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 Commissioner[1] 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 *Personal Health Information Act*.
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.

[1] 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 Scotia[1] 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* ("*PHI*A").

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: http://foipop.ns.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
1660 Hollis Street, Suite 1002
Halifax, NS B3J 2M4
Phone: 902-424-4684 Toll Free: 1-866-243-1564

[1] The Information and Privacy Commissioner for Nova Scotia is also known as the Review Officer and is appointed as the 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 3). 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 4). Record your evaluation of each element by describing the current state of affairs in your organization. Be as honest and critical as you can. The goal here is to accurately state your organization's current status.

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

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

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

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

Sample - Gap Analysis Summary – 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[2]
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

[2] 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 *PHIA*.		
(ii) Ensure that all agents are informed of their duties under the *PHIA*.		
(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 *PHIA*.		
(vi) Facilitate the communications to and training of the custodian's staff about policies and procedures under *PHIA*.		
(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.		
(ii) How to contact the contact person/Privacy Officer;		
(iii)How to obtain access to or request correction of a record.		
(iv)How to make a complaint to the custodian and the Information and Privacy Commissioner for Nova Scotia (s. 68 *PHIA*).		
7. A complaints policy has been completed and implemented that includes: (i) A requirement that an individual submit a complaint in writing.		
(ii) The length of time the custodian will take to process, investigate and make a decision on the complaint (s. 62(2) *PHIA* and Regulation s. 8).		
8. Records retention schedule is in place that includes: (i) All legitimate purposes for retaining the information.		
(ii) The retention period and destruction schedules for each purpose (s. 50 *PHIA*).		
9. Notice of purposes is readily available that describes the purpose for the collection, use or disclosure of personal health information (s. 15 *PHIA*).		

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. (*PHIA* 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 *PHIA*) 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 *PHIA*) 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.		
16. Research agreements are always used for disclosures to researchers. The agreements include the eight requirements set out in s. 60 of *PHIA*.		
17. There is a process in place to notify the Information and Privacy Commissioner for Nova Scotia of all research disclosures made without consent (s. 57(d) *PHIA*).		

Gap Analysis Summary – Phase 1 PHIA		
Building Blocks – Program Controls		
List of Expectations	**Evidence of Compliance**	**Gap Rating**
h. Research Agreements	**Overall Rating**	
18. All disclosures for research are via research agreements as set out in s. 60 *PHIA*.		
19. There is a process in place to notify the Information and Privacy Commissioner for Nova Scotia of research disclosures without consent (s. 57(d) *PHIA*).		
i. Safeguards – Information Practices	**Overall Rating**	
20. Information practices have been implemented that: (i) Are reasonable in the circumstances.		
(ii) Ensure that personal health information is protected against theft or loss.		
(iii)Protect personal health information against unauthorized access to or use, disclosure, copying or modification of information (*PHIA* s. 62).		
21. A record of user activity can be generated from all electronic information systems that are used to maintain personal health information (*PHIA* s. 63(2)).		
22. A record of user activity with the data required under Regulation s. 11(2) can be produced within 30 days of a request.		
23. Additional safeguards have been implemented for all electronic information systems maintained by the custodian in compliance with *PHIA* 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 Scotia[1] 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: http://foipop.ns.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
1660 Hollis Street, Suite 1002
Halifax, NS B3J 2M4
Phone: 902-424-4684 Toll Free: 1-866-243-1564

[1] The Information and Privacy Commissioner for Nova Scotia is also known as the Review Officer and is appointed as the 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 3). When complete this will serve as a one page summary of your review results. Your goal is to develop a visual gap analysis by assigning red, yellow or green to the outcome of your assessment for each of the elements of your privacy management program ("PMP").

Step 1: Begin by assessing the two categories of building blocks: organizational commitment and program controls. Within each category are a series of requirements. For each requirement we have provided a list of essential elements. So, for example the Organizational Commitment requirement for buy-in from the top lists a requirement from senior management (see page 3). 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 3.

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

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

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

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

[2] 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[3]
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.

[3] 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**	
1. 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**	
2. The Privacy Officer is supported by dedicated staff.		
3. The role of the privacy office is defined.		
4. Staff have delegated responsibilities to monitor compliance.		
d. Reporting	**Overall Rating**	
5. 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.		
6. The reporting program has documented reporting structures.		
Building Blocks – Program Controls		
a. Personal Information Inventory	**Overall Rating**	
7. The organization is able to provide detailed information about inventory.		
b. Policies	**Overall Rating**	
8. 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**	
9. 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.		
10. 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**	
11. Privacy training is mandatory for all new employees.		
12. Training processes are documented and participation and success is measured.		
13. Individuals who handle personal health information directly need additional training specifically tailored to their roles.		
e. Breach and Incident Management Response Protocols	**Overall Rating**	
14. There is a procedure for management of personal health information breaches.		
15. Responsibilities for internal and external reporting of the breach are defined.		
f. Service Provider Management	**Overall Rating**	
16. Contractual or other means are in place to protect personal health information.		
17. The request for proposal process includes a survey of proponent's privacy management framework structure.		
18. Transborder data flows and requirements of the foreign regime are addressed in the service provider arrangements.		
19. Sensitivity of personal health information is addressed in the service provider arrangements.		
20. 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**	
21. There is a procedure for informing individuals of their privacy rights.		
22. There is a procedure for informing individuals of the program controls.		
23. 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 Scotia[1] 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: http://foipop.ns.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
1660 Hollis Street, Suite 1002
Halifax, NS B3J 2M4
Phone: 902-424-4684 Toll Free: 1-866-243-1564

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

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

Step 1: Begin by assessing the two categories of building blocks: organizational commitment and program controls. Within each category are a series of requirements. For each requirement we have provided a list of essential elements. 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 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 4.

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[2]
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

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

[2] 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[3]
b. Privacy Officer	Completed in phase 1	n/r
c. Privacy Office	**Overall Rating**	
1. Staff foster a culture of privacy within the organization.		
2. Staff work to ensure that privacy protection is built into every major function involving the use of personal health information.		
d. Reporting	**Overall Rating**	
4. An internal audit and assurance program monitors compliance with privacy policies.		
5. 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**	
6. Procedures have been developed for conducting such assessments and a review and approval process has been developed that involves the privacy office when designing new initiatives, services or programs.		
d. Training and Education Requirements	**Overall Rating**	
7. 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

[3] 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.[1] 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 http://foipop.ns.ca/.

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

PMP Requirement	Done	PMP Requirement	Done
Phase 1			
Organizational Commitment		**Building Blocks – Program Controls continued**	
a. Buy-in from the Top • Senior management endorses privacy controls. • Senior management provides resources needed.		**f. Service Provider Management**	
b. Privacy Officer • Privacy Officer appointed with seven essential authorizations.		**g. External Communication** • 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** • All disclosures for research are via research agreement set out in s. 60 of *PHIA*. • Process in place to notify Information and Privacy Commissioner for Nova Scotia of research disclosures without consent (s. 57(d) *PHIA*).	
d. Reporting • Senior management and health custodian receive regular reports.			
Building Blocks – Program Controls			
a. Personal Information Inventory completed.			
b. Policies • Privacy policy including information practices and contact information. • Complaints policy. • Record retention and destruction policy.		**i. Safeguards** • 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 PHIA requirements can be produced within 30 days from any electronic information system.	
c. Privacy Risk Assessments	n/r		
d. Privacy Training • All employees receive privacy training.			
e. Breach Management • 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 • Senior management monitors program.		**d. Privacy Training** • Participation and success is measured and documented. Privacy training is mandatory for all new employees. • Additional training is provided to those who handle personal information.	
b. Privacy Officer	n/r	**e. Breach Management** • There is a procedure in place for the management of breaches. • Internal and external reporting roles are defined.	
c. Privacy Office • 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.		**f. Service Provider Management** • 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.	
d. Reporting • Privacy reporting mechanisms are developed and used. • The reporting program has documented reporting structures.			
Building Blocks – Program Control			
a. Personal Information Inventory • The organization is able to provide detailed information about inventory.			
b. Policies • Responsible use policy in place.			
c. Privacy Risk Assessments • Privacy risk assessments are required for all new projects. • Process in place for identifying and mitigating privacy and security risks.		**g. External Communication** • There is a procedure for informing individuals of program controls. • There is a procedure for informing individuals of their privacy rights. • Further detailed notification provided.	
		h. Research Agreements	n/r
		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** • 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 • Staff foster a culture of privacy within the organization. • Staff work to ensure privacy is built into every major function.			
d. Reporting • Internal audit and assurance program monitors compliance with privacy policies. • Escalation procedure is in place for privacy breaches and complaints.		**b. Update Personal Information Inventory** • The personal information inventory is kept current with new collections and uses identified and evaluated.	
Building Blocks – Program Control			
a. Personal Information Inventory	n/r	**c. Revise Policies** • Policies are reviewed and revised as needed.	
b. Policies	n/r		
c. Privacy Risk Assessments • Review and approval process in place for all new initiatives.		**d. Treat Risk Assessment Tools as Evergreen** • Privacy impact assessments and security threat and risk assessments are treated as evergreen.	
d. Privacy Training • Training is recurrent and content is updated.		**e. Modify Training and Education** • 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** • Protocols are reviewed and revised to implement best practices or recommendations.	
i. Safeguards	n/r		
Ongoing Assessment and Revision – Oversight and Review Plan			
a. Develop Oversight and Review Plan • 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.		**g. Fine-tune Service Provider Management** • Contracts with services providers are reviewed and improved with experience.	
		h. Improve External Communication • External communications are reviewed, updated and clarified as needed.