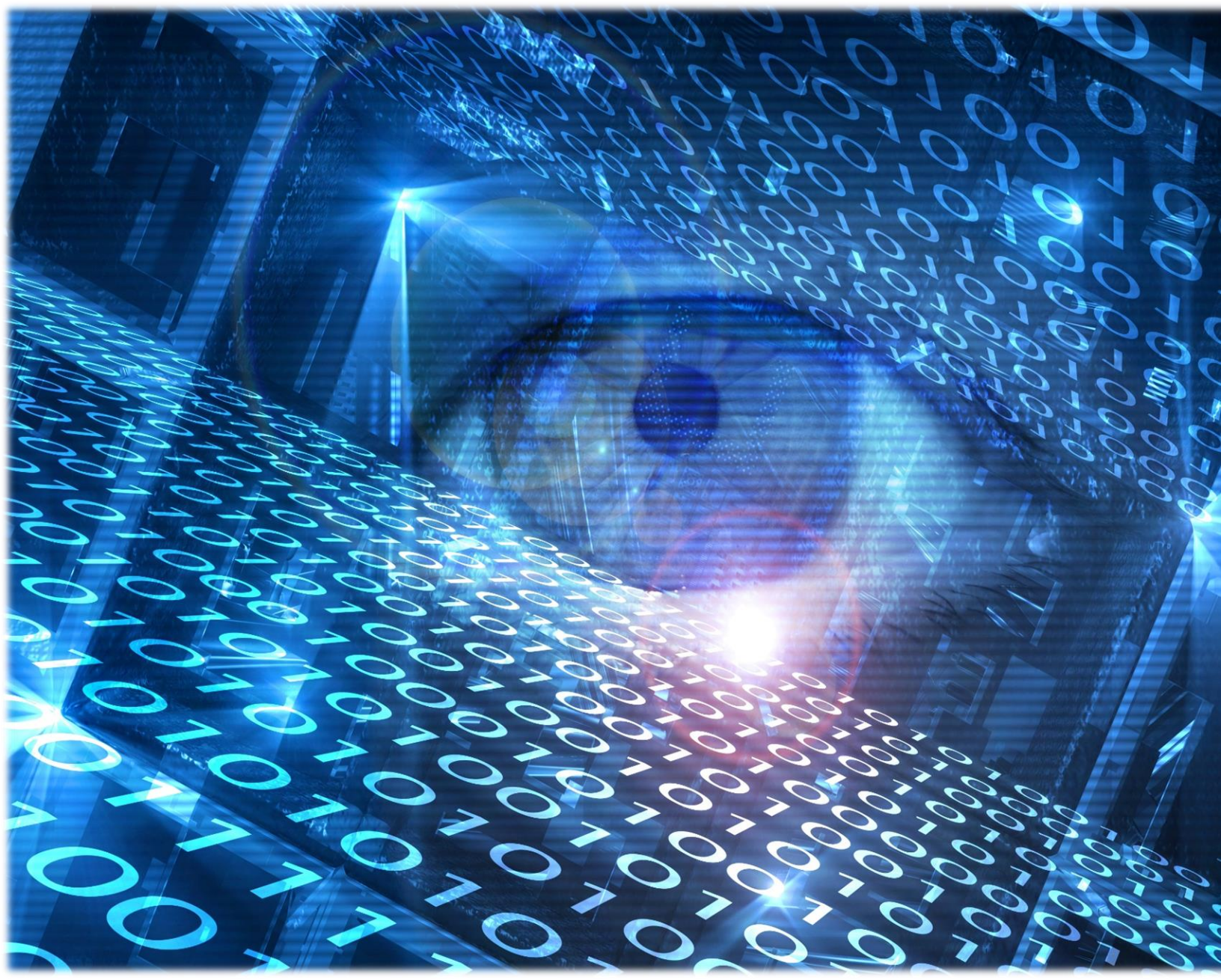




Chief Privacy Officer

PHIA Toolkit

Office of the Information and Privacy Commissioner for Nova Scotia
oipcns@novascotia.ca 902-424-4684 <https://oipc.novascotia.ca>



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 - PHIA 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 Toolkit for Health Custodians Gap Analysis Phase 1- Focus on PHIA Compliance Gap Analysis Phase 2 – Building Blocks Gap Analysis Phase 3- Ongoing Oversight and Revision Building a Privacy Management Program – Compliance Checklist	3
Training	
Training Deck: PHIA Basics for Staff	4
Five Minute Privacy Checkup	5
Security	
Reasonable Security Checklist	6
Privacy Impact Assessment	
Privacy Impact Assessment (PIA) Template - PHIA	7
Breach Management	
Key Steps to Responding to Privacy Breaches	8
Privacy Breach Checklist	9
Privacy Breach Management Protocol Template	10
PHIA Rules	
1. PHIA Index	11
2. PHIA Rules at a Glance	12
3. PHIA Disclosures Without Consent	13
4. PHIA Fee Fact Sheet	14

A large, solid blue oval shape centered on a white background.

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 (CPO) 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 and 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 training deck you can use to provide basic access and privacy training to all staff. Contact us at oipcns@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 oipcns@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/PHIA_Custodians.	
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 Toolkit for Health Custodians</i> is available on the OIPC website at https://oipc.novascotia.ca/PHIA_Custodians	



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 and monitor compliance.
	Communication	<ul style="list-style-type: none"> • Inform individuals of their rights and 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>.

A large, solid blue oval shape centered on a white background.

Tab 3



Office of the Information and Privacy Commissioner for Nova Scotia

Privacy Management Program Toolkit

Health Custodians

Personal Health Information Act

Introduction:

This toolkit was prepared by the Information and Privacy Commissioner² for Nova Scotia. It is intended to assist health custodians in developing a robust privacy management program.

Inside this Toolkit:

Document:	Description:
Privacy Management Program Gap Analysis Phase 1	Phase one focuses on the elements of the privacy management program that are required under the <i>Personal Health Information Act</i> .
Privacy Management Program Gap Analysis Phase 2	Phase two builds upon the elements completed in phase one and should be undertaken upon completion of the phase one analysis.
Privacy Management Program Gap Analysis Phase 3	Phase three is focused on ensuring effective ongoing assessment and revision of the privacy management program. Begin phase three immediately following completion of the phase two review.
Privacy Management Program Compliance Checklist	This checklist provides an overview of the status of your organization's implementation of all elements of a strong privacy management program.

To have a complete privacy management program you must complete all three phases of the privacy management program development.

² 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*.



Office of the Information and Privacy Commissioner for Nova Scotia

Privacy Management Program Gap Analysis Phase 1 –Health Custodians

Personal Health Information Act

Introduction:

This document was developed by the Information and Privacy Commissioner for Nova Scotia³ and is intended to assist health custodians with developing and implementing a robust privacy management program. This is phase one of the implementation of the program. To have a complete privacy management program you must complete all three phases of the PMP development. Phase one focuses on the elements of the privacy management program that are required under the *Personal Health Information Act* (“PHIA”).

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 for a phased implementation of a privacy management program and includes the elements specified in the PHIA. 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.

Contact Us:

If you have 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
5670 Spring Garden Road, Suite 509
Halifax, NS B3J 1H6
Phone: 902-424-4684 Toll Free: 1-866-243-1564

³ 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*.

Instructions:

This gap analysis tool begins with a Gap Analysis Summary document (page 4). When complete it 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 Organizational Commitment requirement for buy-in from the top lists two requirements from senior management (see page 5). 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 on page 4.

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 4. Colour ratings are explained on page 5.

Step 5: Once you have completed all of your ratings, review the summary sheet at page 4 and develop a plan to move all of your ratings to green (a privacy oversight and review plan).

Sample - Gap Analysis Summary – Phase 1 PHIA	
PMP Requirement	Overall Gap Analysis Rating
Building Blocks – Organizational Commitment	
a. Buy-in from the Top	2.2
b. Privacy Officer	1.9
c. Privacy Office	n/r ⁴
d. Reporting	1.3
Building Blocks – Program Controls	
a. Personal Information Inventory	2.8
b. Policies	2.0
c. Risk Assessment Tools	n/r
d. Training and Education Requirements	1.6
e. Breach and Incident Management Protocols	2.4
f. Service Provider Management	n/r
g. External Communication	1.5
h. Research Agreements	2.4
i. Safeguards – Information Practices	2.6

⁴ n/r = rating not required because this element is evaluated in future phases of the PMP implementation process.

Gap Analysis Summary – Phase 1 PHIA	
PMP Requirement	Overall Gap Analysis Rating
Building Blocks – Organizational Commitment	
a. Buy-in from the Top	
b. Privacy Officer	
c. Privacy Office	n/r
d. Reporting	
Building Blocks – Program Controls	
a. Personal Information Inventory	
b. Policies	
c. Risk Assessment Tools	n/r
d. Training and Education Requirements	
e. Breach and Incident Management Protocols	
f. Service Provider Management	n/r
g. External Communication	
h. Research Agreements	
i. Safeguards – Information Practices	

Gap Analysis and 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.

Gap Analysis Summary – Phase 1 PHIA		
Building Blocks – Organizational Commitment		
List of Expectations	Evidence of Compliance	Gap Rating
a. Buy-in from the top	Overall Rating	
1. Senior management endorses the program controls (policies, risk assessments, training).		
2. Senior management provides resources that the privacy management program needs to succeed.		
b. Privacy Officer (s. 67(1) PHIA)	Overall Rating	
3. The health custodian or a person appointed by the health custodian is authorized to:		
(i) Facilitate the custodian's compliance with <i>PHIA</i> .		
(ii) Ensure that all agents are informed of their duties under the <i>PHIA</i> .		
(iii) Respond to inquiries about the custodian's information practices.		
(iv) Respond to request for access to or correction of records.		
(v) Receive and process complaints under <i>PHIA</i> .		
(vi) Facilitate the communications to and training of the custodian's staff about policies and procedures under <i>PHIA</i> .		
(vii) Develop information to explain the organization's policies and procedures.		
c. Privacy Office	To be completed in phases 2 & 3	n/r
d. Reporting	Overall Rating	
4. Health custodian and senior management receive regular reports on privacy compliance.		

Gap Analysis Summary – Phase 1 PHIA		
Building Blocks – Program Controls		
List of Expectations	Evidence of Compliance	Gap Rating
a. Personal Information Inventory	Overall Rating	
5. The organization has completed a personal information inventory or equivalent.		
b. Policies	Overall Rating	
6. A privacy policy has been completed that explains:		
(i) The custodian's information practices. (s. 68(a) <i>PHIA</i>)		
(ii) How to contact the contact person/Privacy Officer (s. 68(b) <i>PHIA</i>).		
(iii) How to obtain access to or request correction of a record (s. 68(c) <i>PHIA</i>).		
(iv) How to make a complaint to the custodian and the Information and Privacy Commissioner for Nova Scotia (s. 68(d) <i>PHIA</i>).		
7. A complaints policy has been completed and implemented that includes:		
(i) A requirement that an individual submit a complaint in writing. (s. 62(2) <i>PHIA</i> and Regulation s. 8).		
(ii) The length of time the custodian will take to process, investigate and make a decision on the complaint (s. 62(2) <i>PHIA</i> and Regulation s. 8).		
8. Records retention schedule is in place that includes:		
(i) All legitimate purposes for retaining the information (s. 50(1)(a) <i>PHIA</i>).		
(ii) The retention period and destruction schedules for each purpose (s. 50(1)(b) <i>PHIA</i>).		
9. Notice of purposes is readily available that describes the purpose for the collection, use or disclosure of personal health information (s. 15 <i>PHIA</i>).		

Gap Analysis Summary – Phase 1 PHIA		
Building Blocks – Program Controls		
List of Expectations	Evidence of Compliance	Gap Rating
c. Risk Assessment Tools	To be completed in phases 2 & 3	n/r
d. Training and Education Requirements	Overall Rating	
10. All employees receive general privacy protection training.		
e. Breach and Incident Management Response Protocols	Overall Rating	
11. There is a person responsible for managing a breach.		
12. There is a procedure for notifying affected individuals and/or notifying the Information and Privacy Commissioner for Nova Scotia of breaches. (<i>PHIA</i> s. 70).		
f. Service Provider Management	To be completed in phases 2 & 3	n/r
g. External Communication	Overall Rating	
13. Notice of purposes (s. 15 <i>PHIA</i>) is readily available that describes the purpose for the collection, use or disclosure of personal health information.		
14. A Notice of Information Practices (s. 68 <i>PHIA</i>) is available that includes contact information and describes how an individual may access or correct a record and how to complain.		
15. The external communication is clear and understandable and not simply a reiteration of the law.		

Gap Analysis Summary – Phase 1 PHIA		
Building Blocks – Program Controls		
List of Expectations	Evidence of Compliance	Gap Rating
h. Research Agreements	Overall Rating	
16. All disclosures for research are via research agreements as set out in s. 60 <i>PHIA</i> .		
17. There is a process in place to notify the Information and Privacy Commissioner for Nova Scotia of research disclosures without consent (s. 57(d) <i>PHIA</i>).		
i. Safeguards – Information Practices	Overall Rating	
18. Information practices have been implemented that: (i) Are reasonable in the circumstances (s. 62(1)(b) <i>PHIA</i>).		
(ii) Ensure that personal health information is protected against theft or loss (s. 62(1)(c) <i>PHIA</i>).		
(iii) Protect personal health information against unauthorized access to or use, disclosure, copying or modification of information (<i>PHIA</i> s. 62(1)(c)).		
19. A record of user activity can be generated from all electronic information systems that are used to maintain personal health information (<i>PHIA</i> s. 63(2)).		
20. A record of user activity with the data required under Regulation s. 11(2) can be produced within 30 days of a request.		
21. Additional safeguards have been implemented for all electronic information systems maintained by the custodian in compliance with <i>PHIA</i> s. 10 and Regulation s. 10 including: (i) Protect network, hardware and software.		
(ii) Create and maintain written policies in support of the safeguards.		
(iii) Create a record of every security breach.		
(iv) For each breach include details of all corrective procedures taken to diminish the likelihood of future breaches.		



Office of the Information and Privacy Commissioner for Nova Scotia

Privacy Management Program Gap Analysis Phase 2 –Health Custodians

Personal Health Information Act

Introduction:

This document was developed by the Information and Privacy Commissioner for Nova Scotia⁵ and is intended to assist health custodians with developing and implementing a robust privacy management program. This is phase two of the implementation of the program. To have a complete privacy management program you must complete all three phases of the privacy management program development.

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 for a phased implementation of a privacy management program and includes the elements specified in the *Personal Health Information Act*. 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.

Contact Us:

If you have 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
5670 Spring Garden Road, Suite 509
Halifax, NS B3J 1H6
Phone: 902-424-4684 Toll Free: 1-866-243-1564

⁵ 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*.

Instructions:

This gap analysis tool begins with a Gap Analysis Summary document (page 11). 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 a requirement from senior management (see page 12). 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 on page 11.

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 11. Colour ratings are explained on page 11.

Step 5: Once you have completed all of your ratings, review the summary sheet at page 11 and develop a plan to move all of your ratings to green (a privacy oversight and review plan).

Sample - Gap Analysis Summary – Phase 2 PHIA	
PMP Requirement	Overall Gap Analysis Rating
Building Blocks – Organizational Commitment	
e. Buy-in from the Top	2.2
f. Privacy Officer	n/r ⁶
g. Privacy Office	1.9
h. Reporting	1.3
Building Blocks – Program Controls	
j. Personal Information Inventory	2.8
k. Policies	2.0
l. Risk Assessment Tools	2.1
m. Training and Education Requirements	1.6
n. Breach and Incident Management Protocols	2.4
o. Service Provider Management	2.3
p. External Communication	1.5
q. Research Agreements	n/r
r. Safeguards – Information Practices	n/r

⁶ n/r = rating not required because this element is evaluated in previous or future phases of the PMP implementation process

Gap Analysis Summary – Phase 2 PHIA	
PMP Requirement	Overall Gap Analysis Rating
Building Blocks – Organizational Commitment	
a. Buy-in from the Top	
b. Privacy Officer	n/r ⁷
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	
h. Research Agreements	n/r
i. Safeguards – Information Practices	n/r

Gap Analysis and 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.

⁷ No rating required as this element is implemented in phase 1 of the PMP.

Gap Analysis Summary – Phase 2 PHIA		
Building Blocks – Organizational Commitment		
List of Expectations	Evidence of Compliance	Gap Rating
a. Buy-in from the Top	Overall Rating	
3. Senior management monitors program and reports to board of directors as appropriate.		
b. Privacy Officer	Completed in phase 1	n/r
c. Privacy Office	Overall Rating	
4. The Privacy Officer is supported by dedicated staff.		
5. The role of the privacy office is defined.		
6. Staff have delegated responsibilities to monitor compliance.		
d. Reporting	Overall Rating	
7. There are privacy reporting mechanisms that ensure that the right people know how the privacy management program is structured and whether it is functioning as expected.		
8. The reporting program has documented reporting structures.		
Building Blocks – Program Controls		
a. Personal Information Inventory	Overall Rating	
9. The organization is able to provide detailed information about inventory.		
b. Policies	Overall Rating	
10. There is a responsible use of information and information technology policy that includes administrative, physical and technical security controls and appropriate access controls.		
c. Risk Assessment Tools	Overall Rating	
11. Privacy risk assessments are required throughout the organization for all new projects involving personal information and on any new collection, use or disclosure of personal health information.		
12. Organizations have developed a process for identifying and mitigating privacy and security risks including the use of privacy impact assessments and security threat and risk assessments.		

Gap Analysis Summary – Phase 2 PHIA		
Building Blocks – Program Controls		
List of Expectations	Evidence of Compliance	Gap Rating
d. Training and Education Requirements	Overall Rating	
13. Privacy training is mandatory for all new employees.		
14. Training processes are documented and participation and success is measured.		
15. Individuals who handle personal health information directly need additional training specifically tailored to their roles.		
e. Breach and Incident Management Response Protocols	Overall Rating	
16. There is a procedure for management of personal health information breaches.		
17. Responsibilities for internal and external reporting of the breach are defined.		
f. Service Provider Management	Overall Rating	
18. Contractual or other means are in place to protect personal health information.		
19. The request for proposal process includes a survey of proponent's privacy management framework structure.		
20. Transborder data flows and requirements of the foreign regime are addressed in the service provider arrangements.		
21. Sensitivity of personal health information is addressed in the service provider arrangements.		
22. 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 health information.		
(iii) Restrictions on sub-contracting		
(iv) Audits.		
(v) Agreements with service provider employees stating that they will comply with the organization's privacy policies and protocols.		

Gap Analysis Summary – Phase 2 PHIA		
Building Blocks – Program Controls		
List of Expectations	Evidence of Compliance	Gap Rating
g. External Communication	Overall Rating	
23. There is a procedure for informing individuals of their privacy rights.		
24. There is a procedure for informing individuals of the program controls.		
25. External communication (i) Provides enough information so that individuals know the purpose of the collection, use and disclosure of personal health information, 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 health information.		
(iv) Is easily available to individuals.		
(v) Individuals are aware of how to access and correct their personal health 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.		
h. Research Agreements	Completed in phase 1	n/r
i. Safeguards	Completed in phase 1	n/r



Office of the Information and Privacy Commissioner for Nova Scotia

Privacy Management Program Worksheet

Gap Analysis Phase 3 –Health Custodians

Personal Health Information Act

Introduction:

This document was developed by the Information and Privacy Commissioner for Nova Scotia⁸ and is intended to assist health custodians with developing and implementing a robust privacy management program (“PMP”). This Gap Analysis is intended for small and medium sized health custodians – organizations with up to five health care providers. This is phase three of the implementation of the program. To have a complete privacy management program you must complete all three phases of the PMP development.

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 for a phased implementation of a privacy management program and includes the elements specified in the *Personal Health Information Act* (“PHIA”). 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.

Contact Us:

If you have 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
5670 Spring Garden Road, Suite 509
Halifax, NS B3J 1H6
Phone: 902-424-4684 Toll Free: 1-866-243-1564

⁸ 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 17). 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. In phase three only a few building blocks elements are left to complete; most of the work left to do is in the area of ongoing assessment and revision. As you analyze your organization’s level of compliance, 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 organization’s compliance on a scale of 1 to 3. Feel free to give partial points. Ratings are explained on page 17.

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 17. Colour ratings are explained on page 17.

Step 5: Once you have completed all of your ratings, review the summary sheet at page 17 and develop a plan to move all of your ratings to green (a privacy oversight and review plan).

Sample - Gap Analysis Summary – Phase 3 PHIA	
PMP Requirement	Overall Gap Analysis Rating
Building Blocks – Organizational Commitment	
a. Buy-in from the Top	n/r ⁹
b. Privacy Officer	n/r
c. Privacy Office	2.7
d. Reporting	2.4
Building Blocks – Program Controls	
a. Personal Information Inventory	n/r
b. Policies	n/r
c. Risk Assessment Tools	2.2
d. Training and Education Requirements	1.8
e. Breach and Incident Management Protocols	n/r
f. Service Provider Management	n/r
g. External Communication	n/r
h. Research Agreements	n/r
i. Safeguards – Information Practices	n/r
Ongoing Assessment and Revision – Oversight and Review Plan	
a. Develop Oversight and Review Plan	2.6
Ongoing Assessment and Revision – Program Controls	
a. General Requirements	1.3
b. Update Personal Information Inventory	1.6
c. Revise Policies	2.1
d. Treat Risk Assessment Tools as Evergreen	2.2
e. Modify Training and Education	2.0
f. Adapt Breach and Incident Response Protocols	2.8
g. Fine-tune Service Provider Management	1.5
h. Improve External Communication	2.3

⁹ n/r = no rating required as this element is implemented in phase 1 or 2 of the PMP.

Gap Analysis Summary – Phase 3 PHIA	
PMP Requirement	Overall Gap Analysis Rating
Building Blocks – Organizational Commitment	
a. Buy-in from the Top	n/r
b. Privacy Officer	n/r
c. Privacy Office	
d. Reporting	
Building Blocks – Program Controls	
a. Personal Information Inventory	n/r
b. Policies	n/r
c. Risk Assessment Tools	
d. Training and Education Requirements	
e. Breach and Incident Management Protocols	n/r
f. Service Provider Management	n/r
g. External Communication	n/r
h. Research Agreements	n/r
i. Safeguards – Information Practices	n/r
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 and 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.

Gap Analysis Summary – Phase 3 PHIA		
Building Blocks – Organizational Commitment		
List of Expectations	Evidence of Compliance	Gap Rating
a. Buy-in from the Top	Completed in phases 1 & 2	n/r ¹⁰
b. Privacy Officer	Completed in phase 1	n/r
c. Privacy Office	Overall Rating	
26. Staff foster a culture of privacy within the organization.		
27. Staff work to ensure that privacy protection is built into every major function involving the use of personal health information.		
d. Reporting	Overall Rating	
5. An internal audit and assurance program monitors compliance with privacy policies.		
6. An escalation procedure has been clearly defined and explained to all employees for security breaches or when a customer complains.		
Building Blocks – Program Controls		
a. Personal Information Inventory	Completed in phases 1 & 2	n/r
b. Policies	Completed in phases 1 & 2	n/r
c. Risk Assessment Tools	Overall Rating	
7. 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.		
d. Training and Education Requirements	Overall Rating	
8. Training and education are recurrent and the content of the program is periodically revisited and updated to reflect changes.		
e. Breach Management	Completed in phases 1 & 2	n/r
f. Service Provider Management	Completed in phases 1 & 2	n/r
g. External Communications	Completed in phases 1 & 2	n/r
h. Research Agreements	Completed in phase 1	n/r

¹⁰ n/r= not required as this expectation has already been addressed in earlier phases of the PMP development

Gap Analysis Summary – Phase 3 PHIA		
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 PMP'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	
4. The effectiveness of program controls are monitored periodically, audited and revised where necessary.		
5. 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.		

Gap Analysis Summary – Phase 3 PHIA		
Assess & Revise Program Controls		
List of Expectations	Evidence of Compliance	Gap Rating
a. General Requirements continued		
6. Problems identified during monitoring are documented and addressed.		
7. The Privacy Officer conducts periodic assessments to ensure key processes are being respected.		
8. The organization has developed metrics to gauge progress with respect to compliance.		
9. Assessments of program controls are conducted in a focused, continuous and thorough manner.		
b. Update Personal Information Inventory	Overall Rating	
10. The personal information inventory is kept current.		
11. New collections of personal information are identified and evaluated.		
12. New uses of personal information are identified and evaluated.		
c. Revise Policies	Overall Rating	
13. 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	
14. 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.		

Gap Analysis Summary – Phase 3 PHIA		
Assess & Revise Program Controls		
List of Expectations	Evidence of Compliance	Gap Rating
d. Treat Risk Assessment Tools as Evergreen continued		
15. 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
16. Training and education programs are reviewed and modified on a periodic basis as a result of ongoing assessments.		
17. Changes to program controls are effectively communicated to employees as they are made, or in “refreshed” education and training modules.		
f. Adapt Breach and Incident Response Protocols		Overall Rating
18. Breach and incident management response protocols are reviewed and revised to implement best practices or recommendations.		
19. 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
20. Contracts with service providers are reviewed and, where necessary, fine-tuned.		
h. Improve External Communication		Overall Rating
21. External communications explaining privacy policies are reviewed, updated and clarified as needed.		



Office of the Information and Privacy Commissioner for Nova Scotia

Building a Privacy Management Program Compliance Checklist Health Custodians

Personal Health Information Act

This checklist and the accompanying gap analysis worksheets were prepared by the Information and Privacy Commissioner for Nova Scotia.¹¹ They are intended to assist small and medium sized health custodians in developing a robust privacy management program.

Ideally the steps set out below in three phases will be completed as quickly as possible. This checklist recognizes that for small and medium sized health custodians, the tasks of creating and maintaining a privacy management program requires some time. The list below prioritizes the tasks, emphasizing in phase 1 compliance with the statutory requirements of the *Personal Health Information Act* (“PHIA”). The requirements are cumulative so that phase 1 requirements should be maintained as phases 2 and 3 are implemented. Use this checklist in conjunction with the detailed Privacy Management Framework Gap Analysis Worksheets for each of phases 1, 2 and 3. All documents are available on the Office of the Information and Privacy Commissioner of Nova Scotia’s website at <https://oipc.novascotia.ca>.

¹¹ 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*.

PMP Requirement	Done	PMP Requirement	Done
Phase 1			
Organizational Commitment		Building Blocks – Program Controls continued	
a. Buy-in from the Top <ul style="list-style-type: none"> Senior management endorses privacy controls. Senior management provides resources needed. 		f. Service Provider Management	
b. Privacy Officer <ul style="list-style-type: none"> Privacy Officer appointed with seven essential authorizations. 		g. External Communication <ul style="list-style-type: none"> Notice of purposes is readily available and clear. Notice of Information Practices is available. External communications are clear and understandable. 	
c. Privacy Office	n/r ²	h. Research Agreements <ul style="list-style-type: none"> All disclosures for research are via research agreement set out in s. 60 of <i>PHIA</i>. Process in place to notify Information and Privacy Commissioner for Nova Scotia of research disclosures without consent (s. 57(d) <i>PHIA</i>). 	
d. Reporting <ul style="list-style-type: none"> Senior management and health custodian receive regular reports. 			
Building Blocks – Program Controls		i. Safeguards <ul style="list-style-type: none"> Information practices have been implemented and protect personal health information. Additional safeguards are implemented for all personal health information held in electronic information systems. Written policies support the additional safeguards. All privacy breaches involving systems are recorded. A record of user activity that complies with <i>PHIA</i> requirements can be produced within 30 days from any electronic information system. 	
a. Personal Information Inventory completed.			
b. Policies <ul style="list-style-type: none"> Privacy policy including information practices and contact information. Complaints policy. Record retention and destruction policy. 			
c. Privacy Risk Assessments	n/r		
d. Privacy Training <ul style="list-style-type: none"> All employees receive privacy training. 			
e. Breach Management <ul style="list-style-type: none"> Procedure in place to notify individuals and/or Information and Privacy Commissioner for Nova Scotia of breaches. Person responsible assigned to manage breaches. 			

² n/r = no rating required because this requirement is completed in other implementation phases

PMP Requirement	Done	PMP Requirement	Done
Phase 2			
Organizational Commitment		Building Blocks – Program Control continued	
a. Buy-in from the Top		d. Privacy Training	
<ul style="list-style-type: none"> Senior management monitors program. 			
b. Privacy Officer	n/r	e. Breach Management	
c. Privacy Office			
<ul style="list-style-type: none"> Supported by dedicated staff with delegated responsibility. Role of office is defined. Staff foster a culture of privacy within the organization. Staff work to ensure privacy is built into every major function. 		<ul style="list-style-type: none"> There is a procedure in place for the management of breaches. Internal and external reporting roles are defined. 	
d. Reporting		f. Service Provider Management	
<ul style="list-style-type: none"> Privacy reporting mechanisms are developed and used. The reporting program has documented reporting structures. 			
Building Blocks – Program Control		g. External Communication	
a. Personal Information Inventory			
<ul style="list-style-type: none"> The organization is able to provide detailed information about inventory. 		<ul style="list-style-type: none"> Contractual or other means are in place to protect personal information. RFP process includes privacy survey of all proponents. Transborder data flows and requirements of the foreign regime are addresses in service provider contracts. Detailed contract provision (privacy schedule) included in contracts. 	
b. Policies		h. Research Agreements	n/r
<ul style="list-style-type: none"> Responsible use policy in place. 			
c. Privacy Risk Assessments			
<ul style="list-style-type: none"> Privacy risk assessments are required for all new projects. Process in place for identifying and mitigating privacy and security risks. 		i. Safeguards	n/r

PMP Requirement	Done	PMP Requirement	Done
Phase 3			
Organizational Commitment		Ongoing Assessment and Revision – Program Controls	
a. Buy-in from the Top	n/r	a. General Requirements <ul style="list-style-type: none"> Effectiveness of program controls are monitored periodically. Monitoring addresses seven core areas identified. Problem areas are documented and addressed. Privacy Officer conducts periodic assessments to ensure key processes are being respected. The organization has developed metrics. 	
b. Privacy Officer	n/r		
c. Privacy Office <ul style="list-style-type: none"> Staff foster a culture of privacy within the organization. Staff work to ensure privacy is built into every major function. 			
d. Reporting <ul style="list-style-type: none"> Internal audit and assurance program monitors compliance with privacy policies. Escalation procedure is in place for privacy breaches and complaints. 			
Building Blocks – Program Control		b. Update Personal Information Inventory <ul style="list-style-type: none"> The personal information inventory is kept current with new collections and uses identified and evaluated. 	
a. Personal Information Inventory	n/r	c. Revise Policies <ul style="list-style-type: none"> Policies are reviewed and revised as needed. 	
b. Policies	n/r		
c. Privacy Risk Assessments <ul style="list-style-type: none"> Review and approval process in place for all new initiatives. 		d. Treat Risk Assessment Tools as Evergreen <ul style="list-style-type: none"> Privacy impact assessments and security threat and risk assessments are treated as evergreen. 	
d. Privacy Training <ul style="list-style-type: none"> Training is recurrent and content is updated. 		e. Modify Training and Education <ul style="list-style-type: none"> Education programs are reviewed and updated on a periodic basis. Changes to program controls are effectively communicated to employees. 	
e. Breach Management	n/r		
f. Service Provider Management	n/r		
g. External Communications	n/r		
h. Research Agreements	n/r	f. Adapt Breach and Incident Response Protocols <ul style="list-style-type: none"> Protocols are reviewed and revised to implement best practices or recommendations. 	
i. Safeguards	n/r		
Ongoing Assessment and Revision – Oversight and Review Plan		g. Fine-tune Service Provider Management <ul style="list-style-type: none"> Contracts with services providers are reviewed and improved with experience. 	
a. Develop Oversight and Review Plan <ul style="list-style-type: none"> Privacy Officer develops oversight and review plan on an annual basis. The plan establishes performance measures. The plan includes a schedule of when all policies and controls will be reviewed. 		h. Improve External Communication <ul style="list-style-type: none"> External communications are reviewed, updated and clarified as needed. 	

A large, solid blue oval shape centered on a white background.

Tab 4

Training Deck: PHIA Basics for Staff

See the PowerPoint slides provided separately. The slides include note pages to guide the presenter through this presentation intended to provide staff with some basic rules under the *Personal Health Information Act*. The notes include text in red where the text needs to be modified, for example to input contact information of the Chief Privacy Officer.

As part of the presentation, staff are asked to complete the *5-Minute Privacy Checkup* (mentioned on slide 16), which is also provided in the next section (Tab 5).

A large, solid blue oval shape centered on a white background.

Tab 5



Office of the Information and Privacy Commissioner for Nova Scotia

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

A large, solid blue oval shape centered on a white background.

Tab 6



Reasonable Security Checklist

This checklist was prepared by the Office of the Information and Privacy Commissioner for Nova Scotia.¹² 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.¹³ 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

¹² 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-securite/english/AssessRisks.asp?x=1>.

¹³ *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).		

A large, solid blue oval shape centered on a white background.

Tab 7



Privacy Impact Assessment

Personal Health Information Act

What is a Privacy Impact Assessment?

The *Personal Health Information Act (PHIA)* sets out mandatory requirements relating to personal health information held by custodians. *PHIA* also requires that custodians protect the confidentiality of personal health information, and the privacy of the individual who is the subject of that information. This includes protecting the personal health information from theft, loss and unauthorized access to, use of, disclosure, copying, modification or disposal of the information.

A privacy impact assessment is a tool to identify risks and mitigation strategies associated with the use of personal health information. It is an essential tool for ensuring compliance with the privacy requirements set out in *PHIA* and is a building block of a good privacy management program.¹⁴

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. PIAs are “evergreen”. This means that they should be completed at the conceptual, design and implementation phases of each project and should be periodically reviewed to ensure that no new risks have emerged and to confirm that all mitigation strategies have been properly implemented. 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 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 or health custodian to ensure that they comply with their responsibilities under the relevant legislation. Visit us at: <https://oipc.novascotia.ca/>

¹⁴ For more information about Privacy Management Programs visit the website of the Office of the Information and Privacy Commissioner website at: <https://oipc.novascotia.ca/>

Privacy Impact Assessment

Project Name: _____

Document Version, Review and Approval History

Version	Author	Nature of Change	Date

Document Owner

Name	Organization	Title

Document Sign-Off

Name	Organization	Title	Signature	Date

Table of Contents

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
5. Key Program or Service Dates

B. Description

1. Description of the Initiative
2. Scope of this PIA
3. Conceptual Technical Architecture
 - a. Logical Architecture
 - b. Technical Interfaces
4. Elements of Personal Health Information
5. Description of Information Flow – Text & Diagram

C. Authority to Collect, Use and Disclose Personal Health Information

1. Limiting Collection, Use and Disclosure
2. Legal Authority for Collection, Use and Disclosure
3. Legal Authority for Disclosure and Storage Outside of the Province

D. Access Rights for Individuals

1. Access to Information Requests
2. Correction & Accuracy
3. Consent Directives
4. Record of User Activity
5. Retention
6. Access or Privacy Complaints

E. Security of Personal Health Information

1. Reasonable Security
2. Access Matrix

F. Risk Identification & Mitigation

G. Action Plan

Appendices

Appendix A: Sample flow of PHI

Appendix B: Sample summary of authorities under *PHIA*

Appendix C: Sample risk identification & mitigation table

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
5. Key Program or Service Dates

List key program and service dates including those listed in the table below:

Milestone	Due Date	Completion Date
Project initiation		
PIA Commencement		
PIA Completion		
PIA Review		
Threat & Risk Assessment		
Vendor Conformance testing		
Go Live Date		

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. **Conceptual Technical Architecture**
 - a. Logical Architecture - describe
 - b. Technical Interfaces - describe
4. **Elements of personal health information:** List the personal health information data elements involved in the initiative. This could include citizen's name, family member names, age, address, educational history, work status, health information, test results, clinical notes, financial information, photos, personal health card number.
5. **Description of Information Flow (include text and diagram):**

Describe the following information flows:

 - (i) Intended information flow for the new project, program or system. Insert information flow diagram here (see sample at Appendix A). Describe the purposes for collection, use and disclosure of personal health information as illustrated.
 - (ii) If planned, describe how a pilot phase and/or limited roll out flow will occur.
 - (iii) Describe:
 - How the system will implement a patient's requests for her own phi.
 - How the system will implement consent directive to mask phi.
 - How the system will process a record of user activity request.
 - How the system vendor will provide business/technical support.

As noted above, 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 health information, you can stop here and submit this document to your privacy officer.

C. Collection, Use and Disclosure of Personal Health 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 privacy 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 custodian 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 health 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 health 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 C. 2.

- 2. Legal Authority for the Collection, Use and Disclosure of Personal Health Information:** For each of the collection, use and disclosures identified, evaluate the health custodian’s legal authority and complete the following table. Refer to **Appendix B** for a sample of the legal authority tables.

For each type of personal health information collected, complete the following table. Group personal health information types in broad categories such as: client demographic information, medications, test results, allergies and intolerances information, patient observation information, immunization information etc.

Data element	Rationale for collection, use or disclosure		Method of collection	
	Consent (identify lawful purpose)	Permitted or required by law (identify law)	Direct	Indirect (State authority)

3. Legal Authority for storage or disclosure outside the Province

Section 44 provides that a custodian may disclose personal health information about an individual collected in the Province to a person outside the Province in limited circumstances.

- a. Will personal health information be disclosed or stored outside of the Province?
- b. If so, describe the circumstances, reason and the legal authority for disclosure or storage outside of the Province (refer to sections 44(1) (a) – (e)).

D. Access Rights for Individuals

1. Access to Information Requests (s. 71)

Using a diagram and narrative steps explain how the custodian will respond to requests by patients for access to their own personal health information.

2. Correction and Accuracy (s. 85-99)

- a. How is an individual's information updated or corrected?
- b. If personal health information has been disclosed to others, how will the custodian notify them of the update or correction?

3. Consent Directives (s. 17)

Describe how the system will implement consent directives to limit (mask) or revoke an individual's consent to the collection, use or disclosure of personal health information?

4. Record of User Activity (s. 63)

Describe how the system will process a record of user activity request.

5. Retention (s. 50, Reg. s. 11(3))

- a. Confirm that the custodian has an approved written retention schedule that applies to the personal health information affected by this project (s. 50).
- b. How will the custodian ensure that the retention schedule is regularly applied to personal health information collected by virtue of this project?
- c. Confirm that the custodian has an approved written retention schedule that includes a requirement that information that was used to update a record of user activity related to an individual's personal health information is retained for at least one year after each date of access (reg. s. 11(3)).

6. Access or Privacy Complaints (s. 91, s. 62)

- a. Describe how individuals will be informed of their rights to make an access or privacy complaint to the Information and Privacy Commissioner.
- b. Confirm that the custodian has an approved complaints policy (s. 62(2)).

E. Security of Personal Information (s. 62, s. 65, Regulation s. 10)

1. **Reasonable security:** *PHIA* requires that custodians protect personal health information by making reasonable security arrangements against such risks as theft, loss, unauthorized access, use, disclosure, copying or modification of information. (s. 62).
 - a. **Administrative safeguards** – Describe administrative safeguards (such as policies, training, contract provisions, consent forms etc.).
 - b. **Technical Safeguards**
 - i. Describe technical safeguards (such as passwords and user ID, authentication, encryption, firewalls and intrusion detection, secure transmission, disaster recovery).
 - ii. Describe all additional technical safeguards implemented in compliance with Regulation s. 10 (network infrastructure, hardware, software).
 - 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, complete and append a security threat and risk assessment. As part of that assessment, you may also need to complete vulnerability and penetration testing.

2. **Access Matrix (s. 25):** Personal health information should only be used and disclosed as permitted under *PHIA*. Access to personal health information must be limited to those employees whose job responsibilities require that they access the personal health information (need to know). Attach a copy of the user access matrix. A user access matrix lists all of the position types (eg. clerical, head nurse, nursing assistant) across one axis and all of the personal health 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.

F. Risk Identification & 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 C** for examples of risks and mitigation strategies.

Risk Mitigation Table

	Risk	Mitigation Strategy	Likelihood	Impact
1				
2				
3				
4				

G. Action Plan

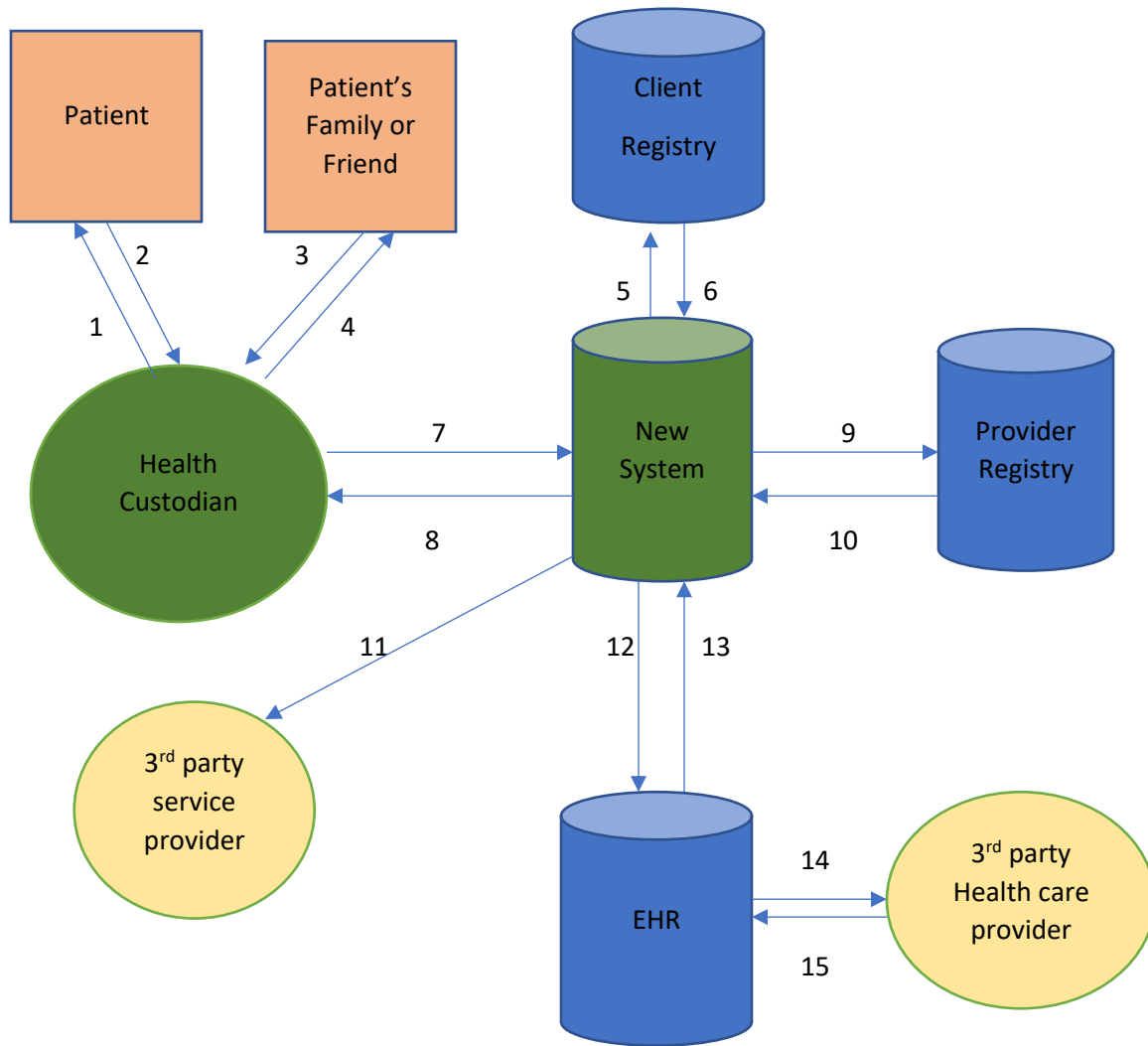
The purpose of this section is to provide an action plan to implement the recommendations listed in section F to reduce the privacy risks that have been identified. This section will provide a mechanism to track the recommendations, as well as describe responses to the recommendations of the PIA. Ensuring 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		
Risk	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.

Appendix A: Sample Flow of PHI



In the narrative explain each arrow into new system (collection) and each arrow out (disclosure).

Appendix B: Sample Summary of Authorities Under *PHIA*

Client Demographic Information

Data element	Rationale for collection, use or disclosure		Method of collection	
	Consent (identify lawful purpose)	Required by law (identify law)	Direct	Indirect (State authority)
Client name	Required to correctly identify the individual		√	
Client HCN	Same		√	√ Consent, if individual unable to recall get from Client Registry
Client date of birth	Same		√	

Immunization Information

Data element	Rationale for collection, use or disclosure		Method of collection	
	Consent (identify lawful purpose)	Required by law (identify law)	Direct	Indirect (State authority & source of data)
Adverse reaction indicator	Required to provide service			√ Consent – client authorized indirect collection from DIS
Immunization date	Required to provide service		√	√ Consent – when client unable to recall dates, from immunization data base (specify)
Immunization type	Required to provide service		√	√ Consent – when client unable to recall dates, from immunization data base (specify)

Audit Log Information

Data element	Rationale for collection, use or disclosure		Method of collection	
	Consent (identify lawful purpose)	Required by law (identify law)	Direct	Indirect (State authority & source of data)
Date/time of record access		63(1) PHIA To identify date & time the access to the patient record occurred		System generated (upload), s. 31(k) & s. 63(1) PHIA
Description of access (type of transaction)		63(1) PHIA Description of type of access to allow assessment of authorization to access		System generated, s. 31(k) & s. 63(1) PHIA
User ID		63(1) PHIA To identify user		System generated, s. 31(k) & s. 63(1) PHIA
User Name		63(1) PHIA To identify user		System generated, s. 31(k) & s. 63(1) PHIA
User Location ID		63(1)PHIA To identify user location – assists with assessing authorization		System generated, s. 31(k) & s. 63(1) PHIA
Patient ID		63(1) PHIA unique patient ID assigned in patient registry		User input or system generated, necessary to create audit log 31(k) & s. 63(1) PHIA
Patient Name		63(1) PHIA first and last name of patient		User input, necessary to create audit log 31(k) & s. 63(1) PHIA

Appendix C: Sample risk identification & mitigation table

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 custodian	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 custodian 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 health 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

A large, solid blue oval shape centered on a white background.

Tab 8

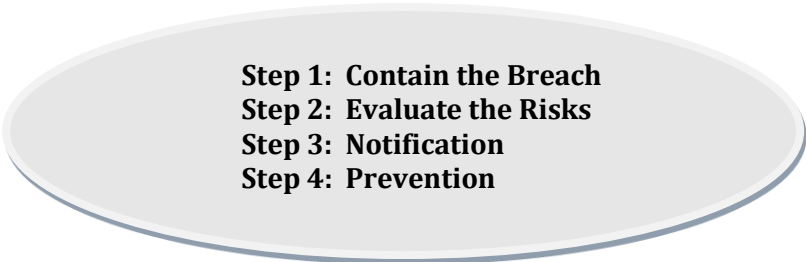


Key Steps to Responding to Privacy Breaches¹⁵

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 (Tab 9 of this toolkit) also available on our website at <https://oipc.novascotia.ca/>.

¹⁵ 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 Tab 9 of this toolkit 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.¹⁶

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;

¹⁶ 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/>.

A large, solid blue oval shape centered on a white background.

Tab 9



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.¹⁷ 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?

¹⁷ 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 on page 16.

(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 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 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,¹⁸ 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?

¹⁸ 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/>.

A large, solid blue oval shape centered in the upper half of the page, serving as a background for the text.

Tab 10

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/sites/default/files/publications/Key%20Steps%20-%20Full%20-%20Final%20-%202015Oct27_0_0.pdf

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.• Conduct a full assessment of the breach – complete the privacy breach checklist (Appendix 2).

	<ul style="list-style-type: none"> • 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		a) Remove, move or segregate exposed information or files. b) Preserve evidence. c) Determine whether personal information was further disclosed to others (verbally or via copies). d) Document the steps taken.

Preliminary Assessment	Yes/ No	Suggested Containment Strategies
leave, home telephone numbers, slides of PowerPoint presentations that contain personal information, etc.)?		e) Complete this <i>Preliminary Report</i> and contact the Chief Privacy Officer.
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.¹⁹ 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?

¹⁹ The OIPC can be reached by phone at 902-424-4684 or 1-866-243-1564, by fax at (902) 424-8303 and by email at oipcns@novascotia.ca.

Steps 1 & 2: Containment & Risk Evaluation

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

(1) Containment

Check all of the factors that apply:

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

Describe any other containment strategies used:

(2) Nature of Personal Information Involved

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

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

(3) Relationship

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

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

(4) Cause of the Breach

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

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

(5) Scope of the Breach

How many people were affected by the breach?

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

(6) Foreseeable Harm

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

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

(7) Other Factors

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

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

Risk Evaluation Summary:

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

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

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

Step 3: Notification

(1) Should affected Individuals be Notified?

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

Consideration	Description	Factor applies
Legislation	Health custodians in Nova Scotia must comply with sections 69 & 70 of <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,²⁰ 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?

²⁰ 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 oval shape centered on a white background.

Tab 11

PHIA Index			
1	Title	Research	
2	Purpose	52	Definitions
3	Definitions	53	Planning & management is not research
4	Personal Health Information – exception	54	Minimum amount necessary
Application of the Act		55	Use for research requirements – custodian reqts
5	Act applies to custodian, not to stats, s/c privilege	56	Disclosure for research – researcher reqts
6	Act does not apply, agents	57	Disclosure without consent
7	Conflicts	58	Forms
8	FIPPA	59	Research plan requirements
9	Act does not apply (regulated health professions, tribunals etc.)	60	Research agreement
10	Consent and authority without consent	Practices to Protect PHI	
Consent		61	Requirement to protect confidentiality
11	Basic consent rule	62	Information practices required – policy
12	Express v. Knowledgeable implied consent	63	Record of user activity
13	Knowledgeable implied consent requirements	64	ROUA – frivolous & vexatious + RO
14	Knowledgeable	65	Electronic information system security
15	Notice – for reasonable belief of knowledge	66	Custodian restrictions with disclosure
16	Express consent – oral or written	67	Contact person
17	Revocation of consent	68	Public statement requirement
18	Age	Reporting a Privacy Breach	
19	Capacity	69	Notification to individual
20	Capacity	70	Notification to RO
Substitute Decision Maker		Access to an Individual's Own PHI	
21	List of & requirements to act	71	Right
22	Guidance to SDM	72	When access can be refused
23	Proof	73	When consultation with health prof. required
Collection, Use and Disclosure		74	FIPPA & agents of public body
24	General rule no cud if other info will serve purpose	Process for Requesting Access	
25	Minimum necessary, need to know	75	Request in writing, fees
26	Application of 24 & 25	76	Insufficient detail
27	Health card number – collection & use	77	Waiver of requirements
28	Agent permissions & notification of breach	78	No reasons required
29	Agent – use not disclosure	79	Must identify requester
Collection		80	Act does not prevent other disclosure
30	Collection authorized	81	Frivolous & vexatious
31	Direct collection & Indirect authorizations	82	Fees
32	Express consent	83	No fee from Minister
Use		84	Time limit
33	Use authorized	Correction	
34	Express consent	85	Request permitted
35	Use without consent	86	Deemed refusal
Disclosure		87	When request shall be granted
36	Custodian to custodian	88	Correction requirements
37	Disclosure to family & friends	89	Frivolous & vexatious
38	Disclosure without consent - RO & pmf	90	Process for frivolous & vexatious
39	Disclosure to non-custodian with Minister's consent	Review & Oversight	
40	Deceased individuals	91	Right to request review
41	Consent	92	Powers of RO
42	Documentation of disclosure without consent	93	RO estimates & annual report
43	Express consent	94	Process to request review
44	Out of province disclosures	95	Power of RO not to review
45	Non custodian may collect authorized disclosures	96	Mediation
46	Health Card Number database	97	Review in private
Retention, Destruction, Disposal & De-Identification		98	Representations
47	Paper and electronic records	99	Power to request production
48	Information practices required	100	Requirements on completing review
49	Secure destruction	101	Custodian obligations on receiving report
50	Written retention schedule required	102-03	Appeal to SC & powers of SC
51	Requirement to follow retention schedule	General	
		104-05	No discipline, proceedings for good faith action
		Offences & Penalties	
		106-15	Offences, review, regulation, repeals

A large, solid blue oval shape centered on a white background.

Tab 12



Personal Health Information Act - Privacy Rules At a Glance

A. Collection

- General Rule
- Best Practices
- Collection by non-custodian
- Indirect Collection

B. Use

- General Rule
- Best Practices
- Use by non-custodian
- Use by Agent
- Uses authorized or permitted under PHIA

C. Disclosure

- General Rule
- Best Practices
- Disclosures without consent – effect of authority
- Disclosures without consent – documentation required
- Disclosures by non-custodians
- Disclosures authorized or permitted under PHIA
 - Disclosures by recipient
 - Disclosures by purpose
 - Disclosures outside NS
 - Disclosures of deceased's phi

D. Health Card Number Rules

E. Consent Rules

F. Agents

G. Retention, Destruction, Security, Breach Reporting

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 *Personal Health Information Act* at <https://nslegislature.ca/sites/default/files/legc/statutes/personal%20health%20information.pdf>

A. Collection	
11	<p>General Rule Health custodians shall not collect personal health information (“phi”) unless</p> <ul style="list-style-type: none"> • The custodians has the individual’s consent <u>and</u> the collection is reasonably necessary for a lawful purpose or • The collection is permitted or required by this Act
24	<p>Best Practice Requirements:</p> <ol style="list-style-type: none"> 1. Collect non- phi first: A custodian shall not collect phi if other information will serve the purpose of collection 2. Minimum necessary: Collection of phi must be limited to the minimum amount of phi necessary to achieve the purpose for which it is collected. <p>Application of s. 24 and 25 rules:</p> <ul style="list-style-type: none"> • These rules apply where the custodian is authorized to collect phi with knowledgeable implied consent, without consent and without consent unless the individual objects • These rules do not apply to phi that a custodian is required by law to collect
25(1)	
26(1)	
26(2)	
45(1)	<p>Collection by non- custodian</p> <ul style="list-style-type: none"> • A non-custodian is authorized to collect the phi that a custodian may disclose to it but does not become a custodian merely by virtue of the collection • A prescribed entity that is not a custodian is authorized to collect the phi that the custodian may disclose to the prescribed entity under clause 38(1)(j)
38(5)	
31	<p>Indirect collection A custodian shall collect directly from the individual about whom the information is being collected except:</p> <ol style="list-style-type: none"> a. Consent: If the individual authorizes indirect collection b. Substitute Decision Maker: The collection is from the substitute decision-maker (“SDM”) if the SDM has authority to act c. Inaccurate or not timely: The information is reasonably necessary for providing health care and it is not reasonably possible to collect directly from the individual phi that can be reasonably relied on as accurate or phi in a timely manner d. Safety: direct collection would prejudice the safety of any individual e. Family history: collection is to assemble family history in the context of providing health care f. Eligibility for program: collection is in the course of processing an application for a benefit or program g. Breach of agreement or proceedings: The custodian is a public body under FOIPOP and is collecting the information for a purpose related to investigating a breach of an agreement, to conduct a proceeding or in relation to a statutory function of the custodian h. Research: Custodian is collecting for a research project approved by a research ethics board i. Prescribed entity: Custodian is a prescribed entity j. Treaty or agreement: Custodian collects the info from a person who is permitted or required by law, treaty or agreement made under this or another Act to disclose it to the custodian k. Permitted or required by law: Custodian collects as permitted or required by law or treaty l. Minister of Health: Collection by minister for the purpose of planning or managing the health system m. Quality or standards of care: Collection is for the purpose of ensuring quality or standards of care within a quality review program n. Payments: collection is reasonably necessary for the administration of payments in connect with the provision for health care o. Minister of Health: Collection is from another custodian for the purpose of creating or maintaining an electronic health record

B. Use	
11	General Rule Health custodians shall not use personal health information unless <ul style="list-style-type: none"> • The custodians has the individual's consent <u>and</u> the use is reasonably necessary for a lawful purpose or • The use is permitted or required by this Act
24 25(1) 25(2)(a) 26(1) 26(2)	Best Practice Requirements: <ol style="list-style-type: none"> 1. Use non-phi first: A custodian shall not use phi if other info will serve the purpose of the use 2. Minimum necessary: Use of phi must be limited to the minimum amount of phi necessary to achieve the purpose for which it is used. 3. Agents need to know: Use of phi by agents of custodian shall be limited to those of its agents who need to know the information to carry out the purposes for which it was collected or a purpose authorized under this Act Application of s. 24 and 25 rules: <ul style="list-style-type: none"> • These rules apply where the custodian is authorized to use phi with knowledgeable implied consent, without consent and without consent unless the individual objects • These rules do not apply to phi that a custodian is required by law to use
45(2)(a) 45(2)(b)	Use by non-custodian A non-custodian (to whom a custodian has disclosed phi) shall not use phi for any purpose other than <ul style="list-style-type: none"> • For the purpose the custodian was authorized to disclose the information under PHIA or • For the purpose of carrying out a legal duty A non-custodian shall not use more information than is reasonably necessary to meet the purpose of the use, unless the use is required by law.
25(2)(a) 29(1) 29(2) 33(c) 35(2)	Use by agent <ul style="list-style-type: none"> • Need to know: Use of phi by agents of custodian shall be limited to those of its agents who need to know the information to carry out the purposes for which it was collected or a purpose authorized under this Act • Authority: Where a custodian is authorized to use phi for a purpose, the custodian may provide the information to an agent who may use it for that purpose on behalf of the custodian. • Use not disclosure or collection: For the purpose of PHIA, the providing of phi between a custodian and an agent of the custodian is a use by the custodian and not a disclosure by the custodian or a collection by the agent • Education: A custodian may use phi for educating agents to provide health care • Non-consensual use: Where custodian is authorized to use phi without consent, the custodian may provide the information to an agent of the custodian who may use if for that purpose on behalf of the custodian
33	Uses permitted or required under PHIA <ol style="list-style-type: none"> a) Use for original purpose: A custodian may use phi for the purpose for which the information was collected or created and for all the functions reasonably necessary for carrying out that purpose b) For purposes which this Act or another Act permit or requires a personal to disclose it to the custodian or c) For the purpose of educating agents to provide health care.

Uses Authorized or Permitted Under PHIA				
Type of information or use	PHIA provision	Express Consent	Implied Consent	No consent = statutory authority
Circle of care – within health care facilities	12, 25(2)(a)		•	•
Consent – may use phi to seek consent – limited to name & contact info	35(1)(e)			•
De-identification	35(1)(d)			•
Educating agents to provide health care	33(c)			•
Electronic Health Record – to create or maintain if the custodian is the Minister	35(1)(ha)			•
Fraud prevention – detect & monitor unauthorized receipt of services or benefits	35(1)(b)			•
Fundraising activities	34(a)	•		
Law – for a purpose permitted under PHIA or another Act	33(b)			•
Law – permitted or required by law or treaty made under PHIA or another Act	35(1)(i)			•
Legal proceeding	35(1)(f)			•
Market research, commercial purpose	34(b)	•		
Original purpose collected and functions reasonably necessary to carry out that purpose	33(a)			•
Payment processing – obtaining, verifying reimbursing claims for payment	35(1)(g)			•
Planning and delivery or programs	35(1)(a)			•
Quality review program	35(1)(c)			•
Research conducted by the custodian <ul style="list-style-type: none"> • Must use minimum amount of info necessary (s. 54) • Must comply with s. 55 	35(1)(h)			•
Risk Management	35(1)(j)			•

C. Disclosure	
11	<p>General Rule</p> <p>Health custodians shall not disclose personal health information unless</p> <ul style="list-style-type: none"> • The custodians has the individual's consent <u>and</u> the disclosure is reasonably necessary for a lawful purpose or • The disclosure is permitted or required by this Act
24	<p>Best Practice Requirements</p> <ol style="list-style-type: none"> 1. Disclose non-phi first: A custodian shall not disclose phi if other information will serve the purpose of disclosure 2. Minimum necessary: Disclosure of phi must be limited to the minimum amount of phi necessary to achieve the purpose for which it is disclosed. 3. Circle of care – facilities: Custodians shall limit disclosure of phi to those regulated health professionals who have the right to treat individuals in the custodian's health care facility, to only that information that the health professionals require to carry out their duties and responsibilities 4. Circle of care – generally: Custodians may disclose phi to a custodian involved in the individual's health care if the disclosure is reasonably necessary for the provision of health care to the individual <p>Application of s. 24 and 25 rules:</p> <ul style="list-style-type: none"> • These rules apply where the custodian is authorized to disclose phi with knowledgeable implied consent, without consent and without consent unless the individual objects • These rules do not apply to phi that a custodian is required by law to disclose
25(1)	
25(2)(b)	
36	
26(1)	
26(2)	
10(2)	<p>Disclosures without consent – effect of authority</p> <p>A provision in this Act that permits a custodian to disclose phi without consent</p> <ul style="list-style-type: none"> • does not require the custodian to disclose it unless required to do so by law, • does not relieve the custodian from a legal requirement to disclose the information and • does not prevent the custodian from obtaining the individual's consent for the disclosure or giving notice to the individual of the disclosure
41(1)	
42(1)	<p>Disclosures without consent – documentation required</p> <ul style="list-style-type: none"> • Disclosures without consent must be documented • Documentation must include: <ul style="list-style-type: none"> ○ Description or copy of phi disclosed ○ Name of person or organization to whom the phi was disclosed ○ Date of disclosure ○ Authority for disclosure
45(2)	<p>Disclosure by non-custodian</p> <p>A non-custodian (to whom a custodian disclosed the phi) shall not disclose phi for any purpose other than</p> <ul style="list-style-type: none"> • For the purpose the custodian was authorized to disclose the information under PHIA or • For the purpose of carrying out a legal duty
45(3)	

Disclosures authorized or permitted under PHIA				
Type of information or disclosure	PHIA provision	Express Consent	Implied Consent	No consent = statutory authority
Disclosure by Recipient				
CIHI – Canadian Institute for Health Information <ul style="list-style-type: none"> For planning and management 	38(1)(i)			•
Circle of care <ul style="list-style-type: none"> Generally Within custodian's facility 	12, 36 12, 25(2)(b)		• •	• •
Family/Close personal relationship <ul style="list-style-type: none"> Information related to deceased family member General information about presence & general condition of individual on day information not contrary to express request 	40(1) & (2) 37		•	• •
Correctional Facility <ul style="list-style-type: none"> to allow the provision of health care 	38(1)(e)			•
Custodian <ul style="list-style-type: none"> Reasonably necessary for the provision of care Not for health care To prevent fraud, an offence or assist in investigation under enactment Within a quality review program To determine or verify eligibility for insured services 	36 43(b) 38(1)(a) 38(1)(f) 38(1)(m)	•	•	• • •
Legal Advisor <ul style="list-style-type: none"> An agent who receives phi for the purpose of a proceeding or contemplated proceeding may disclose the information the agent's or former agent's professional advisor for the purpose of providing advice or representation 	38(7)			•
Legal Guardian <ul style="list-style-type: none"> acting on behalf of the individual 	38(1)(b)(ii)			•
Litigation Guardian <ul style="list-style-type: none"> for purpose of appointment to commence or defend legal action 	38(1)(o) 38(1)(p)			• •
Media	43(e)	•		
Minister <ul style="list-style-type: none"> For planning and management of health system For purpose of creating or maintaining an EHR 	38(1)(g) 38(1)(u)			• •

Type of information or disclosure	PHIA provision	Express Consent	Implied Consent	No consent = statutory authority
Disclosure by Recipient continued				
Non-custodian <ul style="list-style-type: none"> Generally unless authorized by law To avert or minimize an imminent risk to any person For risk management within the custodian's organization To facilitate assessment, care or treatment and with authorization of Minister Administration of payments for health care Risk management or patient safety within the custodian's organization 	43(a) 38(1)(d) 38(1)(t) 39 38(1)(r) 38(1)(t)	•		• • • • •
Prescribed entities <ul style="list-style-type: none"> For planning and management subject to conditions in 38(2) 	38(1)(j)			•
Prescription Monitoring Board <ul style="list-style-type: none"> For monitoring prescriptions pursuant to the Prescription Monitoring Act 	38(1)(h)			•
Provincial or territorial government <ul style="list-style-type: none"> From the Province to another for planning and management 	38(1)(k)			•
Representative, litigation guardian, administrator <ul style="list-style-type: none"> To persons acting on behalf of the individual Proposed litigation guardian or legal representative for the purpose of having them appointed as such Litigation guardian or legal representative authorized to commence or defend a proceeding 	38(1)(b) 38(1)(o) 38(1)(p)			• • •
Regulated health profession body <ul style="list-style-type: none"> For the purpose of carrying out its duties under provincial or federal law 	38(1)(c)			•
Researcher – unless s. 57 applies	38(1)(f)	•		
Researcher – with plan, REB approval and agreement	57			•
Substitute Decision Maker <ul style="list-style-type: none"> Person legally entitled to make health-care decisions on behalf of the individual Legal Guardian Estate Administrator 	38(1)(b)(i) 38(1)(b)(ii) 38(1)(b)(iii)			•
Within health care facility/custodian organization <ul style="list-style-type: none"> Circle of care disclosures Risk management or patient safety 	25(3) 38(1)(t)		•	• •

Type of information or disclosure	PHIA provision	Express Consent	Implied Consent	No consent = statutory authority
Disclosure by purpose				
Administer estate <ul style="list-style-type: none"> To the administrator of an estate if the disclosure is for the purpose of the estate 	38(1)(b)(iii)			•
Eligibility for insured services <ul style="list-style-type: none"> To another custodian to verify or determine eligibility for insured services Administration of payments in connection with health care 	38(1)(m) 38(1)(r)			•
Electronic Health Record <ul style="list-style-type: none"> To Minister for the purpose of creating or maintaining an HER 	38(1)(u)			•
Family concerns <ul style="list-style-type: none"> Information related to deceased family member General information about presence & general condition of individual on day information not contrary to express request 	40(1) & (2) 37		•	•
Fraud or offence detection & prevention <ul style="list-style-type: none"> To another custodian to prevent or assist an investigation of fraud in the use of health services or prevent commission of offence 	38(1)(a)			•
Fund raising	43(c)	•		
Insured services <ul style="list-style-type: none"> To another custodian to verify or determine eligibility for insured services 	38(1)(m)			•
Law, treaty or arrangement <ul style="list-style-type: none"> Disclosures required or permitted by law, treaty or arrangement made pursuant to PHIA or another Act 	38(1)(l)			•
Legal proceedings <ul style="list-style-type: none"> For purpose of legal proceeding in which the custodian or agent is a party or witness To appoint litigation guardian or legal representative To commence or defend litigation To comply with summons, order or procedural rule 	38(1)(s) 38(1)(o) 38(1)(p) 38(1)(q)			• • •
Marketing and service for a commercial purpose	43(d)	•		
Market research	43(d)	•		
Offence prevention <ul style="list-style-type: none"> To another custodian if the disclosure will prevent the commission of an offence under and enactment 	38(1)(a)			•
Payment for healthcare	38(1)(r)			•
Prescription monitoring – to PM Board only	38(1)(h)			•

Type of information or disclosure	PHIA provision	Express Consent	Implied Consent	No consent = statutory authority
Disclosure by purpose continued				
Planning & management of the health system <ul style="list-style-type: none"> • CIHI in accordance with agreement • Minister • Prescribed entities • Provinces & territories • Planning & management does not = research 	38(1)(i) 38(1)(g) 38(1)(j) 38(1)(k) 53			• • • •
Quality review program	38(1)(f)			•
Regulation of professions (to colleges) <ul style="list-style-type: none"> • Information required for the purpose of carrying out its duties under an Act 	38(1)(c)			•
Research generally (unless s.57 applies)	43(f)	•		
Risk management within the custodian's organization	38(1)(t)			•
Safety – to avert or minimize imminent danger	38(1)(d)			•
Treatment related <ul style="list-style-type: none"> • To correctional facility in which the individual is being lawfully detained to allow the provision of health care • To custodian where reasonably necessary for provision of care (circle of care) • To non-custodian for the purpose of facilitating assessment, care or treatment with authorization of Minister • To person acting on behalf of the individual who is legally entitled to make health care decisions • To family member or close relationship information about presence and condition • Outside NS where reasonably necessary for the provision of health care and no express instruction to the contrary 	38(1)(e) 36 39 38(1)(b) 37 44(1)(e)	 •	 •	• • • •
Disclosure outside NS				
Outside NS – generally with consent	44(1)(a)		•	
Outside NS – permitted by PHIA	44(1)(b)			•
To a regulated health professional – prescription monitoring	44(1)(c)			•
Planning and management of health care	44(1)(d)			•
Info relates to health care provided in NS to an individual who resides outside NS	44(1)(d)			•
To the government of a province or Canada	44(1)(d)			•
Reasonably necessary for provision of health care	44(1)(e) 44(2)	•		•

Type of information or disclosure	PHIA provision	Express Consent	Implied Consent	No consent = statutory authority
Deceased (PHI relating to deceased persons)				
• For the purpose of identifying the individual	40(1)(a)			•
• To inform any person that the individual is deceased	40(1)(b)			•
• To listed relatives if the information is needed to make health care decisions	40(1)(c)			•
• For carrying out the deceased person's wishes for the purpose of tissue donation	40(1)(d)	•		
• Info relating to circumstances of death to family members or close personal relationship – so long as not contrary to a prior express request of the individual	40(2)		•	•
• To estate administrator for purpose of the estate	38(1)(b)(iii)			•

D. Health Card Number Rules	
27	A person who is not a custodian or authorized by the regulations (reg. 6) shall not collect or use an individual's health card number
Reg. 6	For the purposes of clause 27 the following non-custodians are authorized to collect and use an individual's health card number for the purposes specified: <ul style="list-style-type: none"> • WCB – assess worker's entitlement to benefits • MCS – facilitate health care for children, indicate eligibility for pharmacare program, determine benefits • MSNS and MR – Vital Statistics division for registering births and deaths • Office of Public Trustee – facilitate health care decisions for clients • Mi'kmaw First Nations band to create and maintain NS FN Client Linkage Registry
Reg. 7	Non custodian is authorized to collect and use an individual's health card number for the purposes of facilitating the provision of insured services
46	Notwithstanding any enactment except the Juries Act and the Elections Act the Minister has the sole authority for deciding who may have access to the information in the health card number database, the Common Client Registry or any successor client information system related to the health card number.

E. Consent Rules Summary	
11	General Rule A custodian shall not collect, use or disclose ("cud") phi unless <ul style="list-style-type: none"> • The custodian has the individual's consent under this Act and the cud is reasonably necessary for a lawful purpose; or • The cud is permitted or required by this Act
10(1)	"With consent" rule doesn't affect "without consent" rules <ul style="list-style-type: none"> • A provision of this Act that applies to cud of phi with consent, does not affect the cud that this Act permits or requires without consent
12	Knowledgeable implied consent - acceptable Unless this Act requires express consent or makes exception to the requirement for consent, knowledgeable implied consent may be accepted as consent for cud of phi
32, 34, 43	Express consent requirements <ul style="list-style-type: none"> • Express consent is required for <u>collection and use</u> of phi for market research, marketing any service for a commercial purpose and fundraising • Express consent is required for <u>disclosure</u> of phi <ul style="list-style-type: none"> ○ By custodian to non-custodian unless required or authorized by law ○ By a custodian to another custodian if it is not for the purpose of providing health care unless required or authorized by law ○ For fund-raising activities ○ For market research or marketing any service for a commercial purpose ○ To media ○ To a personal or organization for the purpose of research unless provided for in s. 57
13	Requirements for consent For both knowledgeable implied consent and express consent, the consent must: <ul style="list-style-type: none"> • Be a consent of the individual • Be knowledgeable • Relate to the specific information at issue and • Be voluntary
14	"Knowledgeable" Consent to cud of phi is knowledgeable if it is reasonable in the circumstances to believe that the individual knows: <ul style="list-style-type: none"> • The purpose of the cud as the case may be and • That the individual may give or withhold consent

Consent Rules continued

15	“Reasonable” It is reasonable to believe that an individual knows the purpose of cud of phi if the custodian: <ul style="list-style-type: none"> • Makes readily available a notice describing the purpose in a manner that the purpose is likely to come to the individual’s attention or • Explains the purpose to the individual • Unless language or reading barrier
17	Revocation An individual may limit or revoke consent to collection, use or disclosure of phi. <ul style="list-style-type: none"> • Revocation is not retroactive • Custodian must take reasonable steps to comply • Custodian shall inform the individual of the consequences of limiting or revoking consent • Custodian shall notify custodian to whom phi is disclosed of limitations • Revocation does not apply to phi that a custodian is required by law to cud
18	Age & capacity Any capable individual, regardless of age may consent or withdraw consent for the purpose of PHIA
20	Capacity includes Where an individual is deemed to have the capacity to consent to cud of phi, this capacity includes disclosure to a parent, guardian or substitute decision-maker where applicable.
3(b)	Definition of “capacity” Means the ability to understand information that is relevant to the making of a decision related to the cud of phi and the ability to appreciate the reasonably foreseeable consequences of a decision or lack of decision
	Substitute decision maker Consent to cud may be given by a substitute decision maker (SDM) if the individual lacks the capacity to make the decision

F. Agents	
3(a)	Agent , in relation to a custodian means a person who, with authorization of the custodian, acts for or on behalf of the custodian in respect of phi. Includes an employee, volunteer, insurer, lawyer or liability protection provider.
6(2)	Regulated health professionals: Except as prescribed, a regulated health professional is not a custodian in respect of phi that the person collects, uses or discloses while performing the person's powers or duties when an agent of a custodian.
28	General rule: A custodian may permit the custodian's agent to cud, retain, destroy or dispose of phi on the custodian's behalf only if: <ul style="list-style-type: none"> • The custodian is permitted or required to cud, retain, destroy, or dispose of the phi • The cud, retention, destruction or disposition of the information is in the course of the agent's duties and not contrary to the limits imposed by the custodian, this Act or another law <u>and</u> • The prescribed requirements, if any, are met (none currently)
25(2)(a)	Use <ul style="list-style-type: none"> • Need to know: Use of phi by agents of custodian shall be limited to those of its agents who need to know the information to carry out the purposes for which it was collected or a purpose authorized under this Act • Authority: Where a custodian is authorized to use phi for a purpose, the custodian may provide the information to an agent who may use it for that purpose on behalf of the custodian. • Use not disclosure or collection: For the purpose of PHIA, the providing of phi between a custodian and an agent of the custodian is a use by the custodian and not a disclosure by the custodian or a collection by the agent • Education: A custodian may use phi for educating agents to provide health care • Non-consensual use: Where custodian is authorized to use phi without consent, the custodian may provide the information to an agent of the custodian who may use if for that purpose on behalf of the custodian
29(1)	
29(2)	
33(c)	
35(2)	
38(7)	Disclosure <ul style="list-style-type: none"> • An agent who receives phi for the purpose of a proceeding or contemplated proceeding may disclose the information the agent's or former agent's professional advisor for the purpose of providing advice or representation

G. Retention, Destruction, Security, Breach Reporting	
50(1) 51 49(2)	Retention Rule <ul style="list-style-type: none"> • Custodian must have a written retention schedule for PHI • Custodian must follow retention schedule • At expiry of relevant retention period PHI must be securely destroyed, erased or de-identified.
49(2)	Destruction Rule <ul style="list-style-type: none"> • Must securely destroy (erase or de-identify) phi at expiry of relevant retention period
61 62(c)	Security Rule <ul style="list-style-type: none"> • Custodian shall protect confidentiality of phi • Shall protect against theft, loss, unauthorized access to or use, disclosure, copying or modification of information
69 70	Breach Reporting <ul style="list-style-type: none"> • Must notify affected individual at first reasonable opportunity if the custodian believes information is stolen, lost, subject to unauthorized access, use, disclosure, copying and, as a result, there is a potential for harm or embarrassment to the individual • Where the custodian believes on a reasonable basis that there is no potential for harm or embarrassment, notification of the affected individual is not required but the custodian shall notify the Review Officer as soon as possible

A large, solid blue oval shape centered on a white background.

Tab 13



Personal Health Information Act

Disclosures Without Express Consent

Office of the Information and Privacy Commissioner for Nova Scotia

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, municipal body 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 Commissioner (Review Officer) will keep an open mind. It remains the responsibility of each public body, municipal body and health custodian to ensure that they comply with their responsibilities under the relevant legislation. Visit us at: <https://oipc.novascotia.ca>.

INTRODUCTION

Health custodians are entrusted with some of our most private and sensitive personal information. Traditionally, health custodians have carefully guarded that personal health information. But from time to time, other organizations request that health custodians disclose personal health information to them for some other purpose. For example, police may be investigating a crime and believe that their suspect suffered an injury for which he or she is likely to seek treatment at the local emergency department. They may seek information from the local emergency department in hopes of capturing their suspect. Is the identity of an individual at an emergency department personal health information? Can the health custodian disclose the information without the consent of the individual?

Another example is when a young adult seeks mental health treatment. If the young adult is at risk of harm to herself can the health custodian disclose personal health information to the young adult's parents? If so, under what circumstances?

These guidelines are designed to walk health custodians in Nova Scotia through a four-step process when they are faced with a request for disclosure of personal health information without consent. The four-step approach will help ensure that any disclosure takes into account the rules in the *Personal Health Information Act (PHIA)*.

To assist readers, each rule described below includes a reference to the relevant section of *PHIA*. Health custodians should always take the time to read the exact section of *PHIA* they are relying on to authorize a disclosure to ensure that the circumstances fit the rule.

GENERAL RULE

Under *PHIA*, a custodian must have the individual's consent to collect, use or disclose personal health information, or the collection, use or disclosure must be permitted or required by law (s. 11).

Express consent is required for the disclosure of personal health information by a custodian to a non-custodian unless required or authorized by law (s. 43). *PHIA* and other statutes provide authority for non-consensual disclosures in limited circumstances.

APPROACH

The analysis of whether or not a disclosure of personal health information is authorized under *PHIA* involves a four-step process:

1. Is the information in question “personal health information” within the meaning of *PHIA*?
2. Does *PHIA* permit the disclosure without the consent of the individual?
3. Even if authorized, should the health custodian disclose the information?
4. Has the authorized disclosure been properly documented?

PHIA defines disclosure as making the information available or releasing it to another person. Keep in mind that even if *PHIA* permits disclosure without consent, best practice is to get consent whenever possible (s. 41(1)). Where express consent is required, it can be given orally or in writing (s. 16).

Also note that providing information to an “agent” is not a disclosure under *PHIA* (s. 29(2)). An “agent” is defined in *PHIA* (s. 3(a)) and includes a person who, with the authorization of the custodian, acts for or on behalf of the custodian in respect of personal health information for the purposes of the custodian and not the agent’s purposes. Agents can include employees of a custodian, volunteers, insurer, lawyers retained by the custodian and liability protection providers. At the end of this document there is a discussion that explains the seven essential rules about sharing personal health information with agents.

Use the following table to determine if a disclosure of personal health information without consent is authorized.

PHIA DISCLOSURE DECISION TABLE

Step 1: Is the information “personal health information” (both recorded & unrecorded)?

If one or more of the following statements apply, the requested information is personal health information (phi) and so the *PHIA* disclosure rules also apply.

- | | |
|---|--|
| 1. The information relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family. | |
| 2. The information relates to the application, assessment, eligibility and provision of health care to the individual, including the identification of a person as a provider of health care to the individual. | |
| 3. The information relates to payments or eligibility for health care in respect of the individual. | |
| 4. The information relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance. | |
| 5. The information is the individual's registration information, including the individual's health card number. | |
| 6. The information identifies an individual's substitute decision-maker. | |

If one or more of the following statements apply, the *PHIA* disclosure rules do not apply.

- | | |
|--|--------------------|
| 1. Employee information: PHI does not include the identifying information contained in the record if the record relates primarily to an employee or agent of the custodian and the record is created or maintained primarily for a purpose other than the provision of health care or assistance in providing health care to the employee or agent. | Not phi |
| 2. Aggregate information: <i>PHIA</i> does not apply to statistical, aggregate or de-identified health information. | Not
<i>PHIA</i> |
| 3. Age of records: <i>PHIA</i> does not apply to records that are 120 years old or 50 years after the death of an individual (whichever is earlier). | Not
<i>PHIA</i> |

Step 2: Is the disclosure authorized?

If the information in question is personal health information within the meaning of *PHIA* (step 1), you must next determine whether the disclosure is authorized either because there is implied consent to the disclosure or because consent is not required.

Using the table below, identify all potential authorities for the proposed disclosure. It is very important to read each authority carefully and ensure that all of the requirements of the authority are met.

Implied consent

Health custodians may disclose personal health information based on implied consent in two circumstances:

1. **Provision of health care:** A custodian may disclose personal health information about an individual to a custodian involved in the individual's health care if the disclosure is reasonably necessary for the provision of health care to the individual (ss. 36 and 25(2)(b)).
2. **Family or close personal relationship:** A custodian may disclose personal health information to family or an individual in a close personal relationship if the information is given in general terms and concerns the presence, location and general condition of the individual on the day on which the information is disclosed and the disclosure is not contrary to the express request of the individual (s. 37).

Consent not required

A custodian may disclose personal health information without consent in limited circumstances as follows:

To another custodian:

1. If the custodian disclosing the information has a reasonable expectation that the disclosure will prevent or assist an investigation of fraud or prevent the commission of an offence under an enactment of a province or Canada (s. 38(1)(a)).
2. For the purpose of ensuring quality or standards of care within a quality review program (s. 38(1)(f)). Note in May 2015 this authority was repeated in the *Quality Improvement & Information Protection Act*, SNS 2015, c. 8.
3. For the purpose of determining or verifying an individual's eligibility for insured services (s. 38(1)(m)).

Safety and treatment-related disclosures:

4. To any person if the custodian believes the disclosure will avert or minimize an imminent and significant danger to health or safety of any person or class of persons (s. 38(1)(d)).
5. For the purpose of risk management or patient safety within the custodian's organization (s. 38(1)(t)).
6. To a non-custodian for the purpose of facilitating assessment, care or treatment services for the individual and with authorization of the Minister (s. 39)²¹ (see further discussion below on disclosures for the purpose of facilitating assessments).

²¹ Exchange of phi under this section may involve police and mental health service providers for example. Exchanges may include information necessary to adequately assess the situation, engage identified individuals within the formal mental health system, assist them in avoiding unnecessary utilization of emergency and inpatient services, determine obstacles to engagement with outpatient and/or community based services, and jointly plan an appropriate intervention.

Step 2: Is disclosure authorized?

Consent not required (cont'd)

Correctional facilities:

7. To an official of a correctional facility in which the individual is being lawfully detained if the purpose is to allow the provision of health care (s. 38(1)(e)) (Health Information Transfer Form).

To a representative of an individual or following death:

8. To a person legally entitled to make health care decisions on behalf of the individual, such as a legal guardian or administrator of the estate (for the purpose of the estate) (s. 38(1)b)).
9. To a proposed litigation guardian or legal representative of the individual for the purpose of having the person appointed as such (s. 38(1)(o)).
10. To a litigation guardian or legal representative who is authorized under the Civil Procedure Rules or by a court order (s. 38(1)(p)).
11. Custodians may disclose personal health information of an individual who is deceased in limited circumstances (identification, reasonable notification, organ donation (s. 40(1)).

In relation to regulation, administration and planning of health care:

12. To a regulated health profession body that requires the information for the purpose of carrying out its duties under an enactment (s. 38(1)(c)).
13. To the Nova Scotia Prescription Monitoring Board for monitoring prescriptions pursuant to the *Prescription Monitoring Act* (s. 38(1)(h)).
14. Where disclosure is reasonably necessary for the administration of payments in connection with the provision of health care or for contractual or legal requirements in that connection (s. 38(1)(r)).
15. To the Canadian Institute for Health Information to assist in the planning and management of the health system (s. 38(1)(i)).
16. To a prescribed entity (none have been prescribed) for the planning and management of the health system (s. 38(1)(j)).
17. To the Minister for the purpose of planning and management of the health system (s. 38(1)(g)).
18. From the Province to another provincial or territorial government or the Government of Canada to assist in the planning or management of the health system (s. 38(1)(k)).
19. To the Minister for the purpose of creating or maintaining an electronic health record (s. 38(1)(u)).

Step 2: Is disclosure authorized?

Consent not required (cont'd)

Legal proceedings, law and investigations:

20. For the purpose of complying with a summons, order or procedural rule that relates to the production of information in a proceeding (s. 38(1)(q)).
21. For the purpose of a proceeding or a contemplated proceeding in which the custodian or an agent is expected to be a party or witness (s. 38(1)(s)).
22. The disclosure is required or permitted by law or a treaty, agreement or arrangement made pursuant to this Act or another Act of the Province or the Parliament (s. 38(1)(l)). Examples include the *Children and Family Services Act*, *Gunshot Wounds Mandatory Reporting Act*, *Adult Protection Act*, and *Health Protection Act*.
23. To a person carrying out an inspection, investigation or similar procedure that is (s. 38(1)(n)):
 - (i) Authorized
 - by a warrant; or
 - by or under this Act or another Act of the Province or Parliament (for example the *Fatality Investigations Act*).
 - (ii) For the purpose of
 - complying with the warrant; or
 - facilitating the inspection, investigation or similar procedure.
 - (iii) Subject to the requirements and restrictions, if any, that are prescribed (none have been prescribed).
24. An agent or former agent who receives personal health information for the purpose of a proceeding or contemplated proceeding may disclose the information to a professional advisor if the advisor is under a professional duty of confidentiality. (s. 38(7)).

Step 3: Should you disclose the information?

If you have identified one or more authorities that permit disclosure of the personal health information (step 2), you must next ensure that you follow best privacy practices and further, that if you have discretion as to whether or not to disclose the phi, you properly exercise your discretion. The table below will assist you in identifying the relevant questions that must be addressed.

1. If the disclosure is authorized, identify the minimum amount of phi necessary to meet the authorized needs of the requester.

2. Is the disclosure authority such that the disclosure is mandatory (reasons 20, 21, 22 above)? For example:
 - Is there another statute that requires the disclosure?
 - Is there a court order?
 - Is there a warrant or subpoena?

If so, you can skip the next step on exercise of discretion because you must comply with any mandatory requirement. Read the statutory provision, court order, warrant or subpoena carefully and ensure that only information clearly captured by the mandatory authority is disclosed.

3. Except as noted above, disclosures without express consent under *PHIA* are discretionary. The law says that health custodians “may” disclose personal health information, not that they must disclose it. Review the proposed disclosure and determine whether or not you should exercise discretion in favour of disclosure. You may want to consider such things as:
 - Your organization’s policy regarding disclosures without consent. The policy may limit the circumstances under which disclosure may occur and may also limit who is authorized to disclose the phi.
 - Professional code of ethics requirements.
 - Age of the records.
 - Original purpose for collection versus purpose for disclosure.
 - Expectations of the patient.
 - Sensitivity of the information.
 - Past practice of your organization.

Step 4: Complete documentation requirements

1. Disclosures without consent must be documented (s. 42(1)).
2. The documentation must include:
 - A description or copy of the phi disclosed;
 - The name of the person or organization to whom the phi was disclosed;
 - The date of disclosure; and
 - The authority for the disclosure (s. 42(2)).

NON-CUSTODIANS

Note on further use or disclosure of personal health information by non-custodians

PHIA has rules for the further use and disclosure of phi by non-custodians. The key points are:

- A non-custodian does not become a custodian merely by virtue of its collection of phi (s. 45(1)).
- A non-custodian shall not use or disclose phi for any purpose other than the purpose for which it was disclosed or for the purpose of carrying out a legal duty (s. 45(2)).
- A non-custodian shall not use or disclose more of the information than is reasonably necessary to meet the purpose of the use or disclosure unless required by law (s. 45(3)).

AGENTS

Health custodians may provide personal health information to their agents in limited circumstances under *PHIA*. “Agent” means a person who, with the authorization of a custodian, acts for or on behalf of the custodian in respect of phi for the purposes of the custodian and not the agent’s purposes – whether or not paid. Agents include employees, volunteers, the custodian’s lawyer and insurer (s. 3(a)).

A regulated health professional is not a custodian in respect of phi that the person collects, uses or discloses while performing the person’s powers or duties as an agent of a custodian (s. 6(2)).

Seven essential rules about sharing phi with agents are:

1. Providing phi between a custodian and an agent is a use and not a disclosure (s. 29(2)).
2. Agents are permitted to collect, use or disclose phi only in the same circumstances that the custodian is permitted or required to collect, use or disclose phi (s. 28).
 - a. Custodians shall not collect, use or disclose phi if other information will serve the purpose (s. 24).
 - b. Collection, use or disclosure of phi must be limited to the minimum amount of phi necessary to achieve the purpose (s. 25(1)).
3. Custodians shall limit the use of phi to those of its agents who need to know the information to carry out the purpose for which the information was collected (s. 25(2)(a)).
4. Custodians may use phi for educating agents to provide health care (33(c)).
5. If a custodian is authorized to use phi for a purpose, the custodian may provide the information to an agent to use for that purpose (29(1)).
6. Where the custodian is permitted to use without consent, the custodian can provide the information to an agent for that same purpose (s. 35(2)).
7. The agent shall notify the custodian if phi is lost or accessed by unauthorized persons (28(3)).

A large, solid blue oval shape centered on a white background.

Tab 14



Office of the Information and Privacy Commissioner for Nova Scotia

PHIA Fee Fact Sheet

General rule:

Under the *Personal Health Information Act (PHIA)*, a custodian may charge an individual fees for accessing her personal health information including:²²

1. A basic fee of \$30.²³
2. Additional fees for activities listed in the regulations. If an activity is listed in the regulations fees may not exceed the prescribed amount.
3. If an activity is not listed in the regulation, the custodian may charge a fee for reasonable cost recovery.²⁴

The regulation also lists circumstances in which no fee may be charged (discussed below).

Basic fees:

The \$30 fee covers all of the following:²⁵

- Receiving and clarifying the request;
- Locating and retrieving the record (whether electronic or paper);
- Providing the individual requesting access with a fee estimate;²⁶
- The first 15 minutes of reviewing the record to see if information needs to be withheld;²⁷
- Severing any information the custodian decides to withhold from the record;
- The first 30 minutes of preparing the record for copying, printing, or electronic transmission;
- Writing the response letter to the individual;
- The first 30 minutes of supervising an individual's examination of the original records;
- Mailing the record by regular mail.

²² PHIA s. 82(1).

²³ PHIA regulation 14.

²⁴ PHIA s. 82(2).

²⁵ PHIA regulation 14.

²⁶ PHIA s. 82(1) requires a fee estimate be provided before fees are charged.

²⁷ PHIA s. 72(1) sets out a number of circumstances in which a custodian is authorized to refuse an individual access to his/her own personal health information.

Additional fees:

In addition to the general fee, custodians may also charge specific amounts for each of the following activities:²⁸

Activity	Maximum fee
Making photocopies of a record	\$0.20 per page
Preparing a record for photocopying, printing or electronic transmission	\$12.00 for every 30 minutes after the 30 minutes covered by the general fee
Faxing a record	\$0.20 per page
Copying an electronic record to a CD	\$10.00 per request
Making copies from a microfilm or microfiche	\$0.50 per sheet
Making a copy of an audio cassette recording	\$5.00 per cassette
Making and providing a copy of a ¼", ½" or 8 mm video cassette recording 1 hour long or less	\$20.00
Making and providing a copy of a ¼", ½" or 8 mm video cassette recording longer than 1 hour	\$25.00
Making and providing a copy of a ¾" video cassette recording that is 1 hour long or less	\$18.00
Making and providing a copy of a ¾" video cassette recording that is longer than 1 hour	\$23.00
Producing a record stored on medical film, including x-ray, CT, and MRI films	\$5.00 per film
Printing a photograph from a negative or electronic photograph – 4" x 6"	\$10.00
Printing a photograph from a negative or electronic photograph – 5" x 7"	\$13.00
Printing a photograph from a negative or electronic photograph – 8" x 10"	\$19.00
Printing a photograph from a negative or electronic photograph – 11" x 14"	\$26.00
Printing a photograph from a negative or electronic photograph – 18" x 20"	\$32.00
Reviewing the record to see if information needs to be withheld	\$25.00 for every 15 minutes after the 15 minutes covered by the general fee
Supervising an individual's examination of the original records	\$6.00 for every 30 minutes after the 30 minutes covered by the general fee

²⁸ PHIA regulation 15.

The *PHIA* regulation also permits custodians to charge certain direct costs and costs related to producing a visit history:

Direct costs:

A custodian may pass along direct costs incurred by the custodian for the following:²⁹

- Charges to retrieve a record from and return the record to off-site storage, if an individual requests expedited access to a record for which additional retrieval costs are charged to the custodian;
- Courier costs, if courier delivery is requested by the individual;
- The cost of mailing a record to an address outside Canada;
- Taxes payable on the services provided.

Visit history:

- If a custodian has the ability to produce a visit history, they may produce that visit history at the individual's request for a maximum cost of \$10. The \$30 general fee does not apply.³⁰ [Regulation 17(3)].

Fees do not apply:

The fees do not apply to any of the following:³¹

- **User activity report:** Where a custodian has an electronic information system, the custodian shall make a record of user activity available at the individual's request, and at no charge to the individual.³²
- **New patients:** A request from a regulated health professional who is entitled to personal health information in accordance with a consent³³ given by the individual whose personal health information is the subject of the request;
- **Legal aid representation:** A request made by a solicitor representing a legal aid client;
- **Review Board appearance:** A request from an individual for the purposes of appearing before the Review Board under Section 68 of the *Involuntary Psychiatric Treatment Act*;
- **Police officer:** A search warrant presented by a police officer under section 487 of the Criminal Code (Canada) or a production order presented by a police officer under section 278.7 of the Criminal Code (Canada);
- **Police and probation:** A request by a police officer or probation officer who is entitled to personal health information because the individual whose personal health information is the subject of the request has consented³⁴ to disclosure;
- **Investigation by regulatory colleges:** A request from a regulated health-profession body that is using the information for the purposes of regulating the health profession;³⁵
- **Workers' Compensation:** A request from the Workers' Compensation Board of Nova Scotia.

²⁹ *PHIA* regulation 16.

³⁰ *PHIA* regulation 17(3).

³¹ Items other than the user activity report are set out in *PHIA* regulation 12.

³² *PHIA* s. 63(1), 63(4).

³³ See *PHIA* s. 11(a).

³⁴ See *PHIA* s. 11(a).

³⁵ See *PHIA* s. 38(1)(c).

This document was prepared by the Office of the Information and Privacy Commissioner for Nova Scotia.
We can be reached at:

PO Box 181 Halifax NS B3J 2M4
5670 Spring Garden Road, Suite 509, Halifax
Telephone 902-424-4684
Toll-free 1-866-243-1564
TDD/TTY 1-800-855-0511
<https://oipc.novascotia.ca>