

OIPC Guidance

Privacy Management Program

Step-By-Step Guidance for Public Bodies and Custodians on How to Implement an Effective and Accountable Privacy Management Program

INTRODUCTION

Accountability in relation to privacy means accepting and demonstrating responsibility for the protection of personal information and personal health information. This includes having policies, procedures, and practices in place that comply with the [Access to Information and Protection of Privacy Act, 2015](#) (ATIPPA, 2015) and the [Personal Health Information Act](#) (PHIA). Also, some public bodies and custodians may be subject to other laws with privacy requirements involving personal information and personal health information.

A privacy management program ensures that privacy is built into all initiatives, programs, or services, and assists organizations in meeting their legislative privacy obligations. The Office of the Information and Privacy Commissioner (OIPC) will apply these guidelines in our privacy investigations when looking for indications of accountable privacy management.

Residents entrust public bodies and custodians (organizations) with their personal information, including highly sensitive information, in order to receive services and benefits, and avail of programs. Responsible management of that information is critical for building and maintaining the trust and confidence of citizens necessary to deliver those services, benefits, and programs. Transparency about an organization's measures to protect personal and personal health information is therefore important.

In order to remain practical and effective, privacy management programs need to adapt to and keep current with changes in services, administrative structures, and applicable legislation. Organizations need to review and revise their privacy management programs on an ongoing basis, and this should become part of an organization's routine operational tasks.

Organizations vary in size, mandate, and functions. Also, the volume, type, and sensitivity of personal and personal health information they collect and what they do with it varies widely.

This document provides a scalable framework that can be used by all organizations to implement a privacy management program that fits the unique needs of the organization. This framework includes the following components:

- A. Getting Started; Steps for Setting up a Privacy Management Program
- B. Organizational Commitment;
- C. Program Controls; and
- D. Ongoing Assessment and Revision.

A. GETTING STARTED: STEPS FOR SETTING UP A PRIVACY MANAGEMENT PROGRAM

Prior to designing a privacy management program, an organization should first assess its existing approaches to privacy compliance. This will enable the organization to identify gaps and develop an action plan to implement any elements of a privacy management program that are missing. Appendix A, **Privacy Management Program at a Glance**, outlines the components of a privacy management program and is intended to assist in the privacy program assessment process.

The following are steps to consider in conducting an assessment and implementing a program.

1. Appoint a lead person with sufficient privacy knowledge and authority to assess compliance with privacy requirements in ATIPPA, 2015 or PHIA and review and document existing approaches to managing privacy.
2. Ensure there is oversight of the privacy program assessment process by senior management, through the lead person.
3. Provide progress updates to senior management and include any identified compliance issues.
4. Depending on the size of the organization and complexity of the information systems, the lead person may need to establish a working group or committee to carry out the assessment.
5. To the extent necessary, involve information management, information technology (IT), information security, risk management, internal audit, and human resources personnel.
6. If necessary, obtain outside privacy expertise. In addition to privacy consultants, OIPC (ATIPPA, 2015 and PHIA), the [ATIPP Office](#) (ATIPPA, 2015) and the [Department of Health and Community Services](#) (PHIA) have developed resources to assist public bodies and custodians in interpreting the legislation and identifying best practices and common privacy considerations.
7. Obtain and document information to assess compliance, through such activities as staff interviews, file reviews, IT system reviews, and policy reviews.
8. Provide a final report of all findings to senior management that includes an assessment of compliance with ATIPPA, 2015 or PHIA's requirements and identification of missing or inadequate elements of a privacy management program.
9. Take any other steps that might assist the organization in documenting its current state of compliance, identifying the gaps, and determining the way forward.
10. Develop an action plan to address any identified gaps in the privacy management program.

B. ORGANIZATIONAL COMMITMENT

Organizational commitment to privacy is the foundation that supports a privacy management program. Commitment can be demonstrated by prioritizing compliance with ATIPPA, 2015 or PHIA and fostering a privacy-respectful culture. It also involves ensuring accountability for the protection and responsible management of personal information and personal health information.

Organizational commitment involves:

1. Demonstrating senior management commitment and support;
2. Designating and empowering a privacy officer; and
3. Establishing compliance reporting mechanisms.

1. Demonstrate Senior Management Commitment and Support

Senior management commitment and support is key to a successful privacy management program. Senior management should endorse the program, support the role of the privacy officer, and provide necessary resources to effectively operate a privacy management program. It is important to have processes in place to ensure that senior management is kept informed about the organization's privacy compliance.

2. Designate and Empower a Privacy Officer

The head of a public body is accountable for compliance with ATIPPA, 2015 and they may designate a person to be responsible for the day-to-day management of this task. The custodian is accountable for compliance with PHIA and they may designate a contact person to facilitate the custodian's compliance with the Act and Regulations. It is important to recognize and understand, however, that appointing an individual to be responsible for the program does not transfer the organization's accountability to that individual. Ultimately, the organization remains accountable.

Organizations should expect to dedicate resources to training a privacy officer. Privacy should be seen in terms of improving processes, client relationship management, and reputation. Consequently, the privacy management program's importance must be recognized at all levels.

The person designated to ensure compliance with ATIPPA, 2015 and PHIA would also be responsible for the organization's privacy compliance and practices, and this would include responsibility for the management and direction of the privacy management program. The privacy officer should maintain records of their efforts, such as a record of decisions and action items stemming from meetings and communicating any privacy risks to senior management.

The role of the privacy officer (or access and privacy officer/coordinator) would generally include:

- Establishing and implementing program controls, including creating privacy policies and procedures;
- Designing and implementing employee training;
- Ongoing assessment and revision of program controls;
- Representing the organization in the event of an investigation by OIPC; and
- Demonstrating leadership within the organization in creating and maintaining the desired culture of privacy.

The role of the privacy officer should be clearly communicated throughout the organization and supported by senior management.

Due to continued advances in technology, changes to laws, and evolution of best practices, privacy training is an ongoing need for all staff who handle personal information, and a professional development requirement for the privacy officer.

Adequacy of resources is important. In some organizations, the person responsible for privacy may also be responsible for access to information or other duties. In larger organizations, additional staff may be required to support the work of the privacy officer, and this may involve establishing a privacy office, or access and privacy office.

Each organization should assess, and occasionally reassess, the resources needed to ensure legislative compliance and good practice. This can be done as part of the initial assessment and design of the privacy management program, with appropriate resources and staff being dedicated to carrying it out once the program is approved for implementation.

3. Establish Compliance Reporting Mechanisms

A privacy management program needs to incorporate different types of reporting mechanisms that are reflected within its program controls. This will ensure that the privacy officer and senior management are informed, on a regular basis, whether the privacy management program is functioning as expected and, if not, of the proposed fixes.

A key compliance reporting mechanism is an internal review or audit process. Some form of review or audit should be established to monitor and report on compliance with the organization's privacy policies and procedures. A review or audit may also be triggered by a breach. The results of reviews or audits should be reported to senior management.

Another type of reporting mechanism relates to situations when privacy issues need to be escalated, such as when there is a privacy breach or complaint from a citizen. Escalation means involving people with relevant responsibility within the organization and ensuring that the needed staff are included in the resolution of the issue. Establishing employee reporting procedures ensures that these situations are reported to the privacy officer, who may request assistance from senior management as required. In larger organizations this may include involving IT professionals, security experts, information managers, legal advisors, and communication advisors.

C. PROGRAM CONTROLS

Program controls help ensure that requirements of ATIPPA, 2015 or PHIA are implemented throughout the organization.

Program controls should include the following:

1. Inventory of personal information or personal health information;
2. Policies;
3. Training;
4. Breach management response procedures;
5. Privacy and security risk assessment tools;
6. Information sharing agreements; and
7. Transparent communication with individuals.

1. Inventory of Personal Information or Personal Health Information

Every aspect of an effective privacy management program begins with examining the types of personal information or personal health information the organization holds as well as how it handles this information. If an organization does not know, to a reasonable degree of specificity, the nature and amount of personal information or personal health information it is collecting, using, disclosing, or retaining, and the purposes and conditions for those activities, it is difficult to comply with ATIPPA, 2015 or PHIA. For example, if an organization subject to PHIA is not aware that it holds personal health information, it is unlikely that it is complying with its obligations under PHIA.

In preparing an inventory, it may be helpful to review record schedules or other documentation that describes the types of personal information or personal health information held by the organization (in its custody or under its control). This may already be documented in information management plans or in Privacy Impact Assessments (PIAs) on individual projects. Creation and maintenance of an inventory of personal information or personal health information enables an organization to assess its information handling practices in relation to ATIPPA, 2015 or PHIA. It also enables an organization to determine the risks associated with the information and to implement appropriate administrative, technical, and physical safeguards to protect the information. Moreover, it allows public bodies and custodians to say with relative certainty what information it holds, its location, and who has access to it.

Accountability is at the core of both the ATIPPA, 2015 and PHIA, and adequate documentation, including an inventory of personal information, is essential to achieving, and demonstrating, accountability for privacy protection.

An inventory should include a description of the following:

- The types of personal information or personal health information the organization holds (e.g. names, home addresses, and contact information of clients);
- The sensitivity of the information;
- Where the personal information or personal health information is held, both within the organization (e.g. paper files in staff offices and electronic information in a database) and where it is held by third parties (including service providers);
- The purposes for which the information is collected, used, and disclosed, and how each piece of information collected contributes to those purposes; and
- The details of the retention schedule and any requirements for secure destruction.

Building an inventory is an exercise that will involve a number of roles within the organization, including the privacy officer, program managers, information management, etc.

2. Policies

Policies are an essential part of a privacy management program. Policies help employees to understand their privacy obligations and how to fulfill them. Without written policies and procedures, an organization is more vulnerable to errors and oversights and is at greater risk of being non-compliant with ATIPPA, 2015 or PHIA. PHIA explicitly requires information practices, policies, and procedures to be established and implemented, while under ATIPPA, 2015 that expectation may be read into the requirement that public bodies maintain personal information in a secure manner using measures that are reasonable in the circumstances. Establishing and maintaining policies and procedures as part of a privacy management program would, in most contexts, be an essential element of compliance with that statutory requirement.

Organizations should also incorporate privacy compliance requirements into other types of policies as appropriate; for example, in contract management policies and human resource policies.

Here are some key issues that should be addressed through privacy policies (please note that this is not an exhaustive list):

- a) Requirements for notification of purpose for collection and consent;
 - b) Access to and correction of personal and/or personal health information;
 - c) Retention and secure destruction of personal and/or personal health information;
 - d) Administrative, technical, and physical safeguards; and
 - e) Process for handling privacy-related complaints.
- a) **Requirements for Notification of Collection Purposes and Consent**

It is important that employees understand the types and amount of personal information or personal health information they may collect for authorized purposes.

This not only ensures that the collection complies with ATIPPA, 2015 or PHIA, it also ensures that employees will be able to explain to individuals the reasons why the collection of information is necessary and obtain consent as appropriate.

A policy can help ensure that employees understand their obligation to notify individuals of collection purposes, as well as when and how to obtain consent from individuals, when necessary. For example, a policy could indicate the information that employees must provide to individuals when collecting their information directly from them, in order to meet the requirements in ATIPPA, 2015 or PHIA. It can also indicate the ways in which this notification may be done, such as verbally or on forms that individuals fill out. A policy could also address the circumstances in which employees should obtain consent from individuals to collect their information from another source, or when consent is needed to authorize a use or disclosure of their information under ATIPPA, 2015 or PHIA, which has additional requirements relating to consent.

There are times when consent is not required, and it may be beneficial to include organization-specific examples of these in the policy.

b) **Access to and Correction of Personal Information or Personal Health Information**

Individuals, including the organization's staff, have rights under ATIPPA, 2015 and PHIA to request access to and correction of their own information. Employees can help individuals to exercise these rights by knowing what processes to follow. The best approach is to have policies about how access will be provided and how correction requests should be handled. This promotes consistency, quality, and timeliness in decision making, in addition to compliance with ATIPPA, 2015 and PHIA.

c) **Retention and Secure Destruction of Personal Information or Personal Health Information**

Retention and destruction policies are necessary to ensure that personal information and personal health information is not prematurely destroyed or kept indefinitely, and that it is destroyed in a secure manner when it is no longer needed.

Accountable organizations should create retention schedules and destruction processes for personal information and personal health information. If personal information is used to make a decision that directly affects the individual, ATIPPA, 2015 requires the public body to retain the information for a least a year. Otherwise, the Acts do not specify how long the information should be kept and organizations should consider their operational, legal, financial, audit, or archival reasons in determining appropriate retention periods. Secure methods of destruction for personal information and personal health information in both hardcopy and electronic formats should also be addressed by way of a policy.

Organizations must protect the personal and personal health information they hold by making reasonable security arrangements as required by ATIPPA, 2015 or PHIA.

A policy should detail the special procedures necessary to remove personal information and personal health information from electronic devices before disposal. For example, an organization may have a specific policy to address the destruction of this information stored on copy and fax machines before disposing of them.

d) Administrative, Technical, and Physical Safeguards

Policies should address what is required of employees to protect personal information and personal health information during collection, use, disclosure, and storage of this information. Also, a policy can address how employees should protect this information when they take it from secure locations; for example, when they are taking this information to other work sites or working from home.

Determining what safeguards should be included in policies depends on a variety of factors, including the sensitivity of the information and whether the information is in hardcopy or electronic format. For example, a policy concerning information on an electronic system could inform staff about login requirements and passwords, as well as requirements to log out and not share passwords. In addition, if the electronic system is hosted and/or supported by a third-party provider, a policy should address requirements such as information sharing agreements. Security arrangements can include locked file cabinets and offices, as well as what information can be stored on portable storage devices and a requirement to use encrypted devices.

e) Process for Handling Privacy Complaints

Individuals have the right to challenge an organization's compliance with ATIPPA, 2015 or PHIA. Organizations should have a policy that outlines processes for staff to follow if individuals wish to complain about the organization's personal information or personal health information handling practices, including access and correction, as well as collection, use, disclosure, or security of personal information and personal health information.

In addition to having an internal privacy complaint process, organizations should also inform individuals of their right to make a complaint to OIPC and provide OIPC's contact information.

3. Training

Training is essential. In order for a privacy management program to be effective, employees must be actively engaged in privacy protection. An organization may have sound privacy controls in place, but if employees are not aware of them, the controls are of no real use. Employees will be able to better protect privacy when they are able to recognize and act on privacy issues as they arise.

All employees who may have indirect exposure to personal information or personal health information should receive general privacy training. Employees who handle such information directly should receive additional training specifically tailored to their roles. The content of the training program should be periodically revisited and updated to reflect changes within the organization.

With respect to personal health information, PHIA requires that employees, agents, contractors, and volunteers of the custodian be aware of the duties imposed by the Act, as well as the policies and procedures of the custodian. Additionally, a custodian must ensure that each employee, agent, contractor, and volunteer signs an Oath or Affirmation of confidentiality.

There are many ways in which training can be provided. Examples include mandatory training modules on an organization's intranet, small-group sessions, or one-on-one training. Awareness activities could include a constant privacy topic on meeting agendas, posters, e-mails, regular newsletters, etc. An organization should document its training efforts and participation by employees.

Staff need regular training and awareness activities to reinforce messaging and remind them of policies, procedures, and processes. It is not sufficient to offer generic training; training should be specific to the organization and to the specific role of the employee. For example, the [ATIPP Online Education Program](#) and the [PHIA Online Education Program](#) are good foundation courses, introducing the legislation. Staff should then also be trained on the organization's policies and procedures and receive training specific to their role.

For an organization's training to be effective, it should:

- Be mandatory for all new employees before they are exposed to or handle personal information or personal health information, and periodically thereafter;
- Be tailored for the role of the employee;
- Cover the policies and procedures established by the organization;
- Be delivered in the most appropriate and effective manner, based on organizational needs;
- Be tracked and documented; and
- Circulate essential information to relevant employees as soon as practical if an urgent need arises.

4. Breach Management Response Procedures

When a breach involving personal information or personal health information occurs, it is important that organizations are prepared to respond immediately. This can only be done effectively if the organization has a policy that sets out the process for managing breaches.

An organization should clearly assign responsibilities for managing a breach. These responsibilities include containing and mitigating the impact of the breach, as well as investigating the causes of the breach and ensuring the lessons learned are then incorporated into procedures, practices, or employee training. This may require collaboration on the part of employees from different parts of the organization. The policy should explain the responsibilities for internal and external reporting of breaches.

A policy with procedures for managing breaches is an essential component of a privacy management program. Any breach under ATIPPA, 2015 must be reported to OIPC; any material breach under PHIA must be reported to OIPC.

For more guidance on privacy breach management, refer to our resources for [ATIPPA, 2015](#) and [PHIA](#) on our website.

In addition to having an internal privacy complaint process, organizations notifying individuals of the privacy breach should also inform them of their right to make a complaint to OIPC and provide contact information for OIPC.

5. Privacy and Security Risk Assessment Tools

Conducting risk assessments is an important part of any privacy management program. Risks relating to personal and personal health information can evolve over time due to changes in practices, services, programs, technology, or administrative structures. Proper use of risk assessment tools, such as PIAs and security threat and risk assessments, can help identify and repair associated problems, or prevent them from arising in the first place.

Risk assessments should be conducted for all new projects, services, programs or systems involving personal and/or personal health information, or when significant changes are made to existing ones. Organizations should develop procedures for completing risk assessments and develop a review and approval process that involves the privacy officer in the early stages of planning. These procedures should also involve all relevant operational areas, including IT managers/staff where electronic information systems are involved.

For further information about conducting a PIA, see our guidance resources under the [Privacy Impact Assessment](#) heading on our website's guidance page.

6. Information Sharing Agreements (ISAs)

ISAs are a commonly used administrative safeguard when information is being shared between entities; they are especially important if sharing information with an entity that is not subject to ATIPPA, 2015 or PHIA.

There are many kinds of service provider relationships that involve personal information and personal health information, such as outsourcing of programs or contracting for specific services. A privacy management program should include procedures for ensuring compliance with ATIPPA, 2015 and PHIA with respect to service providers, including those that are "information managers."

PHIA has specific requirements when a custodian shares personal health information with an "information manager" that processes, stores, or destroys the information for a custodian, or provides information management or information technology services to the custodian. PHIA requires custodians to enter into a [written agreement](#) that ensures the information manager complies with the requirements of PHIA. For further information about ISAs, see our guidance resources under the [Custodian Related Topics](#) heading on our website's guidance page.

A privacy management program should ensure that the privacy officer is involved in procurement and contracting processes that involve personal information or personal health information.

7. Transparent Communication

Being accountable for privacy management includes transparency in communications with the public broadly as well as with individuals concerning their personal information or personal health information. A number of ATIPPA, 2015 and PHIA requirements involve communication between organizations and the individuals whose information they collect, use, or disclose, including the organization's own employees. These communications include giving notice about the collection of the information, seeking consent from individuals, responding to requests by individuals for access to their own information, and requests for correction of personal information and personal health information.

Organizations should have procedures for informing the public broadly, as well as clients, patients, and any individuals they interact with about their privacy rights and also about the organization's program controls, including policies. For example, an organization might decide to post its privacy policies online. PHIA has requirements for custodians to inform individuals of their right to access their own personal health information and how to do this, as well as the ability to authorize another person to exercise that right of access.

There should also be information available that informs individuals about the organization's internal procedures for dealing with privacy complaints. This can be done using posters, brochures, etc. Additionally, individuals who have privacy complaints should also be provided with information about their right to make a complaint under ATIPPA, 2015 and PHIA to OIPC.

All communications with individuals should be clear and easy to understand, not just a repeat of the law. Transparency about an organization's privacy policies, practices, and compliance measures is part of its accountability.

D. ONGOING ASSESSMENT AND REVISION

An organization should monitor, assess, and revise its privacy management program to be accountable for its privacy practices, and to make sure its handling of personal information or personal health information is in compliance with ATIPPA, 2015 or PHIA. This ensures that program controls can remain relevant and effective. Changes to services, technology, administrative structures, and applicable legislation may require changes to the program controls.

The development of the review and oversight plan should involve management to better ensure resource availability and general program support.

For ongoing assessment and revision of the privacy management program, the privacy officer would:

1. Develop an oversight and review plan; and
2. Assess and revise program controls.

1. Develop an Oversight and Review Plan

The privacy officer should develop a plan to review the privacy management program periodically. The plan would set out a schedule of when policies and other program controls will be reviewed.

Certain circumstances may trigger a review of and revision to some program controls. For example, a privacy breach may trigger a need to revise a specific policy or provide training to staff to prevent similar breaches. However, it is advisable that all program controls be reviewed on an annual basis.

The plan should also include a documented assessment of any changes in the organization's operating environment. This will involve a review of any relevant changes in the organization's powers, duties, functions, statutory or policy framework, organizational or management structures, or operating programs or activities.

2. Assess and Revise Program Controls

The effectiveness of program controls should be monitored, periodically reviewed, and revised where necessary.

Monitoring is an ongoing process and should address, at a minimum, the following questions.

- What are the latest privacy or security threats and risks?
- Are the program controls addressing new threats and reflecting lessons learned from any privacy breaches as well as the latest investigation findings or guidance of OIPC?
- Are new services being offered that involve increased or new collection, use, or disclosure of personal information or personal health information?
- Is training occurring, is it effective, and are policies and procedures being followed?

If problems are found, they should be documented and addressed by the appropriate staff, in collaboration with the privacy officer.

The privacy officer should review program controls regularly and at the very least:

- Ensure that the inventory of personal information or personal health information is updated and that new collections, uses, or disclosures of this information are identified and evaluated to ensure compliance with ATIPPA, 2015 or PHIA;
- Revise policies as needed following reviews, audits, in response to a breach or complaint, new guidance, best practices, or as the result of environmental scans;
- Review risk assessments to ensure privacy and security risks relating to changes or new initiatives within the organization are identified and addressed;
- Review and modify training and communicate changes made to program controls;
- Review and adapt breach response procedures to implement best practices and lessons learned from post-breach reviews;

- Review and, where necessary, fine tune requirements in information sharing agreements and information manager agreements;
- Update communications with individuals about privacy rights and the organization's privacy policies; and
- Ensure adequate resources are in place to realize program controls.

CONCLUSION

Accountable organizations are able to demonstrate that they have a comprehensive privacy management program in place. As there is no one-size-fits all privacy management program, the scalable framework outlined in this document should be tailored to the size and mandate of the organization and the amount and nature of the personal information or personal health information it has in its custody or control.

It is hoped that the guidance in this document assists organizations in complying with ATIPPA, 2015 and PHIA in implementing best practices and in demonstrating privacy accountability to residents of the province.

RESOURCES

- [Office of the Information and Privacy Commissioner of Newfoundland and Labrador.](#)
- [Access to information and Protection of Privacy \(ATIPP\) Office](#), Executive Council.
- Department of Health and Community Services' [Personal Health Information Act Resource Page](#).

ACKNOWLEDGEMENTS

These guidelines are based on [Guidelines for Implementing a Privacy Management Program for Privacy Accountability in Manitoba's Public Sector](#) published by the Manitoba Ombudsman, [Getting Accountability Right with a Privacy Management Program](#) published jointly by the Office of the Privacy Commissioner of Canada and the Offices of the Information and Privacy Commissioners (OIPC) for Alberta and British Columbia, as well as [Accountable Privacy Management in BC's Public Sector](#) by the OIPC for British Columbia and the OIPC for Nova Scotia's [Privacy Management Program](#) publications.

Office of the Information and Privacy Commissioner
PO Box 13004, Station A
St. John's, NL A1B 3V8
Phone: (709) 729-6309
Toll Free: 1-877-729-6309
commissioner@oipc.nl.ca
<https://www.oipc.nl.ca>

Appendix A: Privacy Management Program at a Glance

A. GETTING STARTED

Conduct an assessment of the organization's existing approaches to privacy compliance. Use this assessment to identify gaps and develop an action plan to implement any elements of a privacy management program that are missing.

B. ORGANIZATIONAL COMMITMENT

1. Demonstrate Senior Management Commitment and Support

Senior management support is key to a successful privacy program and essential for a privacy-respectful culture. This includes providing necessary resources to effectively operate a privacy management program; endorsing the program; monitoring the program and reviewing reports of compliance; and supporting the role of the privacy officer.

2. Designate and Empower a Privacy Officer

The organization ensures that a privacy officer is delegated responsibility for the organization's privacy compliance, including clearly identified roles and responsibilities.

3. Establish Compliance Reporting Mechanisms

Reporting mechanisms should be established and reflected in the organization's program controls.

C. PROGRAM CONTROLS

1. Inventory of Personal Information or Personal Health Information

The organization's information inventory describes the information in its custody or control; the sensitivity of the information; where the information is held; and the purposes for which the information is collected, used, and disclosed.

2. Policies

Key privacy issues that should be addressed through policies:

- Requirements for notification of collection purposes and consent;
- Access to and correction of personal information or personal health information;
- Retention and secure destruction of personal information or personal health information;
- Administrative, technical and physical safeguards; and
- Process for handling privacy complaints.

3. Training

Training should:

- Be mandatory for all new employees before they are exposed to or handle personal information or personal health information, and periodically thereafter;

- Be tailored for the roles of employees who handle personal information or personal health information; and
- Cover the policies and procedures established by the organization.

4. Breach Management Response Procedures

Breach management preparedness includes having a policy that outlines the procedures for the management of breaches; identifying a person responsible for managing a breach; and defining the responsibilities for internal and external reporting of a breach.

5. Privacy and Security Risk Assessment Tools

Responsible assessment and management of risk involves:

- Requiring an assessment of risks to personal information or personal health information in new projects, services, programs, systems, or when significant changes are made to existing ones;
- Having processes in place to assess privacy and security risks, including the use of privacy impact assessments (PIAs) and security threat and risk assessments; and
- Having procedures for a review and approval process that involves the privacy officer.

6. Information Sharing Agreements

To provide for the protection of personal information or personal health information when contracting with service providers and information managers, have standard clauses in contracts or agreements with service providers to ensure service provider compliance with privacy obligations.

7. Transparent Communication with Individuals

The organization's communications with individuals should inform individuals of their information rights, how to exercise them, and be in clear, easy to understand language that is not just a repeat of the law.

D. ONGOING ASSESSMENT AND REVISION

1. Develop an Oversight and Review Plan

The privacy officer should develop an oversight and review plan on an annual basis that sets out how the officer will monitor and assess the effectiveness of the program controls.

2. Assess and Revise Program Controls as Necessary

The privacy officer should review program controls regularly and ensure information is current and up-to-date. This includes revising policies as required based on developments, such as audits, breaches, and reports from oversight bodies; modifying documentation to reflect any changes to the overall operating environment or changes impacting specific initiatives; reviewing training to reflect changes, etc.