



Chief Privacy Officer Toolkit

Office of the Information and Privacy Commissioner for
Nova Scotia



Notice to Users

This document is intended to provide general information only. It is important to read the full legislation not just the sections summarized to understand the full extent of the provision. This document is not intended nor can it be relied upon as legal advice. As an independent agency mandated to oversee compliance with *FOIPOP*, *MGA* and *PHIA* the Office of the Information and Privacy Commissioner for Nova Scotia cannot approve in advance any proposal from a public body, municipality or health custodian. We must maintain our ability to investigate any complaints and to provide recommendations in response to these complaints. The contents of this document do not fetter or bind this office with respect to any matter, including any complaint investigation or other matter respecting which the Information and Privacy Commissioner for Nova Scotia will keep an open mind. It remains the responsibility of each public body, municipality and health custodian to ensure that they comply with their responsibilities under the relevant legislation. Visit us at: <https://oipc.novascotia.ca>

Contents

Chief Privacy Officer Toolkit	
	Tab
Chief Privacy Officer Checklist	
Chief Privacy Officer Checklist – The First Six Months	1
Privacy Management Program	
Privacy Management Program Overview	2
Privacy Management Program Gap Analysis for Chief Privacy Officers	3
Training	
Training Deck: Access & Privacy Basics for Staff	4
Five Minute Privacy Checkup	5
Security	
Reasonable Security Checklist	6
Privacy Impact Assessments	
Privacy Impact Assessment (PIA) Template	7
Breach Management	
Four Key Steps to Responding to Privacy Breaches	8
Privacy Breach Management Protocol Template	9
Resources	
Resources <ul style="list-style-type: none">• Privacy Rules at a Glance• Useful Websites	10



Tab 1



Chief Privacy Officer Checklist – The First Six Months

Office of the Information and Privacy Commissioner for Nova Scotia

Task	✓
1. Communicate your role to staff <ul style="list-style-type: none"> Send out communications to all staff explaining the key responsibilities of your role as Chief Privacy Officer including: <ul style="list-style-type: none"> act as primary point of contact for all privacy related concerns and issues; advocate for compliance with privacy obligations within the public body; coordinate with other appropriate persons responsible for related disciplines and functions within the public body and your access & privacy group; establish and implement program controls; lead the public body's privacy breach investigations; and, represent the public body in the event of a complaint investigation by the Office of the Information and Privacy Commissioner for Nova Scotia (OIPC). 	
2. Engage your executive <ul style="list-style-type: none"> Develop an executive reporting strategy and regularly report identified risks, strategies and outcomes. 	
3. Ensure all staff receive privacy training <ul style="list-style-type: none"> Lead privacy training initiatives within the public body. <ul style="list-style-type: none"> Ensure all staff receive annual appropriate privacy training. Monitor training of all staff and report outcomes to executive. Resource: OIPC NS has a 30-minute access and privacy essentials deck you can use to provide basic access and privacy training to all staff. Contact us at oipecns@novascotia.ca. 	
4. Complete Chief Privacy Officer training <ul style="list-style-type: none"> The CPO will need to be familiar with the privacy rules in Nova Scotia, how to build a privacy management program and how to manage a privacy breach. Resource: The Office of the Information and Privacy Commissioner has a training program for Chief Privacy Officers on key responsibilities and how to conduct a privacy management gap analysis. Contact us at oipecns@novascotia.ca. 	
5. Conduct a personal information inventory <ul style="list-style-type: none"> Lead a project to inventory the size, sensitivity and location of all personal information collections. Once the inventory is complete, lead a project to assess the security and privacy risks associated with each collection. Tool: A <i>Reasonable Security Checklist for Personal Information</i> is available on the OIPC website at https://oipc.novascotia.ca. 	
6. Complete a gap analysis of your public body's privacy management program <ul style="list-style-type: none"> Evaluate the strength of your public body's privacy management program. Develop a plan to address identified weaknesses. Tool: <i>Privacy Management Program Gap Analysis</i> for large and small public bodies is available on the OIPC website at https://oipc.novascotia.ca. 	



Tab 2



Office of the Information and Privacy Commissioner for Nova Scotia

Privacy Management Program Overview¹

A. Building Blocks		
Public Body Commitment	Executive-level support	Senior executive-level management support is key to a successful privacy management program and essential for a privacy respectful culture. Core elements of support include approval of adequate funding and regular review of reports.
	Privacy Officer	<ul style="list-style-type: none"> • Role is defined and is fundamental to business decision-making process. • Role and responsibilities for monitoring compliance are clearly identified and communicated throughout the public body. • Responsible for the development and implementation of the program controls and their ongoing assessment and revision. • Adequate resources are identified. • Public body, municipality or health custodian structure supports the ability of staff to monitor compliance and foster a culture of privacy within the public body. • Ensures privacy protection is built into every major function involving the use of personal information.
	Reporting	Reporting mechanisms should be established and they need to be reflected in the public body's program controls.
Program Controls	Personal Information Inventory	The public body, municipality or health custodian is able to identify: <ul style="list-style-type: none"> • The personal information in its custody or control, • Its authority for the collection, use and disclosure of personal information and • The sensitivity of the personal information.
	Policies	<ul style="list-style-type: none"> • Privacy policy • How to request access or correction • Complaints policy
	Risk assessment tools	<ul style="list-style-type: none"> • Privacy impact assessments • System risk and threat assessments
	Training	<ul style="list-style-type: none"> • Privacy basics for all staff • Privacy breach training for all staff • Advanced and refresher training as required
	Breach management protocols	<ul style="list-style-type: none"> • Privacy breach policy • Breach notification assessment tool • Breach management protocol
	Service provider management	<ul style="list-style-type: none"> • Have standard clauses available to ensure service provider compliance with privacy law requirements & monitor compliance.
	Communication	<ul style="list-style-type: none"> • Inform individuals of their rights & the public body's policies

¹ These materials are based on the paper, "Getting Accountability Right with a Privacy Management Program" prepared by the Office of the Information and Privacy Commissioner of Alberta, the Office of the Privacy Commissioner of Canada and the Office of the Information and Privacy Commissioner of British Columbia.

B. Ongoing Assessment and Revision		
Oversight & Review Plan	Develop an oversight and review plan	Privacy Officer should develop an oversight and review plan on an annual basis that sets out how she will monitor and assess the effectiveness of the public body's program controls.
Assess and Revise Program Controls	Updates and revisions	<ul style="list-style-type: none"> • Update personal information inventory • Revise policies • Treat risk assessment tools as evergreen • Modify training and education • Adapt breach and incident response protocols • Fine-tune service provider management

For a more detailed explanation of each of the elements of a privacy management program see, *Getting Accountability Right With a Privacy Management Program* available at:
<https://www.oipc.bc.ca/guidance-documents/1435>



Tab 3



Office of the Information and Privacy Commissioner for Nova Scotia

Privacy Management Program Gap Analysis For Chief Privacy Officers

Freedom of Information and Protection of Privacy Act and Municipal Government Act Part XX

Introduction:

This document was developed by the Information and Privacy Commissioner for Nova Scotia¹ and is intended to assist Chief Privacy Officers and Privacy Champions in public bodies and municipalities with developing and implementing a robust privacy management program. An overview of the elements of a robust privacy management program is contained in *Privacy Management Program At-a-Glance* on the Office of the Information and Privacy Commissioner for Nova Scotia's website at: <https://oipc.novascotia.ca>. This Gap Analysis document provides detailed information about each of the elements of a privacy management program. The goal of the Gap Analysis is to identify shortcomings in the program. The Gap Analysis results should then be used to develop a privacy oversight and review plan that addresses each of the identified gaps.

We have developed privacy management program tools and gap analysis worksheets for health custodians and smaller municipalities. Check the Tools & Guidance section of our website for these materials.

Contact Us:

If you have any questions or comments with respect to this document please contact us at:

Office of the Information and Privacy Commissioner for Nova Scotia
PO Box 181
Halifax, NS B3J 2M4
Phone: 902-424-4684 Toll Free: 1-866-243-1564

¹ The Information and Privacy Commissioner for Nova Scotia is also known as the Review Officer and is appointed as the oversight authority under the *Freedom of Information and Protection of Privacy Act*, the *Municipal Government Act*, the *Personal Health Information Act* and the *Privacy Review Officer Act*.

Instructions:

This gap analysis tool begins with a Gap Analysis Summary document (page 3). When complete this will serve as a one page summary of your review results. Your goal is to develop a visual gap analysis by assigning red, yellow or green to the outcome of your assessment for each of the elements of your privacy management program (“PMP”)

Step 1: Begin by assessing the two categories of building blocks: organizational commitment and program controls. Within each category are a series of requirements. For each requirement we have provided a list of essential elements. So, for example the Organizational Commitment requirement for buy-in from the top lists three requirements from senior management (see page 4). Record your evaluation of each element by describing the current state of affairs in your organization. Be as honest and critical as you can. The goal here is to accurately state your organization’s current status.

Step 2: For each requirement score your organizations compliance on a scale of 1 to 3. Feel free to give partial points. Ratings are explained below.

Step 3: Average the score for the elements of each requirement to come up with an overall score that you will record in the overall rating row.

Step 4: Record the overall score then assign a colour to it and record the colour on the summary sheet at page 3. Colour ratings are explained below.

Step 5: Once you have completed all of your ratings, review the summary sheet at page 3 and develop a plan to move all of your ratings to green (a privacy oversight and review plan).

Sample – Gap Analysis Summary	
PMP Requirement	Overall Gap Analysis Rating
Building Blocks – Organizational Commitment	
a. Buy-in from the Top	1.9
b. Privacy Officer	2.2
c. Privacy Office	2.6
d. Reporting	2.7
Building Blocks – Program Controls	
a. Personal Information Inventory	1.3
b. Policies	1.8
c. Risk Assessment Tools	2.1
d. Training and Education Requirements	2.0
e. Breach and Incident Management Protocols	2.7
f. Service Provider Management	1.4
g. External Communication	1.5
Ongoing Assessment and Revision – Oversight and Review Plan	
a. Develop Oversight and Review Plan	2.0
Ongoing Assessment and Revision – Program Controls	
a. General Requirements	2.2
b. Update Personal Information Inventory	1.6
c. Revise Policies	2.5
d. Treat Risk Assessment Tools as Evergreen	1.9
e. Modify Training and Education	2.8
f. Adapt Breach and Incident Response Protocols	2.2
g. Fine-tune Service Provider Management	2.1
h. Improve External Communication	1.7

Gap Analysis Summary	
PMP Requirement	Overall Gap Rating
Building Blocks – Organizational Commitment	
a. Buy-in from the Top	
b. Privacy Officer	
c. Privacy Office	
d. Reporting	
Building Blocks – Program Controls	
a. Personal Information Inventory	
b. Policies	
c. Risk Assessment Tools	
d. Training and Education Requirements	
e. Breach and Incident Management Protocols	
f. Service Provider Management	
g. External Communication	
Ongoing Assessment and Revision – Oversight and Review Plan	
a. Develop Oversight and Review Plan	
Ongoing Assessment and Revision – Program Controls	
a. General Requirements	
b. Update Personal Information Inventory	
c. Revise Policies	
d. Treat Risk Assessment Tools as Evergreen	
e. Modify Training and Education	
f. Adapt Breach and Incident Response Protocols	
g. Fine-tune Service Provider Management	
h. Improve External Communication	

Gap Analysis Ratings & Colour Ratings for Summary Chart

Rating	Colour Code	Rating Description
1.0 – 1.9	Red	Little to no evidence of compliance - documented or in practice.
2.0 – 2.5	Yellow	No documented evidence of compliance but some evidence of effective practice in compliance or documented practice requirement with only limited evidence of implementation.
2.6 – 3.0	Green	Documented and substantial practical compliance.

Building Blocks – Organizational Commitment		
List of Expectations	Evidence of Compliance	Gap Rating
a. Buy-in from the Top	Overall Rating	
1. Senior management (e.g. CAO, DM) endorses the program controls (policies, risk assessments, training).		
2. Senior management provides resources that the privacy management program needs to succeed.		
3. Senior management monitors program through regular reporting from Privacy Officer.		
b. Privacy Officer/Privacy Champion	Overall Rating	
4. A senior manager (Director or above) is assigned responsibility for overseeing the organization's compliance.		
c. Privacy Office	Overall Rating	
5. Privacy Officer is supported by dedicated staff.		
6. Role of the privacy office is defined.		
7. Staff have delegated responsibilities to monitor compliance.		
8. Staff foster a culture of privacy within the organization. Staff work to ensure that privacy protection is built into every major function involving the use of personal information including policies, programs, contracts, legislation, regulations, IT systems, communication, etc. For example, practice of regularly conducting PIAs & STRAs for all new systems, projects and programs, mandatory privacy review for all new policies, contracts (beginning at the RFP stage), regular privacy training.		

Building Blocks – Organizational Commitment		
List of Expectations	Evidence of Compliance	Gap Rating
d. Reporting	Overall Rating	
9. There are privacy reporting mechanisms that ensure that the right people know how the privacy management program is structured. (Consider <u>practices</u> in response to privacy breaches and privacy complaints).		
10. Reporting mechanisms are reflected in the organization's program controls. For example, the privacy policy, breach management protocol and standard contract language all include requirements to report incidents or avenues of complaints to the privacy office or officer.		
11. An internal privacy audit and assurance program monitors compliance with privacy policies and monitors the breach escalation procedure to ensure that necessary steps are taken when triggered.		
12. An escalation procedure has been clearly defined and explained to all employees for privacy breaches or when a citizen makes a privacy complaint. (This may be reflected only in practice and may or may not be reflected in existing policies and protocols.)		

Building Blocks – Program Controls		
a. Personal Information Inventory		Overall Rating
1. The organization has completed a personal information inventory or equivalent.		
2. The organization is able to identify: (i) The type of personal information that it holds. (ii) Where the personal information is held. (iii) Why/how it is collecting personal information (iv) Uses of personal information. (v) Why/to whom it is disclosing personal information. (vi) The sensitivity and/or classification of personal information		
b. Policies		Overall Rating
3. Five key <u>policies</u> are in place (they may be in one comprehensive policy or in multiple policy documents): (i) Collection, use, disclosure of personal information including purpose for collection, use & disclosure and authorities		
(ii) Access to and correction of personal information.		
(iii) Retention and disposal of personal information (approved records retention schedule).		
(iv) Responsible use of information and information technology including administrative, physical and technological security controls and appropriate access controls.		
(v) Challenging compliance (privacy complaint policy).		
c. Risk Assessment Tools		Overall Rating
4. Privacy impact assessments (PIAs) are required throughout the organization for all new projects, programs or systems involving personal information and on any new collection use or disclosure of personal information.		
5. Security & threat and risk assessments (STRAs) are required for all systems involving personal information.		
6. Procedures have been developed for conducting such assessments and a review and approval process has been developed that involves the privacy office when designing new initiatives, services or programs.		

Building Blocks – Program Controls continued		
List of Expectations	Evidence of Compliance	Gap Rating
d. Training and Education Requirements	Overall Rating	
7. All employees receive general privacy protection training.		
8. Privacy training is mandatory for all new employees.		
9. Training processes are documented and participation and success are measured.		
10. Individuals who handle personal information directly receive additional training specifically tailored to their roles.		
11. Training and education are recurrent and the content of the program is periodically revisited and updated to reflect changes.		
e. Breach and Incident Management Response Protocols	Overall Rating	
12. There is a procedure for the management of personal information breaches.		
13. There is a person responsible for managing a breach.		
14. Responsibilities for internal and external reporting of the breach are defined (usually through an approved breach management protocol).		
f. Service Provider Management	Overall Rating	
15. Contractual or other means are in place to protect personal information.		
16. Sensitivity of personal information is addressed in service provider arrangements.		
17. Privacy requirements for service providers include:		
(i) Compliance requirement such as binding the service provider to the policies and practices of the organization and requiring breach notification.		
(ii) Training and education for all service provider employees with access to personal information.		
(iii) Restrictions on sub-contracting.		
(iv) Audits by the public body or municipality.		
(v) Agreements with service provider employees stating that they will comply with the organization's privacy policies and protocols.		
(vi) Restrictions on transborder data flows		

Building Blocks – Program Controls continued		
List of Expectations	Evidence of Compliance	Gap Rating
g. External Communication	Overall Rating	
18. There is a procedure for informing individuals of their privacy rights and program controls. (Through published privacy policies or clear notices).		
19. The external communication is clear and understandable and not simply a reiteration of the law.		
20. External communication: <ul style="list-style-type: none"> (i) Provides enough info so that individuals know the purpose of the collection, use and disclosure of personal information and how it is safeguarded and how long it is retained. (ii) Notifies individuals if their personal information is being transferred outside of Canada. (iii) Includes information on who to contact with questions or concerns about the management of personal information. (iv) Is easily available to individuals. (v) Individuals are aware of how to access & correct their personal information. (vi) Individuals are aware of how to complain including the right to submit a complaint to the Information and Privacy Commissioner for Nova Scotia. 		

Ongoing Assessment and Revision (Privacy Brand Management) Oversight and Review Plan		
List of Expectations	Evidence of Compliance	Gap Rating
a. Develop Oversight and Review Plan		Overall Rating
1. The Privacy Officer develops an oversight and review plan on an annual basis that sets out how the privacy management program's effectiveness will be monitored and assessed.		
2. The plan establishes performance measures.		
3. The plan includes a schedule of when all policies and other program controls will be reviewed.		
Assess & Revise Program Controls		
a. General Requirements		Overall Rating
1. The effectiveness of program controls are monitored periodically, audited and revised where necessary.		
2. The monitoring addresses the following: (i) The latest threats and risks. (ii) Whether program controls are addressing new threats. (iii) Whether program controls are reflecting the latest compliance audit findings or guidance of the privacy commissioners. (iv) Whether new services being offered involve increased collection, use or disclosure of personal information. (v) Whether training is occurring and if it is effective. (vi) Whether policies and procedures are being followed. (vii) Whether the privacy management program is up to date.		
3. Problems identified during monitoring are documented and addressed.		
4. The Privacy Officer conducts periodic assessments to ensure key processes are being respected (eg. that mandatory PIAs and STRAs are conducted).		
5. The organization has developed metrics to gauge progress with respect to compliance.		

Assess & Revise Program Controls continued		
List of Expectations	Evidence of Compliance	Gap Rating
b. Update Personal Information Inventory	Overall Rating	
6. The personal information inventory is kept current.		
7. New collections of personal information are identified and evaluated.		
8. New uses of personal information are identified and evaluated.		
c. Revise Policies	Overall Rating	
9. Policies are reviewed and revised as needed, following assessments or audits, in response to a breach or complaint, new guidance, industry-based best practices or as a result of environmental scans.		
d. Treat Risk Assessment Tools as Evergreen	Overall Rating	
10. Privacy impact assessments are treated as evergreen documents so that the privacy and security risks of changes or new initiatives within the organization are always identified and addressed.		
11. Security threat and risk assessments are treated as evergreen documents so that the privacy and security risks of changes or new initiatives within the organization are always identified and addressed.		
e. Modify Training and Education	Overall Rating	
12. Training and education programs are reviewed and modified on a periodic basis as a result of ongoing assessments.		
13. Changes to program controls are effectively communicated to employees as they are made, or in “refreshed” education and training modules.		

Assess & Revise Program Controls continued		
List of Expectations	Evidence of Compliance	Gap Rating
f. Adapt Breach and Incident Response Protocols	Overall Rating	
14. Breach and incident management response protocols are reviewed and revised to implement best practices or recommendations.		
15. The breach and incident response protocol is reviewed and revised to implement lessons learned from post-incident reviews.		
g. Fine-tune Service Provider Management	Overall Rating	
16. Contracts with service providers are reviewed and, where necessary, fine-tuned.		
h. Improve External Communication	Overall Rating	
17. External communications explaining privacy policies are reviewed, updated and clarified as needed.		



Tab 4

Training for Staff

Access & Privacy Rules: The Basics

See the PowerPoint slides provided separately. The slides include note pages to guide the presenter through this 30 minute presentation intended to provide staff with some very basic information about the access and privacy rules in the *Freedom of Information and Protection of Privacy Act*. The notes include text in red. This text needs to be modified – usually it is a place to input a name – such as the name of the Chief Privacy Officer or *FOIPOP* contact.

As part of the presentation, staff are asked to complete the *5 Minute Privacy Checkup* (mentioned on slide 14) which is also provided on the next two pages.



Tab 5

5 Minute Privacy Checkup

As an employee of a public body, municipality or health custodian, you should be aware of your responsibilities to keep personal & sensitive information secure. Current privacy standards require that public bodies, municipalities and health custodians protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

This 5-minute privacy checkup asks a series of questions relating to the security of personal information and sensitive business information both hard copy and electronic. A “no” answer to any of these questions is a warning sign that the information may not be secure.

Physical Security		
	Y	N
Do you have files containing sensitive information stored in your office? <ul style="list-style-type: none">• If yes, is the sensitive information stored in a locked filing cabinet?• Do you lock your office door whenever you leave the office?		
At the end of the day do you always: <ul style="list-style-type: none">• Clear your desktop of all files containing sensitive information?• Store your laptop and all files in a locked filing cabinet?• Lock your office door?• Log off your computer?• Remove all documents containing sensitive information from faxes and printers?		
Email & Faxing		
Before emailing sensitive information do you: <ul style="list-style-type: none">• Ensure that either the owner of the sensitive information has consented to transmission via email or that the information is encrypted?• Always attach a confidentiality notice?		
Before faxing any sensitive information do you: <ul style="list-style-type: none">• Only send from a secure fax machine?• Prior to sending, call the receiver to confirm that the receiving fax machine is secure and to confirm the fax number?• Always use a cover sheet that includes both the sender's name and phone number and the intended recipient's name and phone number?• Always attach a confidentiality notice?		

Security of Electronic Files		
	Y	N
Do you always have to login to any system using a unique identifier and password?		
Is your password complex (numbers, symbols, letters etc) and at least 12 characters?		
Have you changed your password in the last 90 days?		
Do you store all electronic files containing sensitive information on a secure central server? (i.e. no sensitive information stored on local hard drive)		
Is your office computer screen positioned so that no unauthorized individuals can view sensitive information displayed?		
Is your screen saver set to automatically log out after 5 minutes of inactivity?		
Training & Knowledge		
In the last 12 months, have you completed training on privacy and security of sensitive information?		
Do you know whether or not you have authority to collect, use or disclose personal information?		
If you do have authority to collect, use or disclose personal information, do you know the limits and conditions of that authority?		
Mobile & Portable Devices		
Do you always store mobile or portable storage device such as laptops in a locked cabinet when not in use?		
Is all sensitive information contained on your portable storage devices limited to the absolute minimum necessary?		
Have you ensured that all sensitive information contained on any portable storage device you use is encrypted?		
Do you permanently delete sensitive information from your portable storage devices as soon as possible after use?		
Secure Disposal of Sensitive Information		
Do you dispose of hard copy records containing sensitive information by placing them in a secure shredding bin or by shredding them yourself?		
Privacy Habits		
Do you avoid discussing personal information in any area where the conversation can be overheard by unauthorized personnel?		
Do you disclose personal information to co-workers only where the information is necessary for the performance of the duties of your co-workers?		
If you must travel with personal information, do you always ensure that any personal information you have is stored in a locked cabinet or cupboard and never in your car?		

Please see our Reasonable Security Checklist, for more detailed information:

<https://oipc.novascotia.ca/node/471>

We encourage you to contact us if you have any questions about privacy and security in Nova Scotia.

Phone: 902-424-4684
Toll Free (NS): 1-866-243-1564
TDD/TTY: 1-800-855-0511
Fax: 902-424-8303
Email: oipcns@novascotia.ca



Tab 6



Reasonable Security Checklist

This checklist was prepared by the Office of the Information and Privacy Commissioner for Nova Scotia.¹ Under Nova Scotia's privacy legislation, public bodies, municipalities and health custodians must all ensure that they have made reasonable security arrangements against such risks as unauthorized access to or use, disclosure, copying or modifications of personal information.² This checklist is intended to give a quick snapshot of some key security standards. Failure to meet the standards set out in this checklist is an indication that personal information may be at risk and that a thorough review of security should be undertaken immediately.

The checklist includes questions in each of the 17 areas of security compliance listed below and should take about 30 minutes to complete:

1. Risk Management
2. Policies
3. Records Management
4. Human Resources Security
5. Physical Security
6. Systems Security
7. Network Security
8. Wireless
9. Database Security
10. Operating Systems
11. Email and Fax Security
12. Data Integrity and Protection
13. Access Control
14. Information Systems Acquisition, Development and Maintenance
15. Incident Management
16. Business Continuity Planning
17. Compliance

¹ This document is based on "Securing Personal Information: A Self-Assessment Tool for Organizations" created by the Office of the Information and Privacy Commissioners in Alberta and British Columbia and the Office of the Privacy Commissioner of Canada. The full self-assessment tool is available at: <https://www.oipc.bc.ca/guidance-documents/1439> and as an interactive tool at: <https://www.priv.gc.ca/resource/tool-outil/security-secure/english/AssessRisks.asp?x=1>.

² *Personal Health Information Act* s. 62, *Freedom of Information and Protection of Privacy Act* s. 24(3), *Municipal Government Act* s. 483(3).

Risk Management		
	Yes	No
1. We have identified all of our personal information assets and their sensitivity.		
2. We have analyzed, evaluated and documented the likelihood of security failures occurring.		
3. We have a risk treatment plan identifying the appropriate management action, resources, responsibilities and priorities for managing personal information security risks.		
Policies		
4. We have operational security policies (such as secure faxing, end-of-day closing, use of couriers).		
5. Employees, contractors and partners have easy access to our personal information security policy.		
6. We have an acceptable use policy.		
Records Management		
7. Specific retention periods have been defined for all personal information.		
8. Personal information contained on obsolete electronic equipment or other assets is securely destroyed before the equipment or asset is disposed of.		
9. Hard copy records containing personal information is shredded, mulched or otherwise securely destroyed.		
Human Resources Security		
10. Training has been implemented for all employees, data custodians and management to ensure they are aware of and understand their security responsibilities, permitted access, use and disclosure of personal information and retention and disposal policies.		
11. All employees are required to sign confidentiality agreements.		
12. Contractors and other third parties are required to return or securely destroy personal information to the public body upon completion of the contract.		
Physical Security		
13. We have strong physical security measures for storing personal information including locked cabinets, pass cards and motion detectors or other intrusion alarm systems.		
14. Our publicly accessible service counters are kept clear of personal information.		
15. We have a nightly closing protocol that requires employees to clear personal information from their desks and lock it away, log out of all computers and remove all documents containing personal information from fax machines and printers.		
System Security		
16. All terminals and personal computers used for handling personal information are positioned so that unauthorized personnel cannot see the screens.		
17. If a user walks away from her terminal there is an automatic process to lock out all users after a short defined period of inactivity.		
18. Personal information is always stored either on a secure server or is encrypted when stored on mobile and portable devices.		

Network Security		
	Yes	No
19. We use perimeter defence safeguards including firewalls, routers, intrusion detection, anti-virus/anti-spyware/anti-malware software) to mediate all traffic and to protect systems that are accessible from the internet.		
20. All systems exposed to the internet or servers supporting sensitive applications are “hardened” (e.g. by removing or disabling unnecessary services and applications and properly configuring user authentication).		
Wireless		
21. We have a policy in place that addresses the use of wireless technology.		
22. We have enabled the strongest available security features of the wireless devices, including encryption and authentication.		
23. A wireless intrusion detection and prevention capability is deployed on our network to detect suspicious behaviour.		
Database Security		
24. Automated and/or manual controls have been implemented to protect against unauthorized disclosure of personal information.		
25. There is a formal approval process in place for handling requests for disclosure of database contents or for database access that includes an evaluation of the privacy impacts and security risks.		
Operating Systems		
26. Our operating systems are kept up-to-date with all patches and fixes.		
27. We use a regular schedule for updating definitions and running scans with anti-virus, anti-spyware, anti-malware and anti-rootkit software.		
28. We regularly check expert websites and vendor software websites for alerts about new vulnerabilities and patches.		
Email and Fax Security		
29. We regularly update our fax and email lists.		
30. All of our faxes include a fax cover sheet with sender contact information and a confidentiality notice.		
31. We do not send emails with sensitive personal information unless the recipient has consented to the use of email, the email service is secure or the email itself is encrypted.		
Data Integrity and Protection		
32. We have a procedure in place to ensure that any removal of personal information from the premises has been properly authorized.		
33. We use automated and/or manual controls to prevent unauthorized copying, transmission or printing of personal information.		
Access Control		
34. We have a role-based access control policy.		
35. We have a formal user registration process in place.		
36. Each user of our system is uniquely identified.		
37. We limit access privileges to the least amount of personal information required to carry out job-related functions.		
38. Users of our system must first be authenticated by username and unique password that is changed at least every 90 days.		

Information Systems Acquisition, Development and Maintenance		
	Yes	No
39. We always identify security requirements as part of any new system development, acquisition or enhancement.		
40. We have controls in place to prevent or detect unauthorized software.		
Incident Management		
41. We have a privacy incident management policy in place and we have assigned an individual to coordinate our response to any incident.		
Business Continuity Planning		
42. We have a backup process in place to protect essential business information.		
Compliance		
43. We regularly monitor system audit logs that relate to the handling of personal information.		
44. We maintain an up-to-date software/hardware inventory.		
45. We conduct a regular physical inventory of all portable storage devices (laptops, thumb drives, portable hard drives, cell phones).		



Tab 7



Privacy Impact Assessment

Freedom of Information and Protection of Privacy Act

What is a Privacy Impact Assessment?

The *Freedom of Information and Protection of Privacy Act* (“FOIPOP”) sets out mandatory requirements relating to personal information held by public bodies. FOIPOP also requires that public bodies protect the confidentiality of personal information, and the privacy of the individual who is the subject of that information. This includes protecting the information from theft, loss and unauthorized access to, use of, disclosure, copying or disposal of the information.

A privacy impact assessment is a tool to identify risks and mitigation strategies associated with the use of personal information. It is an essential tool for ensuring compliance with the privacy requirements set out in FOIPOP and is a building block of a good privacy management program.¹

When Should I Complete a Privacy Impact Assessment?

You should complete a privacy impact assessment (“PIA”) for all new systems, projects, programs or activities. PIAs should also be completed when any significant changes are being contemplated to projects, programs or systems. There are a variety of PIA templates available online.² This PIA template was created by the Office of the Information and Privacy Commissioner for Nova Scotia and it incorporates elements of a number of existing templates.

Notice to Users

This document is intended to provide general information only. It is not intended nor can it be relied upon as legal advice. As an independent agency mandated to oversee compliance with FOIPOP, MGA and PHIA the Office of the Information and Privacy Commissioner for Nova Scotia cannot approve in advance any proposal from a public body. We must maintain our ability to investigate any complaints and to provide recommendations in response to these complaints. The contents of this document do not fetter or bind this office with respect to any matter, including any complaint investigation or other matter respecting which the Information and Privacy Commissioner for Nova Scotia* will keep an open mind. It remains the responsibility of each public body to ensure that they comply with their responsibilities under the relevant legislation. Visit us at: <https://oipc.novascotia.ca>

¹ For more information about Privacy Management Programs visit the website of the Freedom of Information and Protection of Privacy Review Office website at: <https://oipc.novascotia.ca>

² See for example the Capital District Health Authority’s PIA form at <http://www.cdha.nshealth.ca/privacy-confidentiality/documents>, the Government of Nova Scotia template at: <https://novascotia.ca/just/IAP/docs/Appendix%20B%20PIA%20Template.pdf>, the Government of British Columbia templates and guidance documents at: http://www.cio.gov.bc.ca/cio/priv_leg/foipppa/pia/pia_index.page?#DoINeedCompPIA

* The Information and Privacy Commissioner for Nova Scotia is also known as the Review Officer and is appointed as the independent oversight authority under the *Freedom of Information and Protection of Privacy Act*, the *Municipal Government Act*, the *Personal Health Information Act*, and the *Privacy Review Officer Act*.

Privacy Impact Assessment

Project Name: _____

Document Version, Review and Approval History

Version	Author	Nature of Change	Date

A. General Information

1. Name of Program or Service
2. Name of Department, Branch and Program Area
3. Name of Program or Service Representative
4. Contact Information

B. Description

1. **Description of the Initiative:** Provide a summary of the program, project activity or system, describe its purposes, goals and objectives. Explain the need for the new program, project or system and its benefits.
2. **Scope of this PIA:** Explain what part or phase of the initiative the PIA covers and what it does not cover.
3. **Elements of Information or Data:** List the personal information data elements involved in the initiative. This could include citizen's name, age, address, educational history, work status, health information, financial information, photos, comments on a blog, license numbers or hiring data.
4. **Description of Information Flow (include text and diagram):** Attach an information flow diagram showing how information will be collected and disclosed as a result of the initiative. See **Appendix A** for a sample information flow diagram.

If your initiative will not involve the collection, use or disclosure of personal information, you can stop here and submit this document to your privacy officer.

C. Collection, Use and Disclosure of Personal Information

1. **Limiting Collection, Use and Disclosure:** Privacy is a fundamental right of citizens and so any limitation on the privacy of citizens should be carefully analyzed to ensure such limitation is warranted. If your project involves highly sensitive personal information, a broad collection of personal information or a serious impingement on privacy³ answer the following four questions before proceeding:
 - a. **Is the measure demonstrably necessary to meet a specific need?** At a minimum, the objective must relate to societal concerns which are pressing and substantial in a free and democratic society. To be “demonstrably necessary” the public body should explain the rational connection between the specific need and the project.
 - b. **Is it likely to be effective in meeting that need?** Provide empirical evidence to support the initiative.
 - c. **Is the loss of privacy proportional to the need?** Explain how the collection, use and/or disclosure of personal information will be undertaken in the least privacy invasive manner possible. Minimizing the number of data elements collected, limiting access to the data and short retention periods are all examples of reducing the privacy invasive impact.
 - d. **Is there a less privacy invasive way of achieving the same end?** Explain what other less privacy invasive methods have already been tried to meet the identified need.

Based on this analysis you may decide you do not need to collect, use or disclose personal information for your project. You may decide to reduce the data elements (you need to go back and redo part B before proceeding) or you may determine that you can justify the scope of your collection, use and/or disclosure and so proceed to question 2.

2. **Legal Authority for the Collection, Use and Disclosure of Personal Information:** For each of the collection, use and disclosures identified, evaluate your public body’s legal authority and complete the following table. Refer to **Appendix B** for an example of an authorities summary table. Refer to **Appendix C** for a summary of the authorities to collect, use and disclose personal information under *FOIPOP*.

Personal Information Authorities Summary			
	Personal Information Description/Purpose	Type	FOIPOP Authority
1.			
2.			
3.			
4.			

³ Typically projects such as video surveillance, collection or use of GPS data, any covert surveillance, use of biometrics, etc., should be considered highly sensitive and will require this preliminary analysis.

3. Compliance with *Personal Information International Disclosure Protection Act* (“PIIDPA”):

PIIDPA requires that personal information in the custody or control of a public body shall not be stored or accessed outside of Canada, subject to limited exceptions (s.5(1)). Set out here whether or not there will be any proposed storage or access outside of Canada and if so, describe what *PIIDPA* exceptions apply. See **Appendix D** for a summary of the *PIIDPA* exceptions.

Personal Information International Disclosure Protection Act Authorities			
	Personal Information Description/Purpose	Type	PIIDPA Authority
1.			
2.			
3.			

D. Correction, Accuracy and Retention of Personal Information

1. Correction and Accuracy:

- a. How is an individual's information updated or corrected?
- b. If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated?
- c. If personal information will be disclosed to others, how will the public body notify them of the update, correction or annotation? (See s. 25 of *FOIPOP* for further information on correction and accuracy obligations).

2. Retention:

- a. Does your initiative use personal information to make decisions that directly affect an individual? If yes, please explain.
- b. Do you have a records retention and/or disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual? (See s. 24(4) of *FOIPOP*).

E. Security of Personal Information

1. **Reasonable security:** *FOIPOP* requires that public bodies protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure and disposal of personal information (s. 24(3) *FOIPOP*).
 - a. **Administrative safeguards** – Describe administrative safeguards (such as policies, training, contract provisions, consent forms etc.).
 - b. **Technical Safeguards** – Describe technical safeguards (such as passwords and user ID, authentication, encryption, firewalls and intrusion detection, secure transmission, disaster recovery).
 - c. **Physical Safeguards** – Describe physical safeguards (such as secure access, laptops secured to desk, alarm systems).
 - d. **Auditing** – Describe auditing capability and strategies (audit logs, records of user activity, proactive and focused audit capacity).

If your initiative involves the creation of a new system, consider completing a security threat and risk assessment.

2. **Access Matrix:** Personal information should only be used and disclosed as permitted under *FOIPOP*. Access to personal information must be limited to those employees whose job responsibilities require that they access the personal information. Attach a copy of the user access matrix. A user access matrix will list all of the position types (eg. clerical, manager of investigations, finance director) across one axis and all of the personal information types (or file types or data modules) across the other. The matrix will identify by position which individuals will have access to the identified data. See **Appendix E** for an example of an access matrix.

F. Risk Mitigation

Assess the impact on privacy, confidentiality and security of personal information as a result of the new program or service or change and make recommendations for mitigation of privacy risks. See **Appendix F** for examples of risks and mitigation strategies.

Risk Mitigation Table

	Risk	Mitigation Strategy	Likelihood	Impact
1				
2				
3				
4				

G. Action Plan

The purpose of this section is to provide an action plan to implement the recommendations listed in section F to reduce the privacy risks that have been identified. This section will provide a mechanism to track the recommendations, as well as describe responses to the recommendations of the PIA. Ensuring the recommended mitigations are implemented according to the action plan is the program area's responsibility, and may be followed-up by the privacy officer at any point.

Privacy Risk Action Plan		
Mitigation Strategy	Steps Required & Responsible Employee	Date to be Achieved

PIA Review Date: _____

PIAs require regular review to ensure that the system, project or program has not substantially changed and to ensure that mitigation strategies have been properly implemented. In addition, changes in other areas (such as technology or the implementation of other related programs) may create new risks that should be identified and mitigated. Typically the review date is selected based on the action plan – within six months of the final required completion dates is a good standard to use.

H. Approvals

Completed by:

[Insert position]	Date
-------------------	------

Reviewed by:

Privacy Officer	Date
-----------------	------

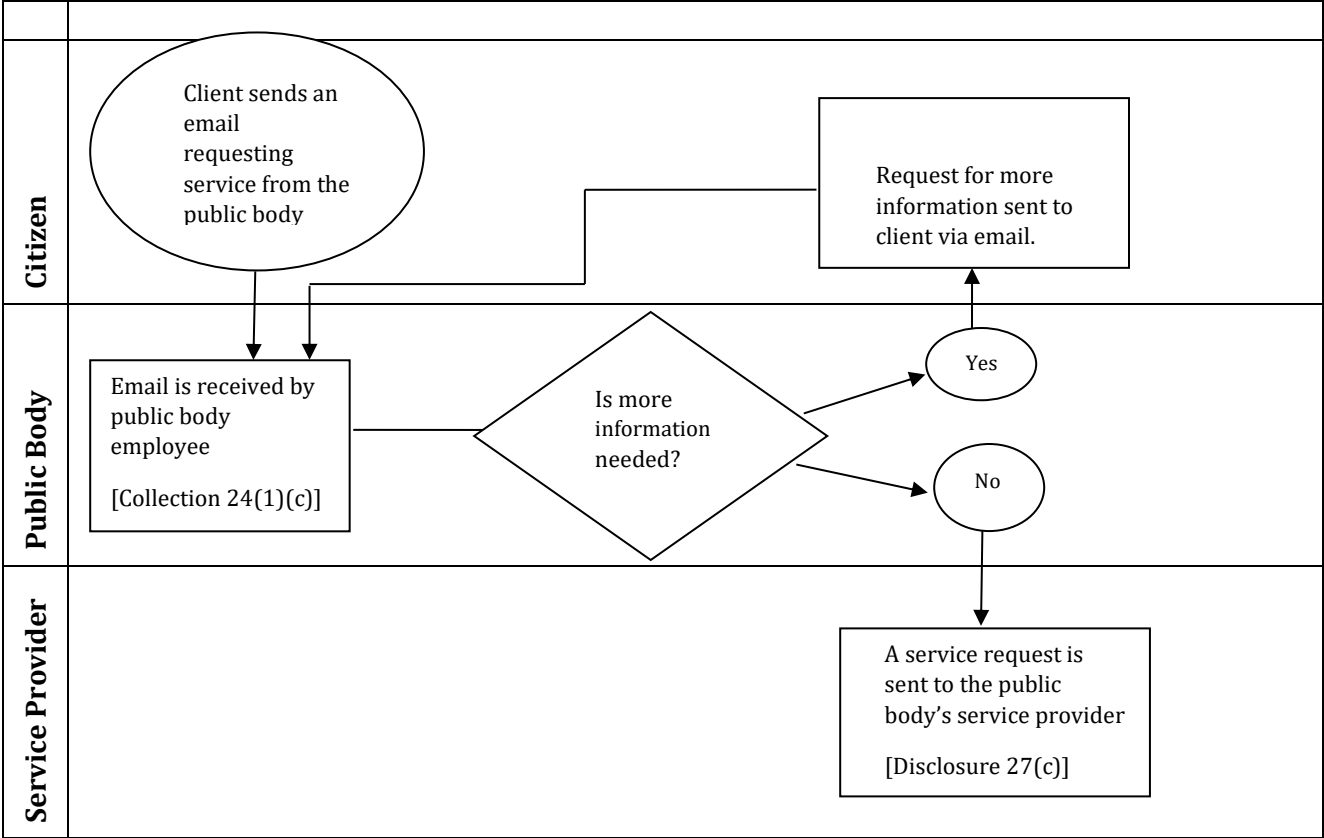
[Insert position]	Date
-------------------	------

Approved by:

[Insert Executive Sponsor]	Date
----------------------------	------

Appendix A: Sample Information Flow Diagram

Example:



Appendix B: Sample Authorities Summary Table

Using the example given in Appendix A, the table below lists the authorities.

Personal Information Authorities Summary			
	Description/Purpose	Type	FOIPOP Authority
1.	Email received from client requesting service	Collection	24(1)(c)
2.	Service request transferred to service provider contracted by public body	Disclosure	27(c)

Appendix C: Summary of Authorities Under *FOIPOP*

Collection	
24(1)(a)	The collection of the information is expressly authorized by or pursuant to an enactment (identify the enactment and section)
24(1)(b)	The information is collected for the purpose of law enforcement (review the definition of law enforcement in s. 3(1)(e) to ensure it applies)
24(1)(c)	The information relates directly to, and is necessary for, an operating program or activity of the public body
Use	
26(a)	Use is for the purpose for which the information was obtained or compiled, or for a use compatible with that purpose (to determine if a use is compatible review the requirements set out in s. 28)
26(b)	The individual the information is about has identified the information and has consented to the use (such consent should generally be in writing, dated and identifying the information)
26(c)	The use is for a purpose for which the information may be disclosed to the public body pursuant to s. 27 (check the disclosure list below)
Disclosure	
27(a)	In accordance with this Act or as provided pursuant to another enactment (identify the enactment and section)
27(b)	The individual the information is about has identified the information and consented in writing to its disclosure
27(c)	For the purpose for which it was obtained or compiled, or a use compatible with that purpose (to determine if a disclosure is for a compatible purpose review the requirements set out in s.28)
27(d)	For the purpose of complying with an enactment or with a treaty, arrangement or agreement made pursuant to an enactment (identify the enactment and section and attached the agreement if applicable)
27(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
27(f)	To an officer or employee of a public body if the information is necessary for the performance of the duties of, or for the protection of the health or safety of, the officer or employee
27(g)	To a public body to meet the necessary requirements of government operation
27(h)	For the purpose of collecting a debt or fine owing by an individual to the public body or making a payment owing by the public body to an individual
27(i)	To the Auditor General or other prescribed person for audit purposes

27(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
27(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
27(l)	To the Public Archives of Nova Scotia, or the archives of a public body for archival purposes
27(m)	To a public body or law-enforcement agency in Canada to assist in an investigation undertaken with a view to law enforcement or from which a law-enforcement proceeding is likely to result
27(n)	If the public body is a law-enforcement agency and the information is disclosed to another law-enforcement agency
27(o)	If the head of the public body determines that compelling circumstances exist that affect anyone's health or safety
27(p)	So that the next of kin or a friend of an injured, ill or deceased individual may be contacted
27(q)	For research, archival or historical purposes as provided in sections 29 and 30

Appendix D: Authority to Disclose & Store Personal Information Outside of Canada

Personal Information International Disclosure Protection Act

Application of the Act		
3	<i>PIIDPA</i> applies to every public body and municipality and to all directors, officers and employees as well as to all employees and associates of a service provider.	
4	<i>PIIDPA</i> does not apply to records listed in s. 4 which include: <ul style="list-style-type: none">• Published material or material that is available for purchase by the public• Material that is a matter of public record	
Access and Storage Outside Canada - Authorities		
5(1)	Rule	A public body shall ensure that personal information is stored and accessed only in Canada unless authorized under <i>PIIDPA</i>
5(1)(a)	Consent	The individual the information is about has identified the information and has consented, in the manner prescribed by regulation, to it being stored in or accessed from outside Canada.
5(1)(b)	PIIDPA Disclosure	The information is stored or accessed outside of Canada for the purpose of disclosure allowed under <i>PIIDPA</i> (see list below)
5(1)(c)	Permission	The head of the public body has allowed storage outside of Canada pursuant to s. 5(2): <ul style="list-style-type: none">• If the head considers the storage or access is to meet the necessary requirements of the public body’s operation, (subject to any restrictions or conditions the head considers advisable)• The head must report the access or storage decision to the Minister within the timeline set out in the Act (s. 5(3))
Disclosure Outside Canada - Authorities		
9(2)(b)	Consent	The individual the information is about has identified the information and consented, in writing, to its disclosure inside or outside Canada
9(2)(c)	Enactment	In accordance with an enactment of the Province, the Government of Canada or the Parliament of Canada that authorizes or requires its disclosure
9(2)(d)	Agreement	In accordance with a provision of a treaty, arrangement or agreement that authorizes or requires its disclosure and is made under an enactment of the Province, the Government of Canada or the Parliament of Canada
9(2)(e)	To head	To the head of the public body, if the information is immediately necessary for the performance of the duties of the head
9(2)(f)	To employee	To an employee of the public body and the information is immediately necessary for the protection of the health or safety of the employee

9(2)(g)	To legal counsel	To legal counsel for the public body, for use in civil proceedings involving the Government of the Province or the public body
9(2)(h)	Debts	To collect moneys owing by an individual to the Province or public body or for making a payment owing by the Province or public body
9(2)(i)	Motor vehicle	For the purpose of licensing or registration of motor vehicles or drivers or verification of motor vehicle insurance, registration or drivers' licenses
9(2)(j)	Compelling circumstances	Where the head of the public body determines that compelling circumstances exist that affect anyone's health or safety
9(2)(k)	Next of kin	So next of kin or friend of injured or deceased individual may be contacted
9(2)(l)	Research	For research purposes in accordance with s. 10
	Archives	To a provincial or public body archive in accordance with s. 11
9(3)	Law enforcement	A public body that is a law enforcement agency may disclose to another law enforcement agency in Canada or in a foreign country under an agreement or enactment of Canada or the province
9(4)	Temporary	The head of a public body may allow an employee to transport personal information outside Canada temporarily if the head considers it is necessary for the performance of the duties of the employee to transport the information in a computer, cell phone or other mobile device.

Appendix E: Sample Access Matrix

The following example is for a database intended to manage landlord and tenant complaint information. Access to personal information must be strictly limited to those needing the information to carry out their job duties. Depending on how duties are assigned, it may be the clerk's responsibility to input the initial information identifying the landlord, tenant and the complaint summary. If this is not true, then limit the clerk's access to those data elements required.

The Deputy Minister would not typically have access to a database of this nature and so has not been assigned any access rights in the matrix below. The matrix assumes that the landlord and tenant identity information is not contained in the complaint summary nor in the enforcement outcome. The investigation notes could, of course, contain a variety of information including personally identifiable information of the landlord and tenant.

	Landlord Information⁴	Tenant Information	Complaint Summary	Investigation Notes	Enforcement Outcome
Clerical	✓	✓	✓		✓
Program Director	✓	✓	✓		✓
Manager of Investigations	✓	✓	✓	✓	✓
Investigator	✓	✓	✓	✓	✓
Deputy Minister					

⁴ Identification information would include name, address and other contact information. This module may be common across a variety of databases.

Appendix F: Sample Risks and Mitigation Strategies

You will need to adopt a scale to measure likelihood and impact. High, medium and low will do or you can choose a numerical scale for greater subtlety in choice.

	Risk	Mitigation Strategy	Likelihood	Impact
1	Authorized user views record for personal reasons	<ul style="list-style-type: none"> • Log all read only and change activity • Monitor logs regularly, conduct spot audits and ensure audit capacity in response to complaints • Oath of employment and confidentiality agreements • Training 	Likelihood increases with more users	<ul style="list-style-type: none"> • More sensitive data results in higher impact • More data exposed by incident results in higher impact
2	Service provider fails to report privacy breach to public body	Contractual terms: <ul style="list-style-type: none"> • Require reporting within 24 hours • Impose penalties for failure to report and late reporting • Require the service provider to log all read only and change activity and to monitor the logs regularly • Permit the public body to conduct audits and to review service provider audit logs 	<ul style="list-style-type: none"> • Experience with the service provider may help determine this • Severity of consequences for service provider may lower the likelihood 	Same considerations as above
3	Client's personal information is compromised when transferred to the service provider	Transmission is encrypted and over a secure line	Low – depending on the quality of the encryption	Same considerations as above



Tab 8

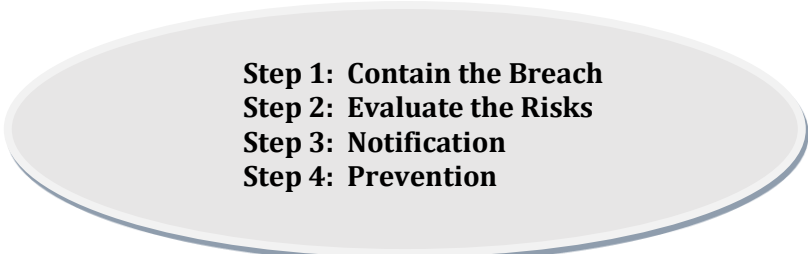


Key Steps to Responding to Privacy Breaches⁵

What is a privacy breach?

A privacy breach occurs whenever there is unauthorized access to or collection, use, disclosure or disposal of personal information. Such activity is unauthorized if it occurs in contravention of the *Freedom of Information and Protection of Privacy Act (FOIPOP)*, the *Municipal Government Act Part XX (MGA)* or the *Personal Health Information Act (PHIA)*.

What are the four key steps?



Step 1: Contain the Breach
Step 2: Evaluate the Risks
Step 3: Notification
Step 4: Prevention

The first three steps should be undertaken immediately upon discovery of the breach or in very quick succession. The fourth step is undertaken once the causes of the breach are known, in an effort to find longer term solutions to the identified problem.

Purpose of the Key Steps Document

Privacy breaches take many different forms, from misdirected faxes containing tax data, to the loss of hard drives containing personal information, to medical files blowing out the back of a garbage truck. Public bodies, municipalities and health custodians in Nova Scotia should be prepared to manage their responses to privacy breaches. The four key steps to responding to privacy breaches are steps that have been adopted across most Canadian jurisdictions in both the public and private sector. They represent best privacy practices for mitigating the harm arising from a privacy breach.

Use this document in combination with the Privacy Breach Checklist (p. 12 of this document) also available on our website at <https://oipc.novascotia.ca>.

⁵ This document is adapted from material prepared by the Office of the Information Commissioner of British Columbia entitled: *Privacy Breaches: Tools and Resources* available at <https://www.oipc.bc.ca/tools-guidance/guidance-documents>.

Step 1: Contain the Breach

Before continuing, you should ensure that you record all steps taken to investigate and manage the breach. The Privacy Breach Checklist tool can be used to complete all of the steps set out below and to record all relevant information. That tool is available at p. 12 of this document and at: <https://oipc.novascotia.ca>.

You should take immediate and common sense steps to limit the breach including:

- **Contain:** Immediately contain the breach by, for example, stopping the unauthorized practice, shutting down the system that was breached, revoking or changing computer access codes, sending a remote “kill” signal to a lost or stolen portable storage device, correcting weaknesses in physical security or searching the neighborhood or used item websites (such as Kijiji) for items stolen from a car or house.
- **Initial Investigation:** Designate an appropriate individual to lead the initial investigation. Begin this process the day the breach is discovered. This individual should have the authority within the public body or organization to conduct the initial investigation and make initial recommendations. If necessary, a more detailed investigation may subsequently be required.
- **Privacy Officer & Other Internal Notifications:** Immediately contact your Privacy Officer and the person responsible for security in your organization. Determine others who need to be made aware of the incident internally at this stage. It is helpful to prepare in advance a list of all of the individuals who should be contacted along with current contact information.
- **Breach Response Team:** Determine whether a breach response team must be assembled which could include representatives from appropriate business areas (labour relations, legal, communications, senior management). Representatives from privacy and security should always be included and generally the privacy team is responsible for coordinating the response to the incident.
- **Police:** Notify the police if the breach involves theft or other criminal activity.
- **Preserve Evidence:** Do not compromise the ability to investigate the breach. Be careful not to destroy evidence that may be valuable in determining the cause, or, that will allow you to take appropriate corrective action.

Step 2: Evaluate the Risks

To determine what other steps are immediately necessary, you must assess the risks. Consider the following factors:

Personal Information Involved

- As soon as possible get a complete list of all of the personal information at risk. Generally this means developing a list of the data elements lost, stolen or inappropriately accessed. For example, the data could include, name, address, date of birth, medical diagnosis and health card number (MSI). At this stage it is important that the investigator confirm the data at risk as quickly as possible. Be aware that if the breach is caused by an error or oversight by an employee, he or she may be reluctant to fully disclose the scope of the lost data.
- Next, evaluate the sensitivity of the personal information. Some personal information is more sensitive than others. Generally information including health information, government-issued pieces of information such as social insurance numbers, health care numbers and financial account numbers such as credit card numbers, is considered sensitive.
- Also consider the context of the information when evaluating sensitivity. For example, a list of customers on a newspaper carrier's route may not be sensitive. However, a list of customers who have requested service interruption while on vacation would be more sensitive.
- Finally, in your evaluation of sensitivity, consider the possible use of the information. Sometimes it is the combination of the data elements that make the information sensitive or capable of being used for fraudulent or otherwise harmful purposes.
- The more sensitive the information, the higher the risk.

Cause and Extent of the Breach

The cause and extent of the breach must also be considered in your analysis of the risks associated with the breach. Answer all of the following questions:

- What is the cause of the breach?
- Is there a risk of ongoing or further exposure of the information?
- What was the extent of the unauthorized collection, use or disclosure, including the number of likely recipients and the risk of further access, use or disclosure, including in mass media or online?
- Was the information lost or stolen? If it was stolen, can it be determined whether the information was the target of the theft or not?
- Is the information encrypted or otherwise not readily accessible?
- Has the personal information been recovered?
- What steps have you already taken to minimize the harm?
- Is this a systemic problem or an isolated incident?

Individuals Affected by the Breach

Knowing who was affected by the breach will shape your strategies in managing the breach and may also determine who will help manage the breach (e.g. union employees affected likely means labour relations should be on the breach management team), it will also determine who you decide to notify – if business partners are affected, then you will likely want to notify them.

- How many individuals are affected by the breach?
- Who was affected by the breach: employees, public, contractors, clients, service providers, other organizations?

Foreseeable Harm from the Breach

- Who is in receipt of the information? For example, a stranger who accidentally receives personal information and voluntarily reports the mistake is less likely to misuse the information than an individual suspected of criminal activity.
- Is there any relationship between the unauthorized recipients and the data subject? A close relationship between a victim and the recipient may increase the likelihood of harm – an estranged spouse is more likely to misuse information than a neighbour.
- What harm to the individuals will result from the breach? Harm that may occur includes:
 - Security risk (e.g. physical safety);
 - Identity theft or fraud;
 - Loss of business or employment opportunities;
 - Hurt, humiliation, damage to reputation or relationships;
 - Basis for potential discriminatory action that may be taken against the individual;
 - Social/relational harm (damage to the individual's relationships).
- What harm could result to the public body or organization as a result of the breach? For example:
 - Loss of trust in the public body or organization
 - Loss of assets
 - Financial exposure including class action lawsuits
 - Loss of contracts/business
- What harm could result to the public as a result of the breach? For example:
 - Risk to public health
 - Risk to public safety

Once you have assessed all of the risks described above you will be able to determine whether or not notification is an appropriate mitigation strategy. Further, the risk assessment will help you to identify appropriate prevention strategies.

The table below summarizes the risk factors and suggests a **possible** risk rating. Each public body, health custodian or municipality must make its own assessment of the risks given the unique circumstances of the situation. The table is intended to provide a rough guide to ratings.

Risk Rating Overview			
Factor	Risk Rating		
	Low	Medium	High
Nature of personal information	✓ Publicly available personal information not associated with any other information	✓ Personal information unique to the organization that is not medical or financial information	✓ Medical, psychological, counselling, or financial information or unique government identification number
Relationships	✓ Accidental disclosure to another professional who reported the breach and confirmed destruction or return of the information	✓ Accidental disclosure to a stranger who reported the breach and confirmed destruction or return of the information	✓ Disclosure to an individual with some relationship to or knowledge of the affected individual(s), particularly disclosures to motivated ex-partners, family members, neighbors or co-workers ✓ Theft by stranger
Cause of breach	✓ Technical error that has been resolved	✓ Accidental loss or disclosure	✓ Intentional breach ✓ Cause unknown ✓ Technical error – if not resolved
Scope	✓ Very few affected individuals	✓ Identified and limited group of affected individuals	✓ Large group or entire scope of group not identified

Risk Rating Overview			
Factor	Risk Rating		
	Low	Medium	High
Containment efforts	<ul style="list-style-type: none"> ✓ Data was adequately encrypted ✓ Portable storage device was remotely wiped and there is evidence that the device was not accessed prior to wiping ✓ Hard copy files or device were recovered almost immediately and all files appear intact and/or unread 	<ul style="list-style-type: none"> ✓ Portable storage device was remotely wiped within hours of loss but there is no evidence to confirm that the device was not accessed prior to wiping ✓ Hard copy files or device were recovered but sufficient time passed between the loss and recovery that the data could have been accessed 	<ul style="list-style-type: none"> ✓ Data was not encrypted ✓ Data, files or device have not been recovered ✓ Data at risk of further disclosure particularly through mass media or online
Foreseeable harm from the breach	<ul style="list-style-type: none"> ✓ No foreseeable harm from the breach 	<ul style="list-style-type: none"> ✓ Loss of business or employment opportunities ✓ Hurt, humiliation, damage to reputation or relationships ✓ Social/relational harm ✓ Loss of trust in the public body ✓ Loss of public body assets ✓ Loss of public body contracts or business ✓ Financial exposure to public body including class action lawsuits 	<ul style="list-style-type: none"> ✓ Security risk (e.g. physical safety) ✓ Identify theft or fraud risk ✓ Hurt, humiliation, damage to reputation may also be a high risk depending on the circumstances ✓ Risk to public health or safety

Step 3: Notification

Notification can be an important mitigation strategy that has the potential to benefit the public body, municipality, health custodian and the individuals affected by a breach. Prompt notification can help individuals mitigate the damage by taking steps to protect themselves. The challenge is to determine when notice should be required. Each incident needs to be considered on a case-by-case basis to determine whether the privacy breach notification is required. In addition, public bodies, municipalities and health custodians are encouraged to contact the Office of the Information and Privacy Commissioner for Nova Scotia for assistance in managing a breach.⁶

Review your risk assessment to determine whether notification is appropriate. If sensitive information is at risk, if the information is likely to be misused, if there is foreseeable harm, then you will likely want to notify. The list below provides further information to assist in decision making.

Note to health custodians: There are additional considerations set out specifically in *PHIA*. In particular, *PHIA* requires notification be given to either the affected individual or the Information and Privacy Commissioner in accordance with ss. 69 and 70 of *PHIA*.

Neither *FOIPOP* nor *Part XX* of the *MGA* requires notification. However, as noted above, notification in appropriate circumstances is best privacy practice and will help mitigate the losses suffered by individuals as a result of the breach. The steps taken in response to a breach have the potential to significantly reduce the harm caused by the breach, which will be relevant in any lawsuit for breach of privacy.

Notifying affected individuals

As noted above, notification of affected individuals should occur if it is necessary to avoid or mitigate harm to them. Some considerations in determining whether to notify individuals affected by the breach include:

- Legislation requires notification – s. 69 and s. 70 of *PHIA* for example;
- Contractual obligations require notification;
- There is a risk of identity theft or fraud – usually because of the type of information lost, stolen, accessed or disclosed, such as a SIN, banking information, identification numbers;
- There is a risk of physical harm – if the loss puts an individual at risk of stalking or harassment;
- There is a risk of hurt, humiliation or damage to reputation – for example when the information lost includes medical or disciplinary records;

⁶ The Office of the Information and Privacy Commissioner for Nova Scotia has the responsibility for monitoring how privacy provisions are administered and the ability to provide advice and comments on the privacy provisions when requested by public bodies and custodians. Our contact information is included on the last page of this document.

- There is a risk of loss of business or employment opportunities – if the loss of information could result in damage to the reputation of an individual, affecting business or employment opportunities; and
- There is a risk of loss of confidence in the public body or organization and/or good citizen relations dictates that notification is appropriate.

When and How to Notify

Notification should occur as soon as possible following the breach – within days whenever possible. 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.

On very rare occasions, medical evidence may indicate that notification could reasonably be expected to result in immediate and grave harm to the individual's mental or physical health. In those circumstances, consider alternative approaches, such as having the physician give the notice in person or waiting until the immediate danger has passed.

Direct notification is preferred – by phone, by letter or in person. Indirect notification – via websites, posted notices or media reports – should generally only occur in rare circumstances such as where direct notification could cause further harm or contact information is lacking.

Using multiple methods of notification in certain cases may be the most effective approach.

What Should be Included in the Notification?

Notifications should include the following information:

- Date of the breach;
- Description of the breach;
- Description of the information inappropriately accessed, collected, used or disclosed;
- Risk(s) to the individual caused by the breach;
- The steps taken so far to control or reduce the harm;
- Where there is a risk of identity theft as a result of the breach, typically the notice should offer free credit watch protection as part of the mitigation strategy;
- Further steps planned to prevent future privacy breaches;
- Steps the individual can take to further mitigate the risk of harm (e.g. how to contact credit reporting agencies to set up a credit watch, information explaining how to change a personal health number or driver's license number);
- Contact information of an individual within the public body, municipality or health organization who can answer questions or provide further information;

- Information and Privacy Commissioner for Nova Scotia contact information and the fact that individuals have a right to complain to the Information and Privacy Commissioner under the *Privacy Review Officer Act* and *PHIA*. If the public body, municipality or health custodian has already contacted the Information and Privacy Commissioner, include this detail in the notification letter.

Other Sources of Information

As noted above, the breach notification letter should include a contact number within the public body, municipality or health custodian, in case affected individuals have further questions. In anticipation of further calls, you should prepare a list of frequently asked questions and answers to assist staff responsible for responding to further inquiries.

Others to Contact

Regardless of what you determine your obligations to be with respect to notifying individuals, you should consider whether the following authorities or organizations should also be informed of the breach:

- Police – if theft or other crime is suspected;
- Insurers or others - if required by contractual obligations;
- Professional or other regulatory bodies - if professional or regulatory standards require notification of these bodies;
- Other internal or external parties not already notified – your investigation and risk analysis may have identified other parties impacted by the breach such as third party contractors, internal business units or unions;
- Office of the Information and Privacy Commissioner for Nova Scotia - the mandate of the Office of the Information and Privacy Commissioner includes a responsibility to monitor how the privacy provisions are administered and to provide advice and comments on the privacy provisions when requested by public bodies and health custodians.

The following factors are relevant in deciding whether or not to report a breach to the Office of the Information and Privacy Commissioner for Nova Scotia:

- For health custodians, s. 70 of *PHIA* sets out when the Office of the Information and Privacy Commissioner for Nova Scotia must be contacted. Health custodians may wish to contact the Office of the Information and Privacy Commissioner even when notification is not required, based on some of the factors listed below:
- The sensitivity of the information – generally the more sensitive the information at risk, the more likely the Office of the Information and Privacy Commissioner for Nova Scotia will be notified;
- Whether the disclosed information could be used to commit identity theft;
- Whether there is a reasonable chance of harm from the disclosure including non-pecuniary losses;

- The number of people affected by the breach;
- Whether the information was fully recovered without further disclosure;
- Your public body, municipality or health custodian wishes to seek advice or comment from the Information and Privacy Commissioner to aid in managing the privacy breach;
- Your public body, municipality or health custodian requires assistance in developing a procedure for responding to the privacy breach, including notification;
- Your public body, municipality or health custodian is concerned that notification may cause further harm; and/or
- To ensure steps taken comply with the public body's obligations under privacy legislation.

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 further breaches.

Typically, prevention strategies will address privacy controls in all of the following areas:

- Physical
- Technical
- Administrative
- Personnel

So, for example, if any physical security weaknesses contributed to the breach, changes made to prevent a recurrence should be undertaken. Systems controls should also be reviewed to ensure that all necessary technical safeguards are in place. This could mean encrypting all portable storage devices or improving firewall protections on a database.

Administrative controls would include ensuring that policies are reviewed and updated to reflect the lessons learned from the investigation and regularly after that. Your resulting plan should also include a requirement for an audit at the end of the process to ensure that the prevention plan has been fully implemented. If you do not already have a privacy breach protocol in place, ensure that one is developed as part of your plan.

Staff of public bodies, municipalities and health custodians should be trained to know the organization's privacy obligations under *FOIPOP*, *MGA Part XX* and/or *PHIA*.

In the longer term, public bodies, health custodians and municipalities should review and refresh their privacy management framework to ensure that they continue to comply with their privacy obligations. For more information on privacy management frameworks visit the Office of the Information and Privacy Commissioner for Nova Scotia website at: <https://oipc.novascotia.ca>.



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 for Nova Scotia.⁷ For a further explanation of how to manage a privacy breach see *Key Steps to Responding to Privacy Breaches* available at: <https://oipc.novascotia.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?

⁷ The Office of the Information and Privacy Commissioner for Nova Scotia's mandate includes an obligation to monitor how privacy provisions are administered and to provide advice and comments on privacy provisions on the request of health custodians and public bodies.

Steps 1 & 2: Containment & Risk Evaluation

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

(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 was 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 usernames 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 <i>PHIA</i> which require notification.	
Risk of identity theft	Most likely when the breach includes loss of SIN, credit card number, driver's license 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 <u>Direct</u> 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 <u>Indirect</u> 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 for Nova Scotia	
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	<ul style="list-style-type: none">• 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,⁸ 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?

⁸ For information on what constitutes a privacy management framework visit the tools tab on the Office of the Information and Privacy Commissioner for Nova Scotia's website at: <https://oipc.novascotia.ca>.



Tab 9

Insert Organization Name
Nova Scotia
Privacy Breach Management Protocol Template

Introduction:

This template was drafted by the Office of the Information and Privacy Commissioner for Nova Scotia. All words highlighted require consideration by the organization adapting this template for its own purposes. Sometimes the words need to be deleted (as with this paragraph) or sometimes the organization may wish to substitute words or names in place of the highlighted text (for example insert the organization's name in every place where "the organization" is mentioned). Use this document in combination with the *Key Steps to Responding to Privacy Breaches* document produced by the OIPC Nova Scotia and available at:

<https://oipc.novascotia.ca>

Organization:

Date:

Author:

Index:

1. What is the purpose of the privacy breach management protocol?
2. What is a privacy breach?
3. Roles and responsibilities
4. Breach management process
 - Step 1: Preliminary Privacy Breach Assessment Report & Containment
 - Step 2: Full Assessment
 - Step 3: Notification
 - Step 4: Mitigation and Prevention
 - Step 5: Lessons Learned

Appendix 1: Preliminary Privacy Breach Assessment Report

Appendix 2: Privacy Breach Checklist

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

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

2. What is a privacy breach?

A breach is any event that results in personal information in the custody or control of the organization 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 organization's personal information assets.

3. Roles and responsibilities

Note: Below is a sample of the positions that will have some responsibility for managing a privacy breach. Titles may vary from organization to organization and so when completing this template, insert the appropriate title for your organization. The responsibilities listed must be assigned to someone within your organization if the breach is to be properly managed. The responsibilities listed are described in more detail in the breach management process section of this document.

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

Position	Responsibilities
<ul style="list-style-type: none">• All staff	<ul style="list-style-type: none">• Complete preliminary breach assessment report. (Appendix 1) and immediately report privacy breach to Chief Privacy Officer.• Immediately undertake containment efforts.• Assist with breach investigations as required.
<ul style="list-style-type: none">• Chief Privacy Officer	<ul style="list-style-type: none">• 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.• Conduct appropriate internal notifications of the breach.

	<ul style="list-style-type: none"> • 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.
<ul style="list-style-type: none"> • Chief Security Officer 	<ul style="list-style-type: none"> • 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.
<ul style="list-style-type: none"> • Legal counsel 	<ul style="list-style-type: none"> • Participate as required on the Incident Response Team. • Assist Chief Privacy Officer in assessing whether notification is required.
<ul style="list-style-type: none"> • Communications staff 	<ul style="list-style-type: none"> • Assist in the drafting of breach notification letters.
<ul style="list-style-type: none"> • Labour relations/human resources staff. 	<ul style="list-style-type: none"> • Assist in implementation of containment and prevention strategies that require cooperation of staff, particularly unionized staff.
<ul style="list-style-type: none"> • Office of primary responsibility – manager or supervisor 	<ul style="list-style-type: none"> • Participate on Incident Response Team. • Assist in identifying containment, mitigation and prevention strategies. • Implement containment, mitigation and prevention strategies.
<ul style="list-style-type: none"> • Executive 	<ul style="list-style-type: none"> • Receive and review all reports of privacy breaches. • Follow up with Chief Privacy Officer 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 Chief Privacy Officer 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 Chief Privacy Officer 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 Incident Response Team, in consultation with the Chief Privacy Officer, will determine whether and to whom notification will be given. Notification is an important mitigation strategy that can benefit both the organization 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 organization 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 Chief Privacy Officer 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 Chief Privacy Officer 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 Chief Privacy Officer and the Incident Response Team 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 plan 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 organization'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 Chief Privacy Officer 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 patterns 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 Chief Privacy Officer.

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)?		<ul style="list-style-type: none"> 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 <i>Preliminary Report</i> and contact the Chief Privacy Officer.
2. Was personal information inappropriately disclosed (e.g. improper application of severances (material removed or blacked out), incomplete de-identification)?		<ul style="list-style-type: none"> 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 <i>Preliminary Report</i> and contact the Chief Privacy Officer.
3. Was personal information lost (e.g., through the mail, during a move or on a misplaced electronic device)?		<ul style="list-style-type: none"> 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 <i>Preliminary Report</i> and contact the Chief Privacy Officer.

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 <i>Preliminary Report</i> and contact the Chief Privacy Officer .
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 <i>Preliminary Report</i> and contact the Chief Privacy Officer .
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 <i>Preliminary Report</i> and contact the Chief Privacy Officer .
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 <i>Preliminary Report</i> and contact the Chief Privacy Officer .
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 <i>Preliminary Report</i> and contact the Chief Privacy Officer .
9. Was there an inappropriate display of personal information clearly visible to employees or clients? (e.g. posting of medical appointments or types of leave, home telephone numbers, slides of PowerPoint		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. e) Complete this <i>Preliminary Report</i> and contact the Chief Privacy Officer .

Preliminary Assessment	Yes/ No	Suggested Containment Strategies
presentations that contain personal information, etc.)?		
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 <i>Preliminary Report</i> and contact the Chief Privacy Officer.
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 <i>Preliminary Report</i> and contact the Chief Privacy Officer.
12. Was there an improper or unauthorized creation of personal information?		a) Complete this <i>Preliminary Report</i> and contact the Chief Privacy Officer.
13. Was there an improper or unauthorized retention of personal information?		a) Complete this <i>Preliminary Report</i> and contact the Chief Privacy Officer.
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? <input type="checkbox"/> Yes <input type="checkbox"/> No Whether yes or no, request direction from the Chief Privacy Officer or the OIPC.
8. Format of information involved: <input type="checkbox"/> Electronic records <input type="checkbox"/> Paper records <input type="checkbox"/> Other (describe): _____	9. What information was involved (check all that apply): <input type="checkbox"/> Medical <input type="checkbox"/> Employee <input type="checkbox"/> 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? <input type="checkbox"/> Yes <input type="checkbox"/> 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 **Chief Privacy Officer** 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:

<https://oipc.novascotia.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.

(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 <i>PHIA</i> 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 <u>Direct</u> 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 <u>Indirect</u> 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	<ul style="list-style-type: none">• 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: <https://oipc.novascotia.ca>.

A large, solid blue circle is centered on a white background. Inside the circle, the text "Tab 10" is written in a white, serif font.

Tab 10



Freedom of Information and Protection of Privacy Act - Privacy Rules At a Glance

Privacy Rules		
24	Collection	<ul style="list-style-type: none"> Public bodies shall not collect personal information unless: <ul style="list-style-type: none"> The collection is expressly authorized by an enactment The information is collected for the purpose of law enforcement The information relates directly to and is necessary for an operating program or activity of the public body
24(2)	Accuracy	<ul style="list-style-type: none"> If personal information will be used to make a decision that directly affects the individual the public body must ensure the information is accurate and complete
24(3)	Security	<ul style="list-style-type: none"> The public body must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure and disposal
24(4)	Retention	<ul style="list-style-type: none"> Where a public body uses an individual's personal information to make a decision that directly affects the individual, the public body must retain the information for at least one year
25	Correction	<ul style="list-style-type: none"> Applicant may request a correction Where no correction is made, the public body must annotate
26	Use	<ul style="list-style-type: none"> A public body may use personal information only: <ul style="list-style-type: none"> for the purpose for which that information was obtained or compiled or for a use compatible with that purpose if the individual has consented to the use for a purpose for which the information may be disclosed to the public body under s. 27- 30
27	Disclosure	<ul style="list-style-type: none"> A public body may disclose personal information only: <div style="margin-left: 20px;"> <p>Compatible use & consent</p> <ul style="list-style-type: none"> For the purpose the information was obtained or compiled or a use compatible with that purpose If the individual has consented in writing to the disclosure <p>Note: "compatible" is defined in s. 28 to mean a use of the personal information that has a reasonable and direct connection with the purpose for which it was originally collected <u>and</u> that is necessary for performing the statutory duties of, or for operating a legally authorized program of the public body.</p> <p>Law, subpoena, court orders</p> <ul style="list-style-type: none"> As provided pursuant to an enactment For the purpose of complying with an enactment or with a treaty or agreement made pursuant to an enactment To comply with a subpoena, warrant, summons or order issued by a court or person with jurisdiction to compel production of information <p>Public bodies</p> <ul style="list-style-type: none"> To an officer or employee of a public body if the information is necessary for the performance of the duties of, or for the protection of the health or safety of, the officer or employee </div>

Privacy Rules Cont'd		
27	Disclosure	<p>Public bodies cont'd</p> <ul style="list-style-type: none"> ○ To a public body to meet the necessary requirements of government operations ○ For the purpose of collecting a debt or fine owing to the Province or public body or to make a payment owed by the Province or public body <p>Law-enforcement</p> <ul style="list-style-type: none"> ○ To a public body or a law-enforcement agency in Canada to assist in an investigation undertaken with a view to a law-enforcement proceeding or from which a law-enforcement proceeding is likely to result ○ If the information is disclosed by a law-enforcement agency to another law-enforcement agency in Canada or in a foreign country under a written agreement, treaty or legislative authority <p>Auditor, bargaining agent, public archives & research</p> <ul style="list-style-type: none"> ○ To the Auditor General for audit purposes ○ 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 ○ To a representative or bargaining agent who has been authorized in writing by the employee whom the information is about to make an inquiry ○ To the Public Archives of Nova Scotia, or the archives of a public body for archival purposes ○ For the purpose of research or to archives as set out in s. 29 & 30 <p>Safety</p> <ul style="list-style-type: none"> ○ If the head of the public body determines that compelling circumstances exist that affect anyone's health or safety <p>Next of kin</p> <ul style="list-style-type: none"> ○ So next of kin or a friend of an injured, ill or deceased individual may be contacted
	(g)	
	(h)	
	(m)	
	(n)	
	(i)	
	(j)	
	(k)	
	(l)	
	(q)	
	(o)	
	(p)	

Notice

This table is intended as a quick reference tool. The sections are only summarized. You must read the entire provision to properly understand the full requirements of each section. You can find a copy of the *Freedom of Information and Protection of Privacy Act* at:
<http://nslegislature.ca/legc/statutes/freedom%20of%20information%20and%20protection%20of%20privacy.pdf>



Municipal Government Act Privacy Rules – At a Glance

Privacy Rules		
483	Collection	<ul style="list-style-type: none"> • Municipalities shall not collect personal information unless: <ul style="list-style-type: none"> ○ The collection is expressly authorized by an enactment ○ The information is collected for the purpose of law enforcement ○ The information relates directly to and is necessary for an operating program or activity of the municipality
483(2)	Accuracy	<ul style="list-style-type: none"> • If personal information will be used to make a decision that directly affects the individual the municipality must ensure the information is accurate and complete
483(3)	Security	<ul style="list-style-type: none"> • The municipality must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure and disposal
483(4)	Retention	<ul style="list-style-type: none"> • Where a municipality uses an individual's personal information to make a decision that directly affects the individual, the public body must retain the information for at least one year
484	Correction	<ul style="list-style-type: none"> • Applicant may request a correction • Where no correction is made, the municipality must annotate
485(1)	Use	<ul style="list-style-type: none"> • A municipality may use personal information only: <ul style="list-style-type: none"> ○ for the purpose for which that information was obtained or compiled or ○ for a use compatible with that purpose ○ if the individual has consented to the use ○ for a purpose for which the information may be disclosed to the municipality under s. 485(2)
485(2)	Disclosure	<ul style="list-style-type: none"> • A municipality may disclose personal information only: <ul style="list-style-type: none"> Compatible use & consent <ul style="list-style-type: none"> ○ For the purpose the information was obtained or compiled or a use compatible with that purpose ○ If the individual has consented in writing to the disclosure Law, subpoena, court orders <ul style="list-style-type: none"> ○ As provided pursuant to an enactment ○ For the purpose of complying with an enactment or with a treaty or agreement made pursuant to an enactment ○ To comply with a subpoena, warrant, summons or order issued by a court or person with jurisdiction to compel production of information Municipalities <ul style="list-style-type: none"> ○ To an officer or employee of a municipality if the information is necessary for the performance of the duties of, or for the protection of the health or safety of, the officer or employee

Privacy Rules Cont'd		
485(2)	Disclosure	<p>Municipalities cont'd</p> <ul style="list-style-type: none"> ○ To a municipality to meet the necessary requirements of municipal operation ○ For the purpose of collecting a debt or fine owing to the municipality or to make a payment owed by the municipality <p>Law enforcement</p> <ul style="list-style-type: none"> ○ To a municipality or a law-enforcement agency in Canada to assist in an investigation undertaken with a view to a law-enforcement proceeding or from which a law enforcement proceeding is likely to result ○ If the information is disclosed by a law-enforcement agency to another law enforcement agency in Canada or in a foreign country under a written agreement, treaty or legislative authority <p>Auditor, bargaining agent, public archives & research</p> <ul style="list-style-type: none"> ○ To the auditor for audit purposes ○ To a representative or bargaining agent who has been authorized in writing by the employee whom the information is about to make an inquiry ○ To the Public Archives of Nova Scotia, or the archives of a municipality for archival purposes ○ Archives of a municipality may disclose personal information for archival or historical purposes in limited circumstances ○ For the purpose of research or to archives as set out in s. 485(4) and (5) ○ For a research or statistical purpose in limited circumstances ○ For research or archival purposes <p>Safety</p> <ul style="list-style-type: none"> ○ If the responsible officer determines that compelling circumstances exist that affect anyone's health or safety <p>Next of kin</p> <ul style="list-style-type: none"> ○ So next of kin or a friend of an injured, ill or deceased individual may be contacted
(g)		
(h)		
(l)		
(m)		
(i)		
(j)		
(k)		
485(5)		
(na)		
485(4)		
(p)		
(n)		

Notice

This table is intended only as a quick reference tool. The sections are only summarized. You must read the entire provision to properly understand the full requirements of each section. You can find a copy of the *Municipal Government Act* at:

<http://nslegislature.ca/legc/statutes/municipal%20government.pdf>

Useful Websites

Resource	Website
Office of the Information and Privacy Commissioner for Nova Scotia: <ul style="list-style-type: none"> ➤ Tools & Guidance ➤ Legislation ➤ Decisions on interpretation of <i>FOIPOP</i>, <i>MGA</i> & <i>PHIA</i> 	https://oipc.novascotia.ca
Department of Internal Services – Information Access & Privacy Program <ul style="list-style-type: none"> ➤ Forms ➤ Legislation ➤ FAQs 	https://novascotia.ca/is/programs-and-services/information-access-and-privacy.asp
Other Information & Privacy Commissioners <ul style="list-style-type: none"> ➤ Other Canadian jurisdictions produce orders relating to provisions similar to those found in the <i>MGA</i> ➤ The Information Commissioner of Canada has produced an extensive manual explaining her interpretation of the federal <i>Access to Information Act</i>: The Investigator’s Guide to Interpreting the ATIA. 	<p>British Columbia https://www.oipc.bc.ca/</p> <p>Alberta http://www.oipc.ab.ca/pages/home/default.aspx</p> <p>Ontario https://www.ipc.on.ca/english/Home-Page/</p> <p>Information Commissioner of Canada http://www.oic-ci.gc.ca/eng/inv_inv-gui-ati_gui-inv-ati.aspx</p>
Cases and Laws <ul style="list-style-type: none"> ➤ Free online search engine for court cases, Commissioner decisions and laws in Canada 	<p>CanLii https://www.canlii.org/en/</p>
Policy Manuals <ul style="list-style-type: none"> ➤ Governments in other provinces produce policy manuals explaining sections of their access and privacy legislation. Always check to see if the provisions match the <i>MGA</i> but these manuals may provide some guidance for processing requests and managing privacy issues. 	<p>Treasury Board of Canada https://www.tbs-sct.gc.ca/atip-aiprp/tools/administration-application-eng.asp</p> <p>Alberta Government http://www.servicealberta.ca/foip/resources/guidelines-and-practices.cfm</p> <p>British Columbia Government http://www.cio.gov.bc.ca/cio/priv_leg/manual/index.page</p>
PIIDPA Annual Reports	http://novascotia.ca/just/IAP/