control over;

   b. provide individuals with the right to access and correct personal information about themselves;

   c. withhold from disclosure certain records as specified in the *FOIPOP Act;*

   d. prevent the unauthorized collection, use, access, disclosure or disposal of personal information;

   e. provide routine public information and personal information about the person requesting it; and

   f. respond to a formal request for access under the *FOIPOP Act*.

8. The Chair is responsible for ensuring that Board operations comply with the applicable legislation, and for making final decisions regarding the release or withholding of requested information.

9. The Chair will identify those individuals with designated or delegated responsibilities for making reasonable security arrangements for personal information in keeping with the provisions of applicable legislation. Please see Appendix A for current delegations.

10. The Board shall have a Privacy Breach Protocol and follow the template maintained by the Nova Scotia Privacy Commissioner (see Appendix B).

11. The Board shall complete a Privacy Impact Assessment for any new program or service or for a significant change to a program or service, as outlined in the template provided by the Nova Scotia Information Access and Privacy Office (included as Appendix C). See the Executive Director if assistance is needed completing the assessment.

12. The Board is responsible for ensuring that contracts with service providers are compliant with this policy and the *Personal Information International Disclosure Protection Act.*

13. This policy shall be made readily available and will be posted on the Board's website. Requests for correction of personal information or to express concern regarding compliance shall be directed to the Executive Director or Chief Clerk.

Proceeding or Hearing Records

14. The Board, as a quasi-judicial tribunal, is bound by the “open court” principle such that the documents, hearings and decisions of the Board must be open and accessible to all.

[4] See *Freedom of Information and Protection of Privacy Act*, section 2

Particularly, the public has right to attend and observe the proceedings in the hearing room unless the presiding Member determines that the personal or confidential nature of the information to be discussed warrants closing or restricting access to some or all the proceeding.

15. All information that becomes part of the official record is open to public scrutiny unless subject to a statutory or Board-ordered publication or disclosure ban.

16. For the reasons outlined in the paragraph 14 and 15 of this Policy, and in accordance with the Section 4, paragraph (2)(c) of the *FOIPOP Act*, the *FOIPOP Act* does not apply to Board's documents filed in respect of an application or an appeal.

17. In accordance with Rule 12 (1) of the *Board Regulatory Rules*, all documents filed in respect of an application must be placed on the public record. Other rules have similar provisions for appeals. Those documents can be examined by accessing Board's website or by contacting the Board and requesting access through the appropriate Clerk of the Board.

18. In an attempt to balance privacy interests with the "open court" principle, and to prevent harm coming to participants, the Board, in accordance with the Rule 12 (11) of the *Board Regulatory Rules,* may choose to hold information in confidence or otherwise restrict its dissemination. Other rules have similar provisions for appeals.

19. Personal information, other than a person's name, contained in evidence or other documents filed as part of a proceeding will be redacted where posted to the Board's website or case management system in areas which allow for public viewing. Names will not be redacted unless otherwise directed by the Clerk or Member responsible for the file.

20. Records relating to proceedings will be retained and disposed of in accordance with the approved Standard for Operational Records.

21. Destruction of records containing personal or confidential information will be done using a method that ensures the information is protected during the destruction process and will not be retrievable.

Non-proceeding or Non-hearing Records

22. Right to Access. Every individual has the right to access any record held by the Board. Access to records will be given unless the legislation specifically allows the information to be withheld.

23. Mandatory exemptions from disclosure are:

    a. confidential business information; and

    b. personal information.

24. Information of a public and routine nature and personal information about the person requesting it will be released informally. Mandatory and discretionary exceptions are clearly outlined in the *FOIPOP Act*.

25. For the list of documents that are available to the public without a formal request for access under the *FOIPOP Act* please refer to the Board's 2.2.1 Routine Access Policy[5].

26. Release of information other than that listed in paragraphs 24 and 25 of this Policy require a formal written request for access under the *FOIPOP Act.* Search and copy fees may apply.

27. When a formal request is received, it must be forwarded to the Executive Director. In the absence of the Executive Director requests are to be forwarded to the Chair.

28. The Board has 30 business days to respond to requests for access. The Executive Director follows the instructions within the *FOIPOP Act* to meet the requirements of the formal request. This may entail the request or transference of information to another public institution, the request for fees to be paid before a search is undertaken or contact with the requester to clarify the request.

29. All records, electronic or otherwise, relating to Board business are subject to disclosure in accordance with the *FOIPOP Act*.

30. All records, electronic or otherwise, stored on Board media or on Board property are subject to access and monitoring by the Chair or designate.

31. Protection of Privacy. The Board will collect only that personal information for which it has a legal authority to do so. Information not expressly required for the operations of the Board must not be collected.

32. 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[6].

33. When personal information is requested from an individual, the individual must be informed of the purpose for collecting the information, the legal authority for collecting it, and the name of the Board employee to whom questions may be directed.

34. Every effort must be made to ensure that personal information held by the Board is accurate and complete.

35. An individual who believes there is an error or omission in his or her personal information should contact the Board to correct the information.

36. Every reasonable precaution must be taken to protect personal information from unauthorized access, collection, use, disclosure or disposal.

37. Access to personal information must be provided only to employees who require the information for the performance of their duties.

[5] 2.2.1 Routine Access Policy (DM: 205563)

[6] Sections 24-31, Protection of Personal Privacy: Collection, Protection, Retention, Use and Disclosure of Personal Information, *FOIPOP Act*; also see Appendix C, "Privacy Impact Assessment Template and Guide" pg. 13-28

38. Employees who have access, either authorized or unauthorized, to personal information held by the Board may not disclose that information except as authorized under the *FOIPOP Act*.

39. Personal information will be held by the Board only as long as is necessary for the operation of a program, the provision of a service, or as required by legislation, after which time it will be destroyed. [Note: this does not include personal information forming part of the public record related to proceedings. That information may be retained indefinitely.]

40. Retention periods mandated by legislation or the Nova Scotia Government's records management program will be adhered to.

41. Destruction of records containing personal information will be done using a method that ensures the information will not be retrievable.

42. Personal information will be disclosed only in accordance with the *FOIPOP Act* as determined by the Chair.

43. Requests for access to third party information, either personal or economic, will be processed pursuant to Sections 20 - 23 of the *FOIPOP Act* to determine whether such information may be released or would be an unreasonable invasion of the third party's personal privacy.

Accountability and Security

44. The Chair is accountable for compliance with this policy. Each employee of the Board is responsible for complying with this policy.[7]

45. Board employees shall protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal. Measures taken should include, but not be limited to:

    a. Password-protected access to electronic systems containing personal information. Computer passwords will be stored securely and not disclosed to others except as is necessary for the proper discharge of duties.

    b. When sending e-mails to more than one private individual at a time, when those individuals are known to the sender but unknown to each other, individuals are to be blind copied. This will ensure that their e-mail addresses are not inappropriately disclosed to all the other third parties in the e-mail, and will therefore prevent a privacy breach from occurring. For greater certainty, parties in a proceeding are deemed to be known to each other and blind copying is not required unless otherwise requested and approved by the Board, or some substantive risk is known.

    c. Taking special precautions when moving or traveling with personal information. Approval is required from the Chair to take smartphones and other electronic

[7] Note that this policy is written in the context of Member conduct being governed by the *Ethical Principles for Judges* issued by the Canadian Judicial Council.

devices which may contain personal or confidential information outside the country[8] .

d. Ensuring that files containing personal information stored on mobile devices are encrypted or otherwise protected from unauthorized access (e.g.,flash drives stored in locked cabinet or protected area).

e. Filing cabinets containing personal information will be held in secure areas protected by appropriate security (e.g., alarms, cameras, staff presence), or be locked.

f. Files containing personal information will not be removed from offices unless necessary for the conduct of duties. Where removed, it will be appropriately secured.

g. Files containing personal information will not be left unattended outside of secure areas.

h. Disposal of both transitory or 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 by a third party service provider).

i. Sharing personal information with other employees only as necessary for the operation of programs or provision of services.

j. Confirming the identity of persons requesting personal information and their authority to have that information.

46. When an employee ceases to be an employee of the Board, his or her supervisor must ensure that:

a. All personal information in the possession or control of the employee is returned to the Board.

b. All access privileges to Board facilities and information held by the Board are revoked.

c. All ID badges, keys and other means of access are collected.

47. Training and awareness will be provided to all staff on the protection of personal information.

48. The Human Resources Officer shall ensure that all new employees receive a copy of this policy in an orientation package, and provided with training on proper procedures regarding the privacy of personal information.

49. Concerns about compliance with its privacy policy can be expressed to either the Chair or the Executive Director.

[8] See Section 9(4) of the *Personal Information International Disclosure Protection Act* (PIIDPA) and also Appendix C, "Privacy Impact Assessment Template and Guide" pg. 13-28

50. Questions concerning application of the *FOIPOP Act* or any process can be addressed to the Executive Director or the Chair.

Monitoring

51. All supervisors are responsible for monitoring compliance with this policy.

Authority

52. This policy is issued on the authority of the Chair and is effective as of December 9, 2016.

References

53. *Freedom of Information and Protection of Privacy Act and Regulations*

54. *Personal Information International Disclosure Protection Act*

55. *Government Records Act*

56. *Privacy Review Officer Act*

57. Canadian Standards Association Model Code 10 Principles

Appendices

58. Appendix A: Delegations
Appendix B: Privacy Breach Protocol
Appendix C: Privacy Impact Assessment Template and Guide

Revision History

59. This document replaces document 230466 – Privacy Policy issued previously.

Appendix A

Delegations

1. The following persons are delegated by the Chair as making reasonable security arrangements for personal information, for their respective areas of mandate, in keeping with the provisions of applicable legislation:

    a. All Board Members (for their own case notes)

    b. All Clerks of the Board (for operational records relating to cases assigned to them)

    c. Controller (for accounting, payroll and general administration files)

    d. Human Resources Officer (for human resources)

2. Pursuant to Section 44 of the *Freedom of Information and Protection of Privacy Act*, the Chair has delegated responsibility to receive applications for access to a record to the Executive Director.

Appendix B
Privacy Breach Protocol

Privacy Breach Management Protocol Template

Introduction:
This template was drafted by the Office of the Information and Privacy Commissioner for Nova Scotia. Use this document in combination with the *Key Steps to Responding to Privacy Breaches* document produced by the OIPC Nova Scotia and available at: http://foipop.ns.ca/sites/default/files/publications/Key%20Steps%20-%20Full%20-%20Final%20-%202015Oct27.pdf

Organization:
Date:

Author:

Index:

1. What is the purpose of the privacy breach management protocol?

The protocol allows the Board to identify, manage and resolve privacy breaches. It applies to all of the Board's information assets – such as personal information, personal health information, workforce personal information, and employee personal information. All workers at the Board must follow this protocol, including all full-time and part-time employees, contract employees, contractors, people on secondment, temporary workers and students.

2. What is a privacy breach?

A breach is any event that results in personal information in the custody or control of the Board being accessed, used, copied, modified, disclosed or disposed of in an unauthorized fashion, either deliberately or inadvertently.

Some examples of breaches include:

- A USB key with unencrypted personal information being lost or stolen.
- An excel spreadsheet containing employee benefit information being emailed to the wrong person.
- Employees inappropriately browsing data files containing personal information for non-work related purposes.
- Hacker engaging in malicious activity resulting in the compromise of the Board's personal information assets.

3. Roles and responsibilities

The following table summarizes the responsibilities of staff when a privacy breach is discovered.

Position	Responsibilities
• All staff	• Complete preliminary breach assessment report. (Appendix 1) and immediately report privacy breach to the Executive Director (as the designated Privacy Officer). • Immediately undertake containment efforts. • Assist with breach investigations as required.
• Executive Director	• Receive preliminary breach assessment reports. • Assess the preliminary report to determine whether a privacy breach has occurred. • Recommend immediate containment efforts. • Identify and contact individuals to form an Incident Response Team (as needed). • Conduct appropriate internal notifications of the breach. • Conduct a full assessment of the breach – complete the privacy breach checklist (Appendix 2).

	• With the Incident Response Team, determine whether notification of affected individuals is required. • In consultation with communications staff, complete notification. • Notify and liaise with the Information and Privacy Commissioner. • With the Incident Response Team, identify risk mitigation and prevention strategies. • Assign responsibility for completing mitigation and prevention strategies. Follow up to ensure actions are completed. • Conduct trend analysis of privacy breaches. • Keep executive informed of all actions and decisions of the Incident Response Team.
• Manager of IT	• Participate on Incident Response Teams when the privacy breach involves systems. • Assist in investigations as to the cause of system-related breaches. • Identify containment and prevention strategies. • Assist in implementation of containment and prevention strategies involving IT or security resources.
• Legal counsel	• Participate as required on the Incident Response Team. • Assist the Executive Director in assessing whether notification is required.
• Communications staff	• Assist in the drafting of breach notification letters.
• Labour relations/human resources staff.	• Assist in implementation of containment and prevention strategies that require cooperation of staff, particularly unionized staff.
• Office of primary responsibility – manager or supervisor	• Participate on Incident Response Team. • Assist in identifying containment, mitigation and prevention strategies. • Implement containment, mitigation and prevention strategies.
• Board Chair	• Receive and review all reports of privacy breaches. • Follow up with Executive Director to ensure that containment, notification and prevention actions have been completed.

4. Breach Management Process

Step 1: Preliminary Report, Assessment & Containment
Step 2: Full Assessment
Step 3: Notification
Step 4: Mitigation and Prevention
Step 5: Lessons Learned

Step 1: Preliminary Report, Assessment & Containment
When a suspected privacy breach occurs, the employee who discovers the breach must conduct a preliminary assessment to identify the nature of the breach and to identify potential containment steps.

Employees who discover potential breaches must:

- Immediately complete the Preliminary Breach Assessment Report (Appendix 1). The report assists employees in identifying a privacy breach and in identifying useful containment strategies. The preliminary report should be completed on the day the breach is discovered.
- Contact the Executive Director and provide a copy of the Preliminary Breach Assessment Report on the day the breach is discovered.
- Advise their supervisor of the potential privacy breach and of steps taken to contain the breach on the day the breach is discovered.

Supervisors and employees who discover potential breaches must:

- Take immediate action to contain the breach and to secure the affected records, systems, email or websites. Review the Preliminary Breach Assessment Report (Appendix 1) for suggested containment strategies.

Step 2: Full Assessment
Upon receipt of a notification of a potential privacy breach, the Executive Director must:

- Obtain a copy of the Preliminary Breach Assessment Report from the reporting employee (Appendix 1).
- Identify appropriate staff to form an Incident Response Team and organize an immediate meeting of the team.
- Identify breach containment strategies and assign responsibility for their implementation. Containment strategies should be identified and implemented on the day the breach is discovered.
- Conduct an investigation and complete the Privacy Breach Checklist including a risk assessment (Appendix 2). Conduct this step within one to five days of the breach.
- Based on the Privacy Breach Checklist and in consultation with the Incident Response Team, determine whether notification is appropriate and identify prevention strategies. Conduct this step within one to five days of the breach.
- Complete notification of affected individuals and notification of the Information and Privacy Commissioner. Conduct this step as soon as possible, generally within one to five days of the breach.

Step 3: Notification
The Executive Director, in consultation with the Incident Response Team (if any), will determine whether and to whom notification will be given. Notification is an important mitigation strategy that can benefit both the Board and the individuals affected by a breach. There are a number of individuals and organizations that may require notification:

(a) Internal officials: The Incident Response Team should identify appropriate officials within the Board who require notification of the breach.

(b) Affected individuals: If a breach creates a risk of harm to any individuals, those affected should be notified. The Privacy Breach Checklist (Appendix 2) includes an assessment for whether notification should occur and how notification should be completed. The Privacy Breach Checklist also identifies the information that must be included in any breach notification letter.

(c) Office of the Information and Privacy Commissioner
The Executive Director will notify the Office of the Information and Privacy Commissioner by phone, fax or email.

(d) Others
Appendix 2 includes a list of other organizations or individuals who may require notification depending on the facts of the breach. The Executive Director is responsible for implementing any notification decisions made by the Incident Response Team.

Caution: In responding to a privacy breach, be careful not to take steps that may exacerbate the existing breach or create a new one (i.e., disclosing additional personal information, notification letters addressed to the wrong person, notification letters that disclose information in the return address).

Step 4: Mitigation and Prevention
Once the immediate steps have been taken to mitigate the risks associated with the privacy breach and to provide appropriate notification, the Office of Primary Responsibility (the Office where the breach occurred), the Executive Director and the Incident Response Team (if any) must investigate the cause of the breach thoroughly, consider whether to develop a prevention plan and consider what that plan might include.

Mitigation and prevention strategies developed should reflect the significance of the breach and whether the breach was a systemic or isolated event. Mitigation and prevention plans may include the following:

Physical Controls
- Audit physical controls to identify outstanding weaknesses.
- Modify physical controls such as locks, alarms, security monitoring, or visitor access control to improve level of security.

Technical Controls
- Tighten restrictions on access to certain personal information based on roles, responsibilities and need to know.
- Encrypt personal information particularly on portable storage devices.
- Limit the ability to copy data to thumb drives.

- Limit access to non-work email.

Administrative Controls

- Review the enforcement of the Board's policies, directives and process for the protection of personal information throughout its lifecycle.
- Revise or develop internal procedures and policies to address shortcomings identified.
- Develop contractual clauses to deal with breaches of privacy by third party service providers.

Personnel Security Controls

- Training and education
- Coaching/mentoring
- Disciplinary actions (reprimands, suspension, reassignment, termination)
- Revoke privileges and/or user access to system or records

Step 5: Lessons Learned

The Executive Director will track all privacy breaches across the organization and will use that information to identify trends both in the types of breaches occurring and within each step of the privacy breach management process. Collecting this information can facilitate identifying underlying patters with respect to personal information handling practices and may prevent future breaches.

Appendix 1: Preliminary Privacy Breach Assessment Report	
Report Prepared by:	**Date:**
Email:	
Phone:	

A. Breach Identification and Containment

Instructions: Review the preliminary assessment list below. If you answer yes to any of the questions below, complete the remainder of this assessment report and immediately (same day) forward a copy of this report to the Executive Director.

Preliminary Assessment	Yes/ No	Suggested Containment Strategies
1. Was there an abuse of access privileges (e.g., unauthorized access or use of records that contain personal information)?		a) Immediately restrict, suspend or revoke access privileges until completion of the investigation. b) Determine whether personal information was further disclosed to others (verbally or via copies). c) Attempt to retrieve the documents in question, and document the steps taken. d) Complete this *Preliminary Report* and contact the Executive Director.
2. Was personal information inappropriately disclosed (e.g.,improper application of severances (material removed or blacked out), incomplete de-identification)?		a) Attempt to retrieve documents. b) Determine whether personal information was further disclosed to others (verbally or via copies). c) Document the steps taken. d) Complete this *Preliminary Report* and contact the Executive Director.
3. Was personal information lost (e.g., through the mail, during a move or on a misplaced electronic device)?		a) Attempt to retrace steps and find the lost document(s). b) Determine whether personal information was further disclosed to others (verbally or via copies). c) Document the steps taken. d) Conduct an inventory of the personal information that was or may have been compromised. e) Complete this *Preliminary Report* and contact the Executive Director.

Preliminary Assessment	Yes/ No	Suggested Containment Strategies
4. Was personal information stolen (e.g., theft of computer equipment or devices)?		a) Attempt to retrieve the stolen equipment or device. b) Document the steps taken. c) Complete this *Preliminary Report* and contact the Executive Director.
5. Was personal information in an unencrypted email sent to the wrong address?		a) Cease transmission of email or correspondence to the incorrect address. b) Determine whether the email address is incorrect in the system (e.g., programmed incorrectly into the system). c) Attempt to recall the message. d) Determine where the email went. e) Request that the recipient delete all affected email or correspondence, with confirmation via email that this has been done. f) Determine whether personal information was further disclosed to others (verbally or via copies). g) Document the steps taken. h) Complete this *Preliminary Report* and contact the Executive Director.
6. Was personal information faxed, mailed or delivered to a wrong address?		a) Determine where the document went. b) Determine whether the address is incorrect in the system (e.g.,programmed incorrectly into system). c) Request that the recipient return the document(s) if mailed, or request that the fax be destroyed, with confirmation that this has been done. d) Determine whether personal information was further disclosed to others (verbally or via copies). e) Document the steps taken. f) Complete this *Preliminary Report* and contact the Executive Director.
7. Did a third party compromise (hack into) a system that contains personal information?		a) Contact security and IT to isolate the affected system, disable the affected system, or disable the user account to permit a complete assessment of the breach and resolve vulnerabilities. b) Document the steps taken. c) Complete this *Preliminary Report* and contact the Executive Director.
8. Did the sale or disposal of equipment or devices that contain personal information occur without a complete and irreversible purging of the item before its sale or disposal?		a) Contact IT. b) Document the steps taken. c) Complete this *Preliminary Report* and contact the Executive Director.
9. Was there an inappropriate display of personal information clearly visible to employees or clients? (e.g., posting of medical appointments or types of		a) Remove, move or segregate exposed information or files. b) Preserve evidence. c) Determine whether personal information was further disclosed to others (verbally or via copies). d) Document the steps taken.

Preliminary Assessment	Yes/ No	Suggested Containment Strategies
leave, home telephone numbers, slides of PowerPoint presentations that contain personal information, etc.)?		e) Complete this *Preliminary Report* and contact the Executive Director.
10. Was there an inappropriate collection of personal information?		a) Determine whether personal information was further disclosed to others (verbally or via copies). b) Complete this *Preliminary Report* and contact the Executive Director.
11. Was there an unexpected or unintended use of collected data? Is there a risk for re-identification of an affected individual or another identifiable individual?		a) Determine whether personal information was further disclosed to others (verbally or via copies) b) Complete this *Preliminary Report* and contact the Executive Director.
12. Was there an improper or unauthorized creation of personal information?		a) Complete this *Preliminary Report* and contact the Executive Director.
13. Was there an improper or unauthorized retention of personal information?		a) Complete this *Preliminary Report* and contact the Executive Director.
14. Remarks/Other:		

B. Breach Details		
1. Date(s) of breach:	2. Time of breach:	3. Location of breach:
4. When and how was the breach discovered?		
5. Provide a brief description of the breach (what happened, how it happened, etc.):		
6. Identify the person whose information was compromised (name and personal record identifiers, if applicable). If information regarding more than one person was compromised, please attach a list.		7. Is/are the affected individual(s) aware of the breach? __ Yes __ No Whether yes or no, request direction from the Executive Director or the OIPC.
8. Format of information involved: ____ Electronic records ____ Paper records ____ Other (describe): _____	9. What information was involved (check all that apply): ____ Medical _____ Employee ____ Other (describe): _____	
10. List the immediate containment actions and/or interventions, if any:		
11. Is there information or evidence to support the allegation of the breach? If yes, please specify:		
12. Has your supervisor been notified of the breach? __ Yes __ No		
C. Please name the person(s) directly involved in this breach (witnesses, investigator, individual who may have caused the breach, victims, etc.). Attach a list if necessary.		
1. Name	Title/Position	Contact information:
2. How was this person involved?		
3. Name	Title/Position	Contact information:
4. How was this person involved?		

Send this form immediately to the Executive Director at [insert contact information – email & phone #]

Appendix 2: Privacy Breach Checklist

Use this checklist to evaluate your response to a privacy breach and to decide whether or not to report the breach to the Office of the Information and Privacy Commissioner.[9] For a further explanation of how to manage a privacy breach see *Key Steps to Responding to Privacy Breaches* available at: http://foipop.ns.ca.

Date of report: _____

Date breach initially discovered: _____

Contact information:

Public Body/Health Custodian/Municipality: _____

Contact Person (Report Author): _____

Title: _____

Phone: _____ Fax: _____

E-Mail: _____

Mailing Address: _____

Incident Description

Describe the nature of the breach and its cause. How was the breach discovered and when? Where did it occur?

_____

_____

_____

_____

[9] The OIPC can be reached by phone at 902-424-4684 or 1-866-243-1564, by fax at (902) 424-8303 and by email at oipcns@novascotia.ca.

Steps 1 & 2: Containment & Risk Evaluation

Answer each of the following questions and then, based on those answers, complete the risk evaluation summary on page 15.

(1) Containment

Check all of the factors that apply:

- ❑ The personal information has been recovered and all copies are now in our custody and control.
- ❑ We have confirmation that no copies have been made.
- ❑ We have confirmation that the personal information has been destroyed.
- ❑ We believe (but do not have confirmation) that the personal information has been destroyed.
- ❑ The personal information is encrypted.
- ❑ The personal information is not encrypted.
- ❑ Evidence gathered so far suggests that the incident was likely a result of a systemic problem.
- ❑ Evidence gathered so far suggests that the incident was likely an isolated incident.
- ❑ The personal information has not been recovered but the following containment steps have been taken (check all that apply):
    - ❑ The immediate neighbourhood around the theft has been thoroughly searched.
    - ❑ Used item websites are being monitored but the item has not appeared so far.
    - ❑ Pawn shops are being monitored.
    - ❑ A remote wipe signal has been sent to the device but no confirmation that the signal was successful has been received.
    - ❑ A remote wipe signal has been sent to the device and we have confirmation that the signal was successful.
    - ❑ Our audit confirms that no one has accessed the content of the portable storage device.
    - ❑ We do not have an audit that confirms that no one has accessed the content of the portable storage device.
    - ❑ All passwords and system user names have been changed.

Describe any other containment strategies used:

_____

_____

_____

_____

(2) Nature of Personal Information Involved

List all of the data elements involved (e.g., name, date of birth, SIN, address, medical diagnoses, connection with identified service provider such as welfare or counselling, etc.)

- ❑ Name
- ❑ Address
- ❑ Date of birth
- ❑ Government ID number (specify) _____
- ❑ SIN
- ❑ Financial information
- ❑ Medical information
- ❑ Personal characteristics such as race, religion, sexual orientation
- ❑ Other (describe)

_____

_____

_____

_____

(3) Relationship

What is the relationship between the recipient of the information and the individuals affected by the breach?

- ❑ Stranger
- ❑ Friend
- ❑ Neighbour
- ❑ Ex-partner
- ❑ Co-worker
- ❑ Unknown
- ❑ Other (describe)

_____

_____

_____

_____

(4) Cause of the Breach

Based on your initial investigation of the breach, what is your best initial evaluation of the cause of the breach?

- ❑ Accident or oversight
- ❑ Technical error
- ❑ Intentional theft or wrongdoing
- ❑ Unauthorized browsing
- ❑ Unknown
- ❑ Other (describe)

_____

_____

_____

(5) Scope of the Breach

How many people were affected by the breach?

- ❑ Very few (less than 10)
- ❑ Identified and limited group (>10 and <50)
- ❑ Large number of individuals affected (>50)
- ❑ Numbers are not known

(6) Foreseeable Harm

Identify the types of harm that may result from the breach. Some relate strictly to the affected individual; but harm may also be caused to the public body and other individuals if notifications do not occur:

- ❑ **Identify theft** (most likely when the breach includes loss of SIN, credit card numbers, driver's licence numbers, debit card information, etc.)
- ❑ **Physical harm** (when the information places any individual at risk of physical harm from stalking or harassment)
- ❑ **Hurt, humiliation, damage to reputation** (associated with the loss of information such as mental health records, medical records, disciplinary records)
- ❑ **Loss of business or employment opportunities** (usually as a result of damage to reputation to an individual)
- ❑ **Breach of contractual obligations** (contractual provisions may require notification of third parties in the case of a data loss or privacy breach)
- ❑ **Future breaches due to technical failures** (notification to the manufacturer may be necessary if a recall is warranted and/or to prevent a future breach by other users)
- ❑ **Failure to meet professional standards or certification standards** (notification may be required to a professional regulatory body or certification authority)
- ❑ **Other** (specify)

  _____

(7) Other Factors

The nature of the public body's relationship with the affected individuals may be such that the public body wishes to notify no matter what the other factors are because of the importance of preserving trust in the relationship. Consider the type of individuals that were affected by the breach.

- ❑ Client/customer/patient
- ❑ Employee
- ❑ Student or volunteer
- ❑ Other (describe)

_____

Risk Evaluation Summary:

For each of the factors reviewed above, determine the risk rating.

Risk Factor	**Risk Rating**		
	Low	Medium	High
1) Containment			
2) Nature of the personal information			
3) Relationship			
4) Cause of the breach			
5) Scope of the breach			
6) Foreseeable harm from the breach			
7) Other factors			
Overall Risk Rating			

Use the risk rating to help decide whether notification is necessary and to design your prevention strategies. Foreseeable harm from the breach is usually the key factor used in deciding whether or not to notify affected individuals. Step 3 below analyzes this in more detail. In general though, a medium or high risk rating will always result in notification to the affected individuals. A low risk rating may also result in notification depending on the unique circumstances of each case.

Step 3: Notification

(1) Should affected Individuals be Notified?

Once you have completed your overall risk rating, determine whether or not notification of affected individuals is required. If any of the following factors apply, notification should occur. If the *PHIA* test is satisfied, notification must occur.

Consideration	Description	Factor applies
Legislation	Health custodians in Nova Scotia must comply with sections 69 & 70 of *PHIA* which require notification.	
Risk of identity theft	Most likely when the breach includes loss of SIN, credit card number, driver's licence number, debit card information, etc.	
Risk of physical harm	When the information places any individual at risk of physical harm from stalking or harassment.	
Risk of hurt, humiliation, damage to reputation	Often associated with the loss of information such as mental health records, medical records or disciplinary records.	
Loss of business or employment opportunities	Where the breach could affect the business reputation of an individual.	
Explanation required	The public body may wish to notify if the affected individuals include vulnerable individuals, or where individuals require information to fully understand the events, even when the risks have been assessed as low.	
Reputation of public body	Where the public body is concerned that the breach will undermine trust of citizens, the public body may decide to notify in order to ease concerns and to provide clear information regarding the risks and mitigation strategies undertaken, even when risks assessed are low.	

(2) When and How to Notify

When: Notification should occur as soon as possible following a breach. However, if you have contacted law-enforcement authorities, you should determine from those authorities whether notification should be delayed in order not to impede a criminal investigation.

How: The preferred method is direct – by phone, letter, email or in person. Indirect notification via website information, posted notices or media should generally only occur where direct notification could cause further harm, is prohibitive in cost, or contact information is lacking. Using multiple methods of notification in certain cases may be the most effective approach.

Considerations Favouring Direct Notification	**Check If Applicable**
The identities of individuals are known.	
Current contact information for the affected individuals is available.	
Individuals affected by the breach require detailed information in order to properly protect themselves from the harm arising from the breach.	
Individuals affected by the breach may have difficulty understanding an indirect notification (due to mental capacity, age, language, etc.).	
Considerations Favouring Indirect Notification	
A very large number of individuals are affected by the breach, such that direct notification could be impractical.	
Direct notification could compound the harm to the individuals resulting from the breach.	

(3) What to Include in Breach Notification Letters

The information included in the notice should help the individual to reduce or prevent the harm that could be caused by the breach. Include all of the information set out below:

Essential Elements in Breach Notification Letters	**Included**
Date of breach	
Description of breach	
Description of personal information affected	
Steps taken so far to control or reduce harm (containment)	
Future steps planned to prevent further privacy breaches	
Steps individuals can take - consider offering credit monitoring where appropriate	
Information and Privacy Commissioner's contact information – Individuals have a right to complain to the Information and Privacy Commissioner	
Public body, municipality or health custodian contact information – for further assistance	

(4) Others to Contact

Authority or Organization	Reason for Contact	Applicable
Law-enforcement	If theft or crime is suspected	
Information and Privacy Commissioner for Nova Scotia	• For assistance with developing a procedure for responding to the breach, including notification to ensure steps taken comply with obligations under privacy legislation • The personal information is sensitive • There is a risk of identity theft or other significant harm • A large number of people are affected • The information has not been fully recovered • The breach is a result of a systemic problem or a similar breach has occurred before	
Professional or regulatory bodies	If professional or regulatory standards require notification of the regulatory or professional body	
Insurers	Where required in accordance with an insurance policy	
Technology suppliers	If the breach was due to a technical failure and a recall or technical fix is required	

Confirm notifications completed

Key contact	Notified
Privacy officer within your public body, municipality or health custodian	
Police (as required)	
Affected individuals	
Information and Privacy Commissioner for Nova Scotia	
Professional or regulatory body – identify:	
Technology suppliers	
Others (list):	

Step 4: Prevention

Once the immediate steps are taken to mitigate the risks associated with the breach, you need to take the time to thoroughly investigate the cause of the breach. This could require a security audit of both physical and technical security. As a result of this evaluation, you should develop or improve as necessary adequate long-term safeguards against future breaches.

Consider making improvements in each of the following areas listed below. Also, take the opportunity to revisit your privacy management framework,[10] and assess if any further adjustments are necessary as part of your prevention strategy.

Physical Controls
What physical controls were in place at the time of the breach? Describe any modifications to physical controls such as locks, alarms, security monitoring, or visitor access control.

Technical Controls
Was there an IT security strategy in place at the time of the breach? Describe any modification to technical controls intended to prevent future similar breaches.

Administrative Controls
Administrative controls refer to the procedural safeguards implemented for safe handling of personal information, which includes the enforcement of an institution's policies, directives and processes for the protection of personal information throughout its lifecycle. Describe the administrative controls in place at the time of the breach. Describe improvements made to administrative controls in response to the breach. If you do not already have a privacy breach protocol in place, ensure that one is developed as part of your plan.

Personnel Security Controls
Personnel security controls refer to a public body's (or health custodian's) management of its employees – suitability, proper training, supervision and disciplinary procedures. What personnel security controls were in place at the time of the breach - for example, security clearances, confidentiality agreements and privacy training requirements? What steps have been taken to improve personnel security controls in this particular case and in general to prevent future similar breaches?

[10] For information on what constitutes a privacy management framework visit the tools tab on the Office of the Information and Privacy Commissioner website at: http://foipop.ns.ca.

Appendix C
Privacy Impact Assessment Template and Guide

Note: Attach supporting documentation as necessary

1. Introduction

a) Name of Program or Service
b) Name of Group Responsible
c) Name of Program or Service lead
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:

(Signature and title) Date

Reviewed by:

Executive Director Date

Approved by:

Chair 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 Group Responsible (at the Board)

3. Name of Program or Service Lead (the project leader at the Board)

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)

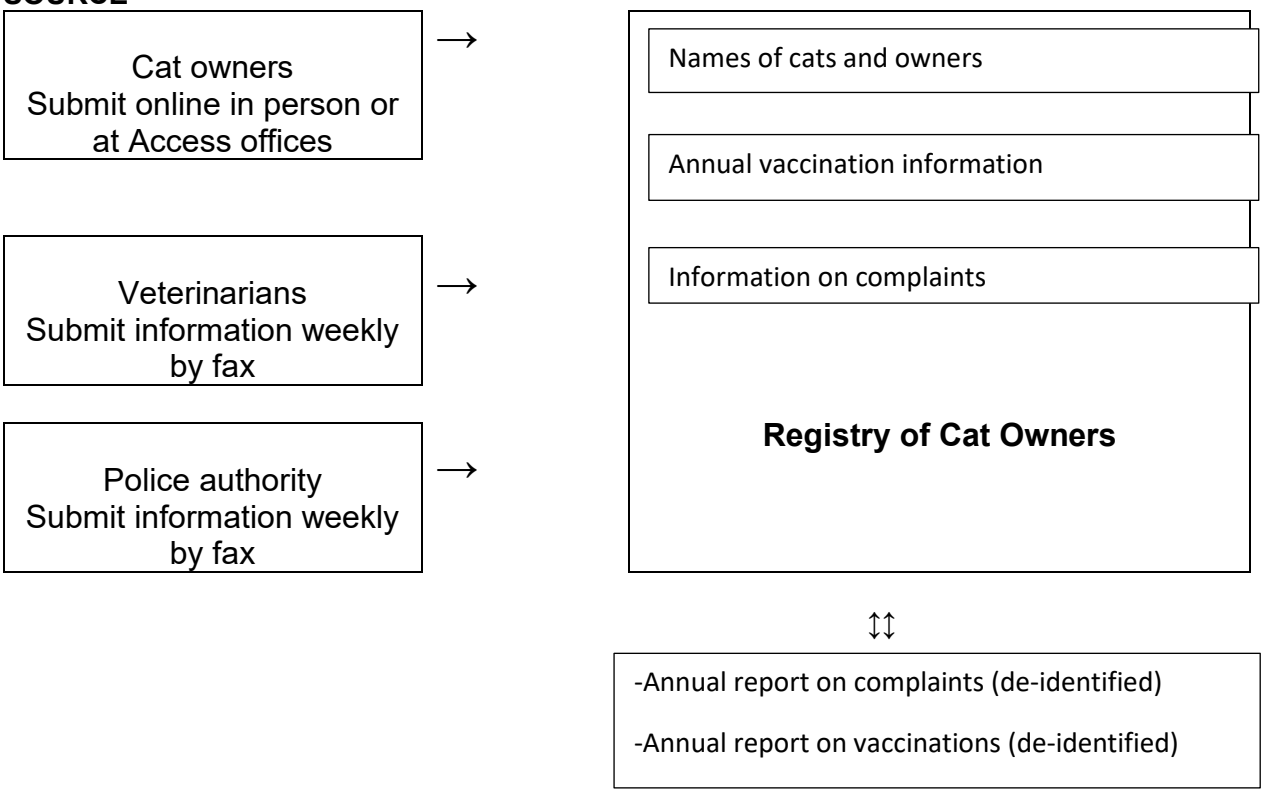
- Identify and describe the types of applications, platforms, and external entities involved in the information flow. Describe their interfaces, services, and the context within which the entities interoperate.

- 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 if 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.

<u>Mock example</u>: 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.

<u>3. Collection, Use and Disclosure of Personal Information</u>

<u>NOTE</u>: 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	Disclose 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 of 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 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:

(Signature and title) Date

Reviewed by:

Executive Director Date

Approved by:

Chair 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 27of 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 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 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.