

Office of the
Privacy Commissioner
of Canada



Commissariat à la
protection de la vie privée
du Canada

PIPEDA SELF-ASSESSMENT TOOL

Personal Information Protection and Electronic Documents Act

TABLE OF CONTENTS

Why this tool is needed.....	3
How to use this tool	4

PART 1: COMPLIANCE ASSESSMENT GUIDE

Principle 1 – Accountability.....	6
Principle 2 - Identifying Purposes.....	10
Principle 3 – Consent.....	13
Principle 4 – Limiting Collection	17
Principle 5 – Limiting Use, Disclosure, and Retention	19
Principle 6 – Accuracy	21
Principle 7 – Safeguards	23
Principle 8 – Openness	27
Principle 9 – Individual Access	29
Principle 10 – Challenging Compliance	33

PART 2: DIAGNOSTIC CHECKLISTS

Introduction	35
Interpreting Self-Assessment Results	35
Action Planning.....	36
Checklist for Principle 1 – Accountability.....	39
Supplemental Assessment for Federal Works, Undertakings or Businesses	40
Checklist for Principle 2 – Identifying Purposes	40
Checklist for Principle 3 – Consent	41
Checklist for Principle 4 – Limiting Collection	41
Checklist for Principle 5 – Limiting Use, Disclosure, and Retention	42
Checklist for Principle 6 – Accuracy	42
Checklist for Principle 7 – Safeguards	43
Checklist for Principle 8 – Openness.....	43
Checklist for Principle 9 – Individual Access.....	44
Checklist for Principle 10 – Challenging Compliance	45
Appendix A	46
Appendix B	49
Appendix C	53

WHY THIS TOOL IS NEEDED

In a world of ubiquitous computing and information sharing it is increasingly difficult to ensure appropriate use and protection of personal information. Strong privacy governance and management within organizations are effective means of mitigating privacy risks and ensuring that fair information principles are applied in business decisions and day to day operations.

The **Office of the Privacy Commissioner of Canada (OPC)**, has developed this self-assessment tool to help medium and large organizations develop and implement good privacy governance and management. Privacy self-assessment is a process whereby an organization initiates an evaluation for the purpose of benchmarking and improving its own privacy systems and practices over time. This includes assessing the organization against a set of expectations to determine the degree to which they are met. In measuring compliance, gaps and/or risks may be identified for the purpose of guiding and following up remedial action.

**The OPC views self-assessment by organizations as an efficient and effective means of promoting privacy principles.
See Annex B for more details.**

This tool is offered to guide you in evaluating and improving your personal information management systems and practices. It is designed for medium to large private sector organizations which are subject to Canada's *Personal Information Protection and Electronic Documents Act (PIPEDA)*, but may be adapted and used by others wishing to apply PIPEDA principles.

Use of this tool is voluntary. How you achieve compliance with PIPEDA is your responsibility. Nothing in this consultation document should be considered to interfere with or fetter the discretion of the OPC to carry out its responsibilities, especially with respect to any complaint filed by an individual under PIPEDA or the *Privacy Act* or the undertaking of an audit by the OPC under either *Act*.

What this tool is

- A set of standards that medium to large businesses can use to monitor compliance with the 10 Fair Information Principles from Schedule 1 of PIPEDA¹ ;
- A framework of principles and criteria to assess the degree to which your business is compliant with your obligations; and
- A means of interpreting results and creating an action plan for improving your personal information management practices or checking the adequacy of practices already in place.

What this tool is not

- A “one-size fits all” application;
- A replacement for “tried and true” assessment methods you may have already developed and implemented;
- Definitive and all-inclusive for all organizations;
- A replacement or substitution for PIPEDA; or
- Relevant for legislation other than PIPEDA.

¹ These ten principles are: Accountability, Identifying Purpose, Consent, Limiting Collection, Limiting Use Disclosure and Retention, Accuracy, Safeguards, Openness, Individual Access, and Challenging Compliance.

HOW TO USE THIS TOOL

This tool is made up of two parts, both of which are described in more detail in later sections:

- Part 1: A *compliance guide*, which will help inform you of your obligations under PIPEDA, and;
- Part 2: A *diagnostic tool*, which is a series of checklists you can use to assess how compliant your business (overall or parts thereof) is with the 10 Fair Information Principles of PIPEDA.

Use both sections together to ensure you understand whether you meet your privacy objectives, to what degree each objective is met, and the evidence that can be used to demonstrate compliance.

Comments on this publication should be sent to the attention of the Director General of Audit & Review,
Office of the Privacy Commissioner of Canada, 112 Kent Street, Ottawa, Ontario, K1A 1H3.

This tool can help you at various stages in your organization's developmental needs. It can be adapted for application to your organization as a whole or to particular business units as you may choose. If you do not have an established privacy program, you can use it to identify the various privacy controls (policies, systems, procedures, access controls, etc.) that need to be designed and implemented within your organization. After these controls have been implemented and operating for a certain period of time, use the checklists to conduct a thorough self-assessment to identify gaps and areas for improving personal information management practices.

Next steps:

If you are:

- A medium to large organization **with an established privacy framework** which addresses all 10 Fair Information Principles of PIPEDA, we suggest you proceed directly to the “checklists” in Part 2 to assess your compliance.
- A medium to large organization **without an established privacy framework** which addresses the principles of PIPEDA, we suggest you proceed to the compliance guide in Part 1 to begin understanding your obligations under the legislation.
- A medium to large organization **with a privacy framework and some policies, but you aren't sure if they address PIPEDA requirements**, we suggest you proceed to the “checklists” in Part 2 to assess your compliance. Completing the checklists will allow you to identify gaps in your privacy framework.

For Further Reference

Appendix A contains an overview of PIPEDA. This self-assessment tool should be used in conjunction with the *Act*. It does not replace, substitute, or override the *Act* in any way.

Appendix B outlines the concept, benefits, and how an organization may set about doing a self-assessment.

Appendix C lists other guidance available from the OPC. We suggest consulting the OPC Web site at <http://www.privcom.gc.ca> where you will find additional guidance on a variety of compliance matters. We also encourage organizations to review complaint case summaries published by the OPC to learn about how the OPC may interpret PIPEDA as well as to gain insight on systemic causes of privacy compliance problems.

PART 1: COMPLIANCE ASSESSMENT GUIDE

INTRODUCTION

Each section of this guide describes one of the 10 Fair Information Principles which form the basis of a privacy standard to evaluate compliance with PIPEDA. In order to ensure your personal information handling policies and practices are compliant, you should address the criteria associated with each principle. For each of the 10 principles, the guide includes two types of information:

- Description of your specific responsibilities for personal information management under the principle being addressed based on PIPEDA; and
- Activities and best practices that enable you to meet each compliance obligation. As these are examples only, you may need to adapt them or choose unique ways to implement requirements.

The Compliance Guide will help you in developing the elements of your privacy framework. Once you have developed your framework and it has been up and running for some time, complete the self-assessment checklists in Part 2 to ensure that it is operating as it should.

PRINCIPLE 1 – ACCOUNTABILITY

An organization is responsible for the personal information under its control and shall designate an individual or individuals who are accountable for the organization’s compliance with the following principles.

Your Organization’s Privacy Responsibilities

Under the “Accountability” principle, your organization must:

- Accept responsibility for personal information under its control;
- Designate at least one representative to be accountable for the organization’s compliance with the 10 principles set out in Schedule 1 of PIPEDA;
- Make the identity of the designated individual(s) known on request;
- Protect all personal information in the organization’s possession or custody, including information that has been transferred to a third party for processing;
- Use contractual or other means to ensure a comparable level of protection while personal information is with a third party for processing;
- Develop and implement policies and practices to uphold the 10 principles set out in Schedule 1 of PIPEDA including:
 - Implementing procedures for protecting personal information;
 - Establishing procedures for receiving and responding to complaints and inquiries;
 - Training staff and communicating information to staff about the organization’s policies and practices; and
 - Developing information to explain the organization’s policies and procedures.

Under the “Accountability” principle, your organization may:

- Delegate other individuals within the organization to act on behalf of the designated privacy representative.

How to Meet these Objectives

Designate a Privacy Representative

- Appoint at least one person in the organization to be accountable for your organization’s personal information handling policies and practices. If this individual is not a dedicated Privacy Officer, ensure that the job description for this person includes responsibility for controlling personal information, as required by law. This person should:
 - be a senior decision maker who is clearly supported in his/her role by senior management in promoting privacy as a corporate value;
 - be able to intervene on privacy issues across the organization when needed; and
 - be expected to ensure that sufficient and appropriate resources are allocated for implementing privacy policies, managing privacy risks, and ensuring periodic assessments are done to see if privacy policies are being met and the organization is complying with PIPEDA.

- Where appropriate, publish the name or title and business address of the privacy officer internally and externally (e.g., on Web sites and in company literature). Be prepared to identify your privacy officer should you receive a request for this information; and
- Develop guidance that will assist staff in responding to questions from customers about your Privacy Program, including information on how to contact the Privacy Officer if they request it.

Develop Privacy Policies and Procedures²

- Develop and implement personal information-handling policies and procedures corresponding to specific principles in Schedule 1 of PIPEDA. If your organization is a “federal work, undertaking, or business”, as defined in Section 2(1) of PIPEDA, these policies and procedures apply to the personal information of your employees as well as your customers;
- Define a privacy policy that will apply to the whole organization, augmented by sub-policies that apply to specific business areas, if required;
- Articulate procedures for:
 - Informing individuals of the purposes for collection (*Principle 2 - Identifying Purposes*);
 - Obtaining appropriate consent (*Principle 3 - Consent*);
 - Allowing individuals to withdraw consent (*Principle 3 - Consent*);
 - Limiting the collection of personal information (in both amount and type of information as well as without misleading or deceiving individuals) to that which is necessary for purposes identified and ensuring it is collected by fair and lawful means (*Principle 4 – Limiting Collection*).
 - Retaining and destroying personal information (*Principle 5 - Limiting Use, Disclosure, and Retention*);
 - Ensuring that information is correct, complete, and up-to-date (*Principle 6 - Accuracy*);
 - Ensuring adequate security measures (*Principle 7 - Safeguards*);
 - Making information on policies and practices available to the public (*Principle 8 - Openness*);
 - Receiving and processing access requests (*Principle 9 - Individual Access*);
 - Receiving and responding to inquiries and complaints (*Principle 10 - Challenging Compliance*).
- Define administrative policies for privacy governance and management setting out expectations regarding:
 - Organizational structures, roles and responsibilities to achieve privacy requirements;
 - Reporting to Senior Management on privacy policy and risk management procedures;
 - Allocation of sufficient and appropriate resources to implement and support privacy policies;
 - Requirements to undertake privacy impact assessments before new products, services or information systems are introduced or existing ones are significantly changed;
 - Information security and management standards to ensure that information is safeguarded against unauthorized disclosure, modification, interruption, removal or destruction;
 - Requirements for periodic review of the design, acquisition, development, implementation, configuration and management of the infrastructure, systems, applications, and Web sites to ensure consistency with privacy policies and procedures;
 - Requirements for identifying, assessing and reporting on the impact of, and correcting the cause of, privacy breaches including loss of personal information or inappropriate use of personal information;
 - Procedures to follow in responding to privacy complaints and undertaking corrective actions as required;
 - Ongoing privacy training for employees; and
 - Auditing for compliance with good privacy management practices.

² Your privacy framework may be comprised of a single, overarching policy or a suite of smaller policies, all of which support the 10 principles.

Ensure Accountability of Organization and Staff

Give your privacy officer senior management support and the authority to intervene on privacy issues relating to any of your organization's operations and reflecting the addition of privacy responsibilities by updating the formal job description;

Make sure your organization's privacy officer can:

- demonstrate knowledge of the organization's personal information handling policies and procedures;
- demonstrate knowledge of the organization's responsibilities under PIPEDA;
- explain the procedures for requesting personal information and filing complaints; and
- conduct or supervise complaint investigations.

Train all front-line and management staff and keep them informed, so that they:

- can either respond to inquiries about your organization's privacy policies and practices themselves or refer inquirers to the privacy officer or another authorized representative;
- can explain the organization's purposes for collecting personal information;
- understand your organization's policy and procedures on consent and can obtain consent as appropriate;
- explain to customers when and how they may withdraw consent and what consequences if any may come of such withdrawal;
- can recognize and process requests for access to personal information;
- can refer complaints about privacy matters to the organization's privacy officer; and
- are up to date on your organization's ongoing activities and new initiatives relating to the protection of personal information.

Ensure that you:

- keep your employees informed of new privacy issues raised by technological changes, internal reviews, public complaints, and decisions of the courts on a day-to-day basis; and
- develop and implement a system to monitor your organization's compliance with PIPEDA on an ongoing basis.

Disseminate Information to the Public

Customers are becoming more aware of privacy issues and the protection of personal information. You should communicate your policies and practices for collection and use of personal information and the steps you take to protect their personal information. To that end:

- Develop and disseminate literature (i.e., brochures, booklets, Web sites, or other written materials) to explain, in plain language, your organization's privacy policies, practices, and procedures to customers and the general public;
- Make sure that any such literature clearly specifies how individuals may:
 - obtain access to their personal information;
 - correct their personal information;
 - make inquiries about the organization's privacy policies or practices; and
 - complain about the organization's privacy policies or practices.

- For customers in particular, make it easy to find out whom in the organization to contact in order to:
 - make general inquiries regarding their personal information;
 - request access to their personal information; and
 - correct their personal information.

Responsibility for Third Party Transfers

Organizations transfer information to third parties for processing for a variety of reasons. It is important to note that the original organization retains control of the information when transferring personal information to a third party for processing. Best practices include:

- Using privacy protection clauses in contracts to ensure that third parties to which personal information is transferred for processing provide the same level of protection under PIPEDA as your organization does, unless the third party is a subsidiary or an affiliate bound by the same privacy code;
- Ensuring that the third party:
 - names a person to handle all privacy matters relating to the information transferred;
 - limits its use of the information to purposes authorized by your organization;
 - limits disclosure of the information to what is authorized by your organization or required by law;
 - refers to your organization any access requests or complaints relating to the information transferred;
 - uses appropriate security measures to protect the personal information;
 - returns or securely disposes of the transferred information upon completion of the contract; and
 - reports on the adequacy of its personal information security/control measures and allows your organization to audit its compliance as necessary.

PRINCIPLE 2 - IDENTIFYING PURPOSES

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

Your Organization's Privacy Responsibilities

Under the “Identifying Purposes” principle, your organization must:

- Identify why it is collecting personal information at or before the time of collection;
- Document its purposes for collecting personal information; and
- Notify your clients or customers before using personal information for any purpose not identified at the time of collection.

Under the “Identifying Purposes” principle, your organization should:

- Determine the amounts and types of information needed to fulfill the purpose you collected it for, in accordance with the “Limiting Collection” principle; and
- Ensure that anyone who collects personal information for the organization can explain why to your clients and customers.

Under the “Identifying Purposes” principle, your organization may:

- Choose how best to explain to your clients and customers why their personal information is being collected, either orally or in writing.

Notes

- The “Identifying Purposes” principle relates closely to the knowledge requirement set out in the “Consent” principle. Specifically, Principle 4.3.2 of Schedule 1 states:

The principle requires “knowledge and consent”. Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

- Subsection 5(3) of PIPEDA is also relevant:

5(3) An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.

How to Meet these Objectives

Identify Purposes

- Review your current practices, and determine the specific purposes for collecting personal information;
- New purposes should be reviewed by the Privacy Officer to determine if they are appropriate, and to consider and mitigate any potential privacy risks stemming from the new uses;
- Determine the amounts and types of information your organization minimally needs to collect in order to fulfill its purposes, keeping the “Limiting Collection” principle in mind;
- Confirm that the reasons you’re collecting personal information are what a reasonable person (e.g., a typical customer) would expect or consider appropriate in normal business circumstances, in keeping with Section 5(3) of PIPEDA (see note above); and
- Clearly distinguish between collection activities that are essential and those that are not to the actual provision of the products or services customers have requested, such as marketing additional products or services. Customers should be able to opt out of non-essential or secondary purposes.

Document Purposes

- Clearly record in writing all the reasons why you collect personal information. Keep this list up-to-date. When compiling your list:
 - Be specific about your intended uses and disclosures of personal information;
 - Do not use broad categories of purposes such as “serving the customer”;
 - Avoid vague or open-ended language such as “... and other uses as appropriate”; and
 - State why you collect personal information in clear, concrete and unambiguous terms, so that customers will be able to understand the specific ways in which your organization intends to use or disclose the information it collects from them.
- To comply with the “Openness” principle, incorporate these purpose statements in your organization’s privacy literature and other relevant documents (e.g., terms of agreement, application forms).

Specify Purposes

- Wherever practicable and reasonable, notify clients and customers, orally or in writing, why you are collecting personal information before you collect it;
- Where notification at or before collection is not practicable or reasonable, notify clients and customers, orally or in writing, before using or disclosing the information;
- As a general rule, notify after collection only if the purposes are new (i.e., not yet conceived at the time of collection);
- In general, before obtaining consent, make every reasonable effort to inform customers of the purposes for which your organization intends to use or disclose their personal information. Keep in mind that their meaningful consent will ultimately depend on their knowledge of what they are consenting to; and
- Inform customers of any intended uses or disclosures of their personal information that they would not reasonably expect when obtaining a product or service from your organization. This includes sharing personal information with third-party marketers.

When You Specify Purposes Orally

- Train employees who collect personal information so that they are able to explain purposes accurately, clearly, and consistently, and inform them of any new reasons for collection;
- Provide a standard script or use other means to ensure that all staff can explain such purposes to customers in a clear and consistent manner; and
- If your organization records telephone calls with customers (e.g., for quality control purposes), make a practice of informing the customer of this practice and its purposes at the beginning of every call. Refer to the OPC document *Guidelines for Recording Customer Telephone Calls* available at <http://www.privcom.gc.ca/>.

When You Specify Purposes in Writing

- If your organization notifies customers of purposes in writing:
 - provide the customer with written purpose statements before or preferably at the time of collecting the customer's personal information wherever possible;
 - provide written purpose statements to the customer at the place or venue of the collection (e.g., at your place of business, at the customer's home, or on your Web site, depending on whether the customer is supplying information in person, by mail or telephone, or electronically) wherever possible; and
 - make written purpose statements readily available to the individual for reference in considering the question of consent.
- When using forms to collect personal information, explain why you are collecting the information on the forms themselves; and
- In any written materials used to notify customers, make sure that purpose statements are prominently displayed and easy to find, read and understand. Use plain language when possible.

Identify New Purposes

- If some time after the original collection your organization intends to use or disclose a customer's personal information for a new purpose not previously identified:
 - seek guidance from your Privacy Officer about possible privacy impacts;
 - identify and document the new purpose and explain it to the customer; and
 - obtain the customer's consent to the new purpose, unless not required by law.

PRINCIPLE 3 – CONSENT

The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate.

Your Organization's Privacy Responsibilities

Under the “Consent” principle, your organization must:

- Obtain the individual's consent for any collection, use, or disclosure of personal information, except where inappropriate (e.g., legal, medical or security reasons), as specified in Section 7 of PIPEDA. Document all exceptions and identify and support those instances when information can be collected, used, or disclosed without consent. Where it is deemed inappropriate to obtain consent, a clear documented rationale must support the exception;
- Ensure that the consent obtained is informed consent;
- Make a reasonable effort to ensure that the individual is advised of the purposes for which personal information will be used or disclosed;
- State and explain purposes in such a manner that the individual can reasonably understand how the personal information will be used or disclosed;
- Never require an individual to consent, as a condition of supplying a product or service, to the collection, use, or disclosure of information beyond what is necessary to fulfill explicitly specified and legitimate purposes;
- Consider the reasonable expectations of the individual in obtaining consent;
- Never obtain consent through deception;
- Take into account the sensitivity of the personal information when determining how you will obtain consent;
- Allow the individual to withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice; and
- Inform the client or customer of any consequences of withdrawing consent.

Under the “Consent” principle, your organization should:

- Seek consent at the time of collection for subsequent uses or disclosures of personal information;
- Treat all medical records and income or financial records as sensitive information;
- Keep in mind that any information can be sensitive, depending on the context; and
- Seek express consent whenever possible and always when the personal information is likely to be considered sensitive.

Under the “Consent” principle, your organization may:

- Seek consent for subsequent uses or disclosures of personal information *after* collection but *before* use in certain circumstances (i.e. when you want to use personal information previously collected for a purpose not previously identified);
- Select an appropriate form of consent, depending on the circumstances and the type and sensitivity of personal information involved; and
- Rely on implied consent only when personal information is not sensitive.

How to Meet these Objectives

Fulfilling the Knowledge Requirement

- Understand that the validity of any consent your organization obtains will usually depend on the customer knowing your organization's purposes at the time you ask for their consent;
- Provide your customers with a sufficient basis of knowledge for valid consent, identify, document, and specify purposes in accordance with the "Identifying Purposes" principle (see preceding section);
- State purposes in such a manner as to enable the customer to form a reasonable understanding of the specific ways in which your organization intends to use or disclose personal information; and
- Take appropriate measures to ensure that your efforts to notify customers of purposes will be considered reasonable.

Fulfilling the Consent Requirement

- Establish clear policies and procedures relating to consent, and ensure that employees who collect personal information understand the process and can implement the procedures consistently;
- Seek the customer's consent for the collection, use, or disclosure of personal information, unless an exception applies as specified in Section 7 of PIPEDA. Review Section 7 of PIPEDA to determine the exceptions to the consent requirement;
- Obtain consent for subsequent uses and disclosures at the time of collection and ensure that any deviation from this rule would meet the customer's reasonable expectations;
- If seeking consent after collection to a use or disclosure not previously identified, make sure that the customer is duly notified of the purpose and asked for consent before the new use or disclosure is made;
- Before requiring any customer to consent to a collection, use, or disclosure of personal information as a condition for receiving a product or service, make sure that the:
 - purposes are legitimate (i.e., reasonable);
 - customer receives explicit notification of the specific purposes; and
 - intended collection, use, or disclosure does not exceed what is necessary to fulfill the purposes.
- Do not make consent for secondary purposes, such as marketing, a condition for supplying a customer with a product or service;
- Where a purpose is secondary or such that consent to it cannot reasonably be required of an individual as a condition for supplying a product or service, identify the purpose and the consent as optional, and notify the individual of his or her options;
- Consent regarding pre-PIPEDA information: For guidance on consent relating to use or disclosure of any personal information your organization collected before becoming subject to PIPEDA, refer to the OPC document *Best Practices for Dealing with Pre-PIPEDA Personal Information (Grandfathering)* available at <http://www.privcom.gc.ca/>; and
- For guidance on consent relating to the recording of customer telephone calls, refer to the OPC document *Guidelines for Recording Customer Telephone Calls* available at <http://www.privcom.gc.ca/>.

Choose the Appropriate Form of Consent

- Before choosing the form of consent to use in a given situation (i.e., express, implied, opt-in, opt-out), refer to the OPC fact sheet Determining the appropriate form of consent under the *Personal Information Protection and Electronic Documents Act* available at <http://www.privcom.gc.ca/>;
- Consider the sensitivity of the personal information, the reasonable expectations of the customer, and the circumstances;
- Use **express (opt-in) consent** wherever feasible and in all situations involving personal medical or financial records or any other personal information likely to be considered sensitive in a given context:
 - As a best practice, use the express (opt-in) form of consent for any intended disclosure of personal information to third parties or any other secondary purpose that customers would not reasonably expect to be involved as a matter of course in their purchase of a product or service from your organization; and
 - If your organization uses cookies or similar technologies on its Web site, notify users of this practice and its purpose, and seek their express (opt-in) consent to it.
- Rely upon **implied consent** only in situations where the intended uses or disclosures are obvious from the context and your organization can reasonably assume a certain understanding, knowledge, or acceptance on the customer's part.

Methods of Obtaining Consent

- When using an **application form** to obtain consent, make sure that the purposes for the collection are clearly stated and prominently placed on the form;
- When using check off boxes to seek consent for sharing personal information with other organizations:
 - identify the other organizations by name;
 - state the purpose clearly;
 - ensure that the check off arrangement itself is clear and unambiguous;
 - as a best practice, use only one box – either a “yes” or a “no”;
 - if the personal information is sensitive or if the other organizations remain unidentified, use strict “opt-in” consent in the form of a single “yes” box and if the customer does not check the box, do not assume consent;
 - use opt-out consent (i.e., a “no” box) only if the personal information is demonstrably not sensitive (this generally means information that is publicly available)
 - if using both a “yes” and a “no” box, clarify the form of consent intended by explaining what happens in the event that the customer does not check either box, indicating whether your organization assumes consent or not; and
 - if using both a “yes” and a “no” box and the personal information is sensitive, treat the check off mechanism as “opt-in” consent; if the customer does not check either box, do not assume consent.
- Ensure that employees responsible for obtaining **consent by phone** understand the process and can consistently follow your organization's procedures; and
- Limit the practice of **assuming implied consent** from a customer's use of a product or service to those situations a customer would reasonably expect to be involved in the provision of the product or service. As a general rule, do not assume a customer's implied consent for secondary purposes from their use of a product or service.

Provide for Withdrawal of Consent

- Since customers have the right to withdraw consent at any time (subject to legal or contractual restrictions and reasonable notice), provide a convenient way for them to do so easily, inexpensively, and with immediate effect. Toll-free telephone is the preferred option;
- Add information on the opportunity and mechanism for consent withdrawal to all published materials relevant to identifying purposes and seeking consent. When relying on opt-out consent to secondary purposes, ensure the consent withdrawal mechanism is brought to customers' attention at the time of assuming consent; and
- Before or at the time any customer requests withdrawal of consent, inform the customer of the implications of such withdrawal. Withdrawal of consent to secondary purposes should not entail serious implications relating to the provision of products or services.

PRINCIPLE 4 – LIMITING COLLECTION

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

Your Organization's Privacy Responsibilities

Under the “Limiting Collection” principle, your organization must:

- Limit its collection of personal information (the amount and the type) to what is necessary for identified purposes;
- Never collect personal information indiscriminately;
- Collect personal information only by fair and lawful means, without misleading or deceiving the individual about the purposes for collection, and without deception in obtaining consent; and
- Specify types of information collected as part of the organization's information handling policies and practices, in accordance with the “Openness” principle.

How to Meet these Objectives

Review Collection Practices

- Verify that your organization consistently collects personal information in a fair and lawful way, not indiscriminately, and without deception about purposes and consent;
- Determine why you collect personal information, and what the minimum amounts and types of information necessary to fulfill those purposes;
- Make a clear distinction between obligatory and optional information. Some key information is necessary to provide a service, while other information may be useful, but is not necessary, such as a driver's license when goods are returned. Designate “nice-to-have” information as optional for the consumer;
- Limit your organization's collection of personal information to the minimum amounts and types necessary for the identified purposes. Information should not be collected on the basis that it might prove useful in the future; and
- Where possible make use of anonymized or non-personal information such as a customer number instead of a name.

Document Collection Practices

- In order to communicate with customers in accordance with the “Openness” principle, document your collection policy and practices in your organization's privacy literature. Specify clearly the types of information you collect, as well as the purposes for collection;
- Assign specific purposes to specific information types. Also be sure to account for information your organization collects from any source other than from the customers themselves (e.g., credit report obtained by lender from credit reporting agency); and
- Establish procedures for collecting personal information. Make sure all staff understand and respect the limitations on collection of personal information.

Obligatory vs. Optional Information

- In notifying customers, orally or in writing, why you're collecting information, distinguish clearly between that which is obligatory and that which is optional. Optional information is merely useful, as opposed to necessary, and includes any information collected solely for secondary purposes;
- If your organization requests any type of information that cannot reasonably be considered strictly necessary for fulfilling a certain purpose (e.g., social insurance numbers for the purpose of identification), notify customers at collection time that the information is optional;
- If your organization collects social insurance numbers for any purpose, make sure that such collection and any subsequent uses or disclosures are in accordance with OPC guidelines as documented in *Best Practices for the Use of Social Insurance Numbers in the Private Sector* (available at <http://www.privcom.gc.ca/>). In general the OPC suggests limiting the use of social insurance numbers to those prescribed by law; and
- In notifying customers of the purposes for collection, clearly indicate types of information your organization is required to collect by law.

PRINCIPLE 5 – LIMITING USE, DISCLOSURE, AND RETENTION

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

Your Organization's Privacy Responsibilities

Under the “Limiting Use, Disclosure, and Retention” principle, your organization must:

- Never use or disclose personal information for purposes other than those for which it was collected, except with the consent of the individual or as required by law;
- Document any new purpose for collecting personal information;
- Retain personal information only as long as necessary to fulfill the purpose;
- If personal information has been used to make a decision about an individual, retain the information long enough to allow the individual access to the information after the decision has been made; and
- Develop guidelines and procedures to govern the disposal of personal information.

Under the “Limiting Use, Disclosure, and Retention” principle, your organization should:

- Destroy, erase, or anonymize any personal information that is no longer required to fulfill identified purposes³;
- Develop guidelines and implement procedures with respect to the retention of personal information; and
- Include minimum and maximum retention periods in these guidelines.

Note

- The “Safeguards” principle also refers to the destruction of personal information. Specifically, Principle 4.7.5 of Schedule 1 states:

Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information.

It should be noted that simple recycling of paper-based personal information is not the same as destruction.

³ Unless a request has been made to access the information in which case it should be retained as long as necessary to allow the individual to exhaust any recourse they may have including complaints to the OPC and any subsequent court proceedings.

How to Meet these Objectives

Limit Use and Disclosure

- Use or disclose personal information only for purposes identified and documented at the time it was collected;
- If your organization wishes to use or disclose personal information for any new purpose not identified at the time it was collected, document the new purpose, notify the persons concerned, and seek their consent (unless the new use or disclosure is required by law or unless an exception in Section 7 of PIPEDA applies); and
- Make sure that all staff handling personal information understand and respect the limitations on use and disclosure.

Retention and Destruction

- Review your organization's information holdings to determine if all personal information on file was collected for specific purposes and whether it is still necessary to fulfill the purposes for which it was collected or to comply with legislative requirements;
- If you determine that some personal information on file has no specific purpose or is no longer necessary, use appropriate safeguards to destroy, erase or anonymize it;
- Develop guidelines and implement secure procedures to retain and destroy personal information. Set retention and destruction schedules, including minimum and maximum retention periods, taking into account any legislative requirements which apply to your organization;
- Where personal information is used to make a decision about an individual, set a retention period that will give the individual a reasonable amount of time to access the information after the decision is made;
- Base your organization's retention policy and practices on the premise that information should be retained only as long as necessary for the fulfillment of the purposes for which it was collected;
- Conduct periodic audits or spot-checks of your holdings to ensure personal information is not being retained beyond established time frames;
- To prevent improper disclosure, establish secure methods for destroying information no longer needed (e.g., shredding paper files or securely deleting electronic records). Consider, for example, the risks associated with the disposal of computers where personal information has been left on the hard drive;
- Develop policies and/or contracts which apply to third parties engaged in the disposal of personal information on behalf of your organization; and
- For guidance on retention of personal information your organization collected before it became subject to PIPEDA, refer to the OPC document, Best Practices for Dealing with Pre-PIPEDA Personal Information available at <http://www.privcom.gc.ca/>.

PRINCIPLE 6 – ACCURACY

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

Your Organization's Privacy Responsibilities

Under the “Accuracy” principle, your organization must:

- Ensure that personal information is as accurate, complete, and up-to-date as necessary for the purposes for which it is to be used;
- Routinely update personal information only if such a process is necessary to fulfill the purposes for which the information was collected;
- Ensure that information is sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual; and
- In determining the extent to which personal information must be accurate, complete, and up-to-date, take into account the use of the information and the interests of the individual.

Under the “Accuracy” principle, your organization should:

- Keep any personal information that is used on an ongoing basis accurate and up-to-date, including information that is disclosed to third parties, where limits are not set out around the requirement for accuracy.

How to Meet these Objectives

Determine accuracy needs

- Review why your organization collects personal information, balancing how the information will be used and the interests of the customer;
- Personal information should be routinely updated only in circumstances where updating is necessary to fulfill the purposes for which the information was collected;
- Accuracy, completeness, and currency are essential in circumstances where the use of inaccurate, incomplete, or outdated information could negatively influence a decision to be made about a customer or otherwise harm the customer⁴;
- Assess the importance of accuracy, completeness, and currency in circumstances where information is used on an ongoing basis or is routinely disclosed to third parties; and
- Consider if you can reasonably expect customers to adopt responsibility themselves to correct or to provide up-to-date information, such as change-of-address notification for subscriptions.

⁴ For example, outdated financial information could cause a bank to deny a customer a loan or service.

Establish an Accuracy Policy

- Ensure that your privacy management framework includes procedures detailing:
 - the types of personal information that need to be routinely updated for accuracy and completeness;
 - where warranted, schedules and procedures for routinely verifying the accuracy of personal information and keeping it accurate and up-to-date;
 - a requirement to record when personal information is received or updated and the steps taken to verify accuracy, completeness, and currency of the information;
 - how customers can challenge the accuracy and completeness of personal information and how to amend their information as appropriate, in accordance with the “Individual Access” principle;
 - clear limits to the requirement for accuracy, and an explanation for any personal information that your organization:
 - › uses or discloses on an ongoing basis but does not intend to keep accurate and up-to-date;
 - › can reasonably expect customers to correct or update on their own initiative.
- Make information on your organization’s accuracy procedures readily available to the public, in accordance with the “Openness” principle.

PRINCIPLE 7 – SAFEGUARDS

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

Your Organization's Privacy Responsibilities

Under the “Safeguards” principle, your organization must:

- Protect personal information by security safeguards appropriate to the sensitivity of the information;
- Institute security safeguards that will protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification;
- Protect personal information regardless of the format in which it is held;
- Make employees aware of the importance of maintaining the confidentiality of personal information; and
- Use care to prevent unauthorized access when destroying or disposing of personal information.

Under the “Safeguards” principle, your organization should:

- Safeguard more sensitive information with a higher level of protection;
- Include among its methods of protection:
 - physical measures such as locked filing cabinets and restricted access to offices;
 - organizational measures such as security clearances and limiting access on a “need to know” basis; and
 - technological measures such as use of passwords and encryption.

Under the “Safeguards” principle, your organization may:

- Use a variety of safeguards, depending on the information's sensitivity, amount, distribution, format, and method of storage.

How to Meet these Objectives

Establishing an Informational Security Policy

- Review your present information security practices, policies, and systems to determine whether your organization is currently meeting its responsibilities outlined above. Take appropriate measures as recommended below to address any deficiencies; and
- Develop and implement a policy, or update your existing procedures, consolidating your information security practices and procedures in accordance with the “Safeguards” principle. Include a requirement and procedures for documenting and following up on security breaches and informing the individuals affected. Ensure that your policy addresses the following responsibilities as applicable.

Physical Safeguards

- Implement physical measures as necessary to ensure the security of personal information holdings, including:
 - locked filing cabinets;
 - clean-desk policy;
 - restricted access to personal information;
 - secured premises; and
 - alarm systems.
- Ensure that physical safeguards are appropriate to:
 - the sensitivity of the personal information (e.g., higher level of protection for information such as medical or financial records);
 - the amounts and types of information held;
 - the manner and extent of distribution or transmission;
 - format(s) (e.g., paper or electronic files);
 - method(s) of storage.
- Ensure that physical safeguards are sufficient to protect against loss or theft, and against unauthorized access, disclosure, copying, use, and modification.

Organizational Safeguards

- Implement organizational measures as necessary to ensure the security of personal information holdings, including:
 - authorization and limiting access on a “need-to-know” basis;
 - security clearances and classifications;
 - confidentiality agreements;
 - specific security procedures;
 - information security training;
 - regular internal monitoring of information security systems; and
 - regular independent monitoring and audit of information security systems.
- Ensure your organizational safeguards are appropriate to:
 - the sensitivity of the personal information (e.g., higher level of protection for information such as medical or financial records);
 - the amount of information held;
 - the manner and extent of distribution or transmission;
 - format(s) (e.g., paper or electronic files); and
 - method(s) of storage.
- Make certain that your organizational safeguards are sufficient to protect against loss or theft, and against unauthorized access, disclosure, copying, use, and modification.

Technological Safeguards

- Implement the technological measures necessary to ensure the security of personal information holdings including:
 - identification requirements (especially for online transactions) to establish legitimate identity for accessing personal information;
 - authentication (i.e., passwords or other unique identifiers for ensuring authorized access to personal information) See the OPC’s *Guidelines for Identification and Authentication* available at <http://www.privcom.gc.ca/>;
 - system access controls;
 - secure channels for transmissions of personal information;
 - encryption of sensitive data for storage and transmission;
 - firewalls and intrusion detection systems and procedures;
 - automatic audit trails for personal information processing systems;
 - system security maintenance controls including logs; and
 - security incident procedures and logs.
- Ensure that technological safeguards are appropriate to the:
 - sensitivity of the personal information (e.g., higher level of protection for information such as medical or financial records);
 - amounts and types of information held; and
 - manner and extent of distribution or transmission.
- Ensure that technological safeguards (regardless of whether wired or wireless technology is used) are sufficient to protect against loss or theft, unauthorized access, disclosure, copying, use, and modification; and
- When disclosing personal information, take measures appropriate to the sensitivity of the information and the method of disclosure to authenticate the identity of the individual.

Employee Awareness

- Set appropriate limits to employees’ access to, and use of, personal information held by your organization. As a general rule, grant authorization for access to personal information on a “need to know basis” (i.e., information required to perform defined job functions);
- Specify who is authorized to access and handle personal information held by the organization;
- Make employees aware of the importance of maintaining security and privacy of personal information. Where personal information is sensitive or where the potential consequences of improper disclosures are significant, use confidentiality agreements with employees;
- Train your staff on your organization’s policies and procedures for maintaining the security and confidentiality of personal information; and
- Conduct regular education and training to ensure continuing awareness and secure information handling on the part of employees.

Secure Disposal

- Institute procedures for secure disposal or destruction of personal information or the equipment or devices used for storing personal information;
- When disposing of or destroying personal information, take appropriate measures to prevent unauthorized parties from gaining access; and
- When disposing of equipment or devices used for storing personal information (such as filing cabinets, computers, diskettes, and audio tapes), take appropriate measures to remove or delete any stored information or otherwise to prevent access by unauthorized parties.

Telework & Working outside the Office

- Develop formal procedures for employees removing personal information outside the company, including the use of PDAs and laptops, working offsite or teleworking. Analyze the particular security risks which these situations create and develop solutions to limit the risks.

Securing Transmissions by Fax

- When transmitting personal information by fax, take security precautions as recommended in the OPC fact sheet, *Faxing Personal Information* available at <http://www.privcom.gc.ca/>; and
- If you must send sensitive personal information, consider more secure alternatives to transmission by fax.

PRINCIPLE 8 – OPENNESS

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

Your Organization's Privacy Responsibilities

Under the “Openness” principle, your organization must:

- Be open about its policies and practices relating to the management of personal information;
- Make specific information about such policies and practices readily available in a form that is generally understandable to your clients and customers;
- Include, in this information:
 - the name or title, and the address, of the person who is accountable for your privacy policies and practices and to whom complaints or inquiries can be forwarded;
 - a description of how to gain access to personal information the organization holds;
 - a description of what personal information is held, including a general account of its use;
 - copies of brochures or other means which explain your policies, standards, or codes; and
 - a description of what personal information you share with related organizations (e.g., subsidiaries).

Under the “Openness” principle, your organization may:

- Make information available in a variety of ways, depending on the nature of the business and other considerations.

How to Meet these Objectives

Developing Information for the Public

- Develop literature to explain your organization's personal information management policies and practices to the public, in keeping with the “Accountability” principle. Such materials may include policies, application forms, questionnaires, survey forms, pamphlets, brochures, Web site, etc.;
- As a minimum, include the following in such literature:
 - the name or title, and the address, of the designated privacy officer;
 - an indication that the privacy officer is the person to whom the public may direct complaints or inquiries about the organization's information management practices;
 - instructions on how the public can make privacy complaints to your organization;
 - instructions on how individuals can gain access to their personal information held by your organization;
 - a description of the types of personal information you collect and hold;
 - a description of the types of personal information you disclose to third parties (including subsidiaries and affiliates);
 - a description of why you use or disclose personal information; and
 - explanations of any other relevant policies, standards, or codes.

- As a best practice, include instructions on how customers may withdraw consent. Include such instructions as standard practice in any document used to notify customers of optional secondary purposes; and
- Make sure that all your public information on how you handle personal information is easy for the general public to understand.

Making Information Available

- In choosing methods and formats for making information available to the public, keep in mind your obligation to enable individuals to obtain information without an unreasonable effort;
- Depending on the nature of your business, make information available in a variety of ways in order to accommodate your clients and customers as far as possible. As appropriate, make brochures available at your place of business, mail information to customers, provide online access to information, or establish a toll-free telephone number for requesting information. Make sure that the message is consistent regardless of format; and
- If you rely on written materials to give notification of purposes and seek consent, make the materials readily accessible to the individual for reference during the consent process. As a best practice, supply such materials directly and draw the individual's attention to the specific purpose statements and consent clauses.

Web site Information

- In consideration of customers who may not have access to computers or the internet, do not use your Web site as the only means of making your privacy information publicly available. Requiring all customers to go online to find information about privacy policies and practices would generally not be considered a reasonable effort at making such information readily available;
- If your organization has a Web site, post your privacy policy on it. Make sure the policy covers all collections, uses, and disclosures of personal information made via the Web site itself; and
- Take appropriate measures to notify Web site users of all your organization's online information practices, notably the use of "cookies" or other non-visible tracking tools, and explain such practices in understandable terms.

PRINCIPLE 9 – INDIVIDUAL ACCESS

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Your Organization's Privacy Responsibilities

Under the “Individual Access” principle and Section 8 of PIPEDA your organization must:

- On written request, inform individuals of the existence, use, and disclosure of their personal information, and provide access to that information, except as specified in Section 9 of PIPEDA;
- Allow individuals to challenge the accuracy and completeness of personal information and have it amended as appropriate;
- Upon receiving a request in writing:
 - inform individuals whether or not you hold personal information about them;
 - allow the individual access to this information;
 - provide an account of how you have used or will use the information; and
 - inform individuals of third parties to which the information has been disclosed.

Note that section 4.9 of PIPEDA does provide that in certain situations, an organization may not be able to provide access to all personal information it holds but exceptions should be limited and specific and reasons for not providing access should be provided to the individual.

- When it is not possible to provide a list of organizations to which personal information has actually been disclosed, provide a list of organizations to which it may have been disclosed;
- On request, provide any assistance required by individuals in preparing an access request;
- Respond to an individual's access request at minimal or no cost to the individual;
- Respond to an individual's access request with due diligence and in any case not more than 30 days after receipt of the request (note that an acknowledgment letter does not constitute a response). You must either provide the information requested or indicate that you do not have the information requested within 30 days;
- Where an extended time limit is required, send the individual notice of extension no later than 30 days after the date of the request, advising of the new time limit, the reasons for the extension, and the right to complain to the OPC;
- Provide requested information in a format that is generally understandable (e.g., explain any abbreviations or codes used to record information);
- If you refuse an access request, inform the individual in writing, along with the reasons for the refusal and any recourse available to them under PIPEDA;
- Retain personal information that is the subject of a request for as long as necessary to allow the individual to exhaust any recourse under PIPEDA;
- When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, amend the information as required;
- Where appropriate, transmit amended information to third parties having access to the information;
- When a challenge is not resolved to the individual's satisfaction, keep a record of the details of the unresolved challenge; and
- Where appropriate, inform third parties having access to the information that an unresolved challenge exists.

Under the “Individual Access” principle, your organization should:

- Be as specific as possible about third parties to which personal information about an individual has been disclosed; and
- Where possible, indicate the source of the information when informing an individual that you hold information about them.

Under the “Individual Access” principle and Section 8 of PIPEDA, your organization may:

- Extend the 30-day time limit for a maximum of 30 extra days if:
 - meeting the time limit would unreasonably interfere with the activities of the organization, or
 - the time required to undertake any consultations necessary to respond to the request would make the time limit impracticable to meet;
- Extend the 30-day time limit for the period necessary for converting the personal information into an alternative format⁵;
- Respond to a request at a cost to the individual only if the individual has been informed of the approximate cost and has advised that the request has not been withdrawn;
- Choose to make medical information available through a medical practitioner;
- Ensure requestors provide sufficient information to permit you to provide an account of the existence, use, or disclosure of personal information, and use such information only for this purpose.

How to Meet these Objectives

Preparing for Access Requests

- Ensure your privacy framework includes procedures for handling requests for access to personal information. Take into account all above-mentioned responsibilities under the “Individual Access” principle and Section 8 of PIPEDA. Ensure you can address requests for personal information in alternative formats;
- Note all exceptions applicable to individual access as listed in Section 9 of PIPEDA. In any case where your organization refuses access, ensure that the refusal can be justified on the basis of a Section 9 exception;
- Ensure that your organization’s information systems can facilitate the retrieval and accurate reporting of an individual’s personal information, including disclosures to third-party organizations, and that requested information can be obtained with minimal disruption to operations;
- Ensure that staff assigned to process access requests know your organization’s responsibilities under the “Individual Access” principle, as well as the specific procedures and time limits to be observed and applicable exceptions under Section 9 of PIPEDA;
- Ensure that staff know how to identify an access request and refer it to an appropriate officer within the organization;
- Make information readily available to the public on how to request access to personal information with your organization.

⁵ Alternative formats can include Braille or audiotapes.

Processing Access Requests

- Help the individual prepare a request for access, which should be in writing, to personal information if required. On receiving an access request that requires clarification, ask the requester to supply enough further information to enable you to fulfill the request and use that information only for this purpose;
- On receiving an access request, record the date of receipt and confirm the requester's identity and right of access to the information;
- Respond to an access request as quickly as possible and in any case within 30 days, and with minimal or no cost to the requester.
- If you intend to charge costs, notify the requester of the approximate amount before processing the request, and confirm that he or she still wants to proceed;
- On a specific request:
 - inform the requester whether or not your organization has any personal information about him or her;
 - indicate the source of the personal information if possible;
 - explain how your organization has used or is using the information;
 - provide a list of any other organizations to which your organization has disclosed the information;
 - when it is not possible to provide a list of organizations to which information has actually been disclosed, provide a list of organizations to which it may have been disclosed;
 - give the requester access to the information; and
 - give the requester a copy of the information requested.
- Make sure all requested information is presented in understandable terms. Explain any acronyms, abbreviations, or codes.

Amending Personal Information

- Allow requesters to challenge the accuracy and completion of their personal information;
- If a requester can demonstrate that personal information is inaccurate or incomplete, amend the information in question. This can mean correcting, deleting or adding to the information;
- If the personal information has been disclosed to third parties, give the amended information to those parties as appropriate; and
- In cases where a challenge is not resolved to the individual's satisfaction, note the disagreement on the individual's file and advise third parties as appropriate.

Denial of Access

- If your organization refuses to provide access to requested personal information:
 - notify the requester, in writing, of the refusal within 30 days of receiving the request;
 - explain to the requester the reasons for the refusal, citing any relevant exceptions specified in Section 9 of PIPEDA; and
 - inform the requester of any recourse he or she may have (such as the right to complain to the OPC).
- Retain personal information that is the subject of a request for as long as necessary to allow the requester to exhaust any recourse under PIPEDA.

Extension of Time Limits

- Make every effort to respond to an access request within the normal 30-day time limit. Rely on a time limit extension only in cases where:
 1. responding within the original 30 days would unreasonably interfere with activities of your organization;
 2. additional time is needed to conduct consultations; or
 3. additional time is needed to convert personal information to an alternative format.
- Where an extension is warranted, do not extend the time limit for more than another 30 days in the case of items 1 and 2 above or for any longer than necessary in respect of item 3 above; and
- Where an extension is warranted, notify the requester in writing within 30 days of receiving the access request. At the same time, notify the requester of the reasons for the extension and of his or her right to complain to the OPC.

PRINCIPLE 10 – CHALLENGING COMPLIANCE

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization’s compliance.

Your Organization’s Privacy Responsibilities

Under the “Challenging Compliance” principle, your organization must:

- Enable individuals to address challenges concerning compliance with the 10 principles to the designated individual or individuals accountable for the organization’s compliance;
- Put in place procedures for receiving and responding to complaints or inquiries concerning the organization’s policies and practices relating to the handling of personal information;
- Establish complaint procedures that are easily accessible and simple to use;
- Inform inquirers or complainants of the existence of relevant complaint procedures;
- Investigate all complaints; and
- Take appropriate measures if a complaint is found to be justified, including amending policies and practices, if necessary.

Under the “Challenging Compliance” principle, your organization should:

- Ensure that the inquiries and complaints procedures it establishes are easily accessible and simple to use.

Under the “Challenging Compliance” principle, your organization may:

- Provide a range of complaint procedures, such as referring complaints about personal information handling practices to the organization’s regulatory body.

How to Meet these Objectives

Implementing Compliance Challenge Procedures

- Develop simple and easily accessible procedures for receiving and responding to inquiries and complaints about your organization’s personal information handling policies and practices;
- Ensure that front-line staff and managers are aware of these policies and procedures, can distinguish between an inquiry and a complaint under the law, and can refer individuals to the designated privacy officer or to other staff assigned to handle inquiries or complaints;
- Ensure that staff assigned to handle inquiries or complaints about your organization’s personal information handling policies and practices can do so knowledgeably, fairly, objectively, promptly, and efficiently;
- Make it easy for the public to find out how to make inquiries or lodge complaints with your organization. In keeping with the “Openness” principle, publicize the name or title, and the business address, of the person to whom inquiries or complaints should be directed (i.e., the privacy officer);

- Inform inquirers or complainants of your organization's procedures for handling inquiries or complaints. Make a point of informing them of any other recourse they may have from your organization's industry association or regulatory body; and
- Ensure management is committed to supporting the findings and recommendations of complaint investigations and to correcting any demonstrated deficiencies in your organization's personal information handling policies and practices.

Receiving Complaints

- Record the date of receipt and the nature of the complaint (e.g., denied access, delayed response to an access request, incomplete or inaccurate information on file, inadequate safeguards, or improper collection, use, disclosure, or retention);
- Promptly acknowledge receipt of the complaint; and
- If necessary, contact the complainant to clarify the matter at issue.

Complaint Investigations

- Investigate all complaints received;
- Assign the matter to a person having the skills necessary to review it competently, fairly, and impartially. Give that person access to all relevant records and to all employees or other parties who handled the personal information or the access request in question;
- Conduct the investigation without delay;
- When an investigation is completed, clearly and promptly notify the complainant of the outcome, of any resulting remedial action, and of any further recourse they may have if unsatisfied with the outcome;
- Where warranted by the findings of the investigation, grant access to information, amend any inaccurate or incomplete information, or modify the specific personal information handling policies, procedures, or practices at issue;
- Make your organization's staff aware of any such modifications; and
- To ensure future consistency in applying PIPEDA, record all investigation findings and remedial actions taken.

PART 2: DIAGNOSTIC CHECKLISTS

Once your privacy framework, has been implemented and has been operating long enough to verify its effectiveness, these checklists will allow you to assess how closely you meet the objectives in Schedule 1 of PIPEDA. Each question requires you to describe the evidence upon which the assessment has been based, and any mitigating circumstances to explain any “not met” responses. Evidence should be sufficient for the assessment to be meaningful. You should describe how you control personal information to meet each objective, whether through policies, procedures, processes, organizational structures and/or values.

There are two aspects to understanding how well a “privacy control” mechanism is working:

1. The privacy control⁶ needs to have been properly designed to meet the requirements of the law; and
2. The privacy control needs to be operating as intended (i.e., employees follow the policy).

You cannot determine how compliant you are with PIPEDA until you have assessed the design of your privacy control mechanisms and how well the mechanism is actually operating in the business environment.

Interpreting Self-Assessment Results

Before finalizing self-assessment results, review them with each business unit that was observed. Note any mitigating circumstances that caused a poor result. For example, a review of employee files for completed consent forms during a two-month period that registered a poor result may have been due to the fact that a summer temporary student was assisting Human Resources. If files were checked from another period in time, the results may have been different.

A mature privacy management framework is characterized by due diligence and documentation of risk acceptance or mitigation decisions which should help set priorities for remedial action and define a realistic timeline for completion.

If your organization is unable to indicate how it has met stated objectives, then there is a risk that your organization may not be in compliance with PIPEDA. You should carefully consider risks involved in any area where you have not met the objectives, and address gaps in your privacy management framework accordingly. Remember that a single corrective action may address multiple objectives, so it is important to track corrective actions and each of the positive impacts to reported assessment deficiencies.

Evaluating the results of the self-assessment will enable your organization to dedicate resources to improving privacy practices in the right areas. Review your self-assessment results to understand if there are particular principles against which your organization exhibits weaknesses, or if it is a case of your organization’s level of maturity.

A privacy program matures over time, so the evaluation of your organization’s compliance should be put into the context of this maturity curve. When considering how to evaluate your program against your compliance objectives and best practices, consider a scale that will have relevance across your organization. The maturity

⁶ In this context, a “privacy control” can be a policy, set of procedures, which you have implemented to address each one of the 10 principles.

scale should also be flexible enough to apply to various business units and stakeholders. You may consider the following to evaluate your total results for each principle reviewed:

- **Maturity Level 1** – Non-existent / Undeveloped (Not Met Assessment)
- **Maturity Level 2** – Early Stages of Development (Partially Met)
- **Maturity Level 3** – Advanced (Requirements Mostly Met – improvements possible)
- **Maturity Level 4** – Fully developed - (Requirements Consistently Met – only minor or no adjustments needed)

Action Planning:

The results of the self-assessment may indicate that risks to privacy and compliance exist within your organization. Privacy risk is the potential that a given threat will exploit vulnerabilities of:

- an asset containing personal information, and/or
- a business process involving personal information to cause unintentional access or modification/damage to the personal information.

Risks may be to your organization, your customers or both.

The impact or severity of the risk is proportional to its estimated likelihood of occurrence and its potential impact to the organization and individual.

A Privacy Impact Assessment is the identification and analysis of relevant risks to privacy, and forms the basis for how these risks should be managed, including what measures should be implemented to mitigate the risk to an acceptable level.

Prioritize the deficiencies in your privacy program and create an action plan. Areas of non-compliance can be ranked by conducting a privacy risk assessment process:

- Identify all “not met” or “partially met” responses in your self-assessment and flag them for review;
- Consider the potential implications of not/partially meeting the objective. As an example:

Objective / Criteria:

You investigate all complaints you receive about your personal information handling policies and practices.

Potential Implications:

If this is not done, it increases the risk that the underlying privacy issues will not be identified and resolved in a timely manner, which will in turn diminish customer satisfaction.

Determine if you have identified any compensating controls to mitigate the potential implications of not meeting your compliance responsibilities. If compensating controls are not in place, identify the additional mitigation strategies necessary to close the gap between required practice and your current practices, in order to better manage the privacy risks identified through the previous step.

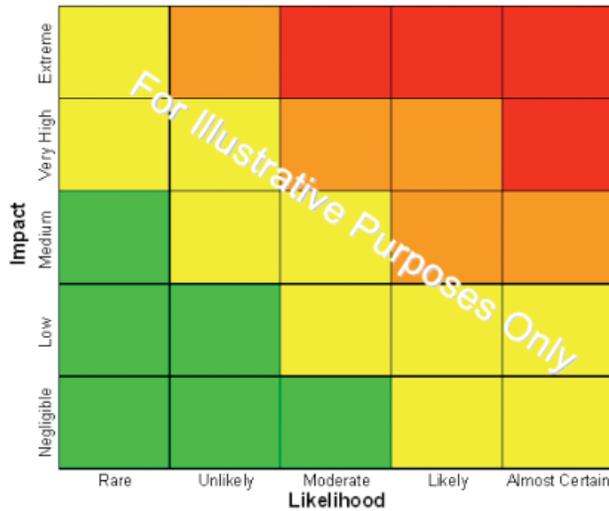
Whether you have partial or no controls in place, use the information from the assessment and your knowledge about the organization to determine how likely it is that this adverse event will occur, and the possible impact if it does. The following is an example of a scale you can use to assess these factors for each of the objectives identified as deficient:

LIKELIHOOD OF OCCURRENCE		
LEVEL	DESCRIPTOR	DESCRIPTION
5	Almost Certain	Event occurs regularly here.
4	Likely	Event has occurred here more than once, or is occurring to others in similar circumstances.
3	Moderate	Event has occurred here before, or has been observed in similar circumstances.
2	Unlikely	Event has occurred infrequently to others in similar circumstances, but has not occurred here.
1	Rare	Event has almost never been observed; it may occur only in exceptional circumstances.

IMPACT		
LEVEL	DESCRIPTOR	DESCRIPTION
5	Extreme	<p>A major event with the potential to lead to long-term damage to an organization’s ability to meet its objectives.</p> <p>The consequences would cause serious, long-term regulatory, reputational, financial or operational problems to the organization and require top-level management intervention. It could also cause significant reputational, financial and/or emotional distress to the individual as the subject of an information privacy breach.</p>
4	Very High	<p>A critical event, which with proper management, can be endured by the organization.</p> <p>The consequences of such an event could include significant regulatory, reputational, financial or operational concerns for the organization, and require top-level management intervention. It could cause significant reputational, financial and/or emotional distress to the individual as the subject of an information privacy breach.</p>
3	Medium	<p>A significant event that can be managed under normal circumstances by the organization.</p> <p>The consequences could cause regulatory, reputational, financial, or operational problems but could be managed internally by the organization. This category could also result in a moderate consequence to the individual, such as exposure of some financial information e.g., salary. The impact to the individual has the opportunity to be contained within the organization and further exposure is limited.</p>
2	Low	<p>An event where consequences can be absorbed, but management effort is required to minimize the impact.</p> <p>The consequences might threaten regulatory, reputational or operational standards but would be dealt with internally. This would be of low consequence for the organization. The impact to the individual has the opportunity to be contained within the organization and further exposure limited.</p>
1	Negligible	<p>An event, the consequences of which can be absorbed through normal activity.</p> <p>The consequences might threaten regulatory, reputational or operational standards but would be dealt with internally. This would be of low consequence for the organization. The impact to the individual has the opportunity to be contained within the organization and further exposure limited.</p>

Rank the results of your risk assessment. If the occurrence of an adverse event is probable (e.g., you know your organization has two complaints a month, and you have no controls in place to handle them) and the impact is also significant (where for example you suspect damage to your credibility and brand or a complaint may escalate to the OPC) then it should be ranked higher than deficiencies that have a lower likelihood of occurrence and a lower impact.

Plot the results of this ranking onto a heat map to understand the relative ranking of your deficiencies. A sample heat map graphic is provided below:



Develop specific actions to close any gaps by modifying your privacy framework to either reduce the likelihood of the adverse event occurring or reduce the impact of the event. Often the controls you choose will have a positive impact on both of these aspects of risk, and may have the potential to address multiple deficiencies.

Go through your list of what you need to do to address gaps in your privacy framework. Identify where a single activity will have an impact on more than one objective. You may also focus on those action items that mitigate higher risks, yet are relatively easy to implement.

Identify specific projects that will improve privacy operations. The information you have gathered from the self-assessment process, including information about risk, can be used to develop a business case for additional budget and resources.

CHECKLIST FOR PRINCIPLE 1 – ACCOUNTABILITY

Statement	Assessment			Evidence	Actions
	Met	Not Met	Partially Met		
You have reviewed your privacy policies and are satisfied that they are complete and easy to understand.					
You have clearly delineated who, within your organization, is responsible for privacy governance and management.					
You have privacy policies and practices that apply to the personal information of your employees as well as that of your customers.					
Your privacy framework clearly articulates that you will be responsible for all personal information you hold or control, including information which has been transferred to a third party for processing.					
You have appointed at least one person to be responsible for the organization's overall compliance with PIPEDA.					
You have directed staff through policy, procedure or training to provide the name, address and phone number of the PIPEDA contact person to individuals when requested.					
You use contractual agreements to ensure a comparable level of privacy protection is offered to personal information while it is in the custody of a third party for processing.					
You have verified that third parties have implemented the privacy controls stated in any contractual agreements.					
You are accountable for the protection of personal information.					
Your privacy framework addresses the principle of "identifying purpose" regarding personal information.					
Your privacy framework addresses the principle of "consent" regarding personal information.					
Your privacy framework addresses the principle of "limiting collection" of personal information.					
Your privacy framework addresses the principle of "limiting use, disclosure and retention" of personal information.					
Your privacy framework addresses the principle of "accuracy" regarding personal information.					
Your privacy framework addresses the principle of "safeguards" with respect to personal information.					
Your privacy framework addresses the principle of "openness" regarding personal information.					
Your privacy framework addresses the principle of "individual access" regarding personal information.					
Your privacy framework addresses the principle of "challenging compliance" regarding personal information.					
You have communicated information related to personal information handling policies, procedures and practices to staff.					
You have trained staff regarding the protection of personal information by informing them of organizational privacy policies, procedures and best practices.					
You have the means in place to identify which of your staff should be trained in privacy, including new staff and refresher training of existing staff.					
You have developed documentation to explain your personal information protection policies and procedures to customers and the general public.					

SUPPLEMENTAL ASSESSMENT FOR FEDERAL WORKS, UNDERTAKINGS OR BUSINESSES:

Statement	Assessment			Evidence	Actions
	Met	Not Met	Partially Met		
You have developed information to explain to your employees the policies and procedures which apply to their own personal information.					

CHECKLIST FOR PRINCIPLE 2 – IDENTIFYING PURPOSES

Statement	Assessment			Evidence	Actions
	Met	Not Met	Partially Met		
You identify why you are collecting personal information at or before the time of collection.					
You have documented your purpose(s) for collecting personal information.					
You have notified clients and customers of new purposes for which you will use information if they weren't identified at the time information was collected.					
You seek the consent of clients and customers before using information for any new purpose if required.					
You have notified clients and customers of the purposes before using or disclosing the information if notification at the time of collection was not practicable.					
You have determined the amounts and types of personal information needed to fulfill your purpose(s).					
You have determined why you are collecting personal information and that the amount and types of personal information collected are reasonable in normal business circumstances.					
You have distinguished between essential information (required for primary business purposes) and non-essential information (voluntary information which facilitates use for secondary purposes).					
You have identified non-essential information as voluntary and have provided staff with information on how to proceed when clients and customers opt out of secondary uses.					

CHECKLIST FOR PRINCIPLE 3 – CONSENT

Statement	Assessment			Evidence	Actions
	Met	Not Met	Partially Met		
You obtain customer consent for any collection, use or disclosure of personal information.					
If you don't obtain customer consent for the collection, use and disclosure of personal information, you have determined that it is not required under s.7 of PIPEDA.					
You make reasonable efforts to ensure that clients and customers are notified of the purposes for which personal information will be used or disclosed.					
You do not require clients and customers to consent to the collection, use or disclosure of personal information beyond what is necessary to fulfill explicitly specified and limited purposes as a condition of supplying a product or service.					
You assess the purposes and limit the collection, use and disclosure of personal information when it is required as a condition for obtaining a product or service.					
You obtain consent through lawful and fair means.					
You allow a client or customer to withdraw consent at any time subject to legal or contractual restrictions and reasonable notice.					
You inform clients and customers of the implication of the withdrawal of consent.					
You consider the sensitivity and intended use of personal information, and the reasonable expectations of clients and customers in determining which form of consent (implied or expressed) you will accept for the collection, use and disclosure of personal information.					

CHECKLIST FOR PRINCIPLE 4 – LIMITING COLLECTION

Statement	Assessment			Evidence	Actions
	Met	Not Met	Partially Met		
You limit the amount and type of personal information you collect to what is necessary for the identified purpose.					
You collect information only by fair and lawful means.					
You have documented the specific types of information you collect along with the purposes for collection.					
You have documented when you collect information from sources other than the individual about whom it pertains.					
You distinguish between mandatory and optional collection of personal information.					
You limit your collection of the SIN to legally established purposes.					

CHECKLIST FOR PRINCIPLE 5 – LIMITING USE, DISCLOSURE, AND RETENTION

Statement	Assessment			Evidence	Actions
	Met	Not Met	Partially Met		
You do not use or disclose information for purposes beyond those for which it was collected, except with the consent of the individual or as required by law.					
You document new purposes conceived after the personal information is collected.					
You only retain personal information as long as necessary to allow for the fulfillment of identified purposes.					
You retain personal information used to make decisions about an individual long enough for the individual to request access to it.					
Your privacy management framework governs the destruction of personal information, including the role of contractors performing such services.					

CHECKLIST FOR PRINCIPLE 6 – ACCURACY

Statement	Assessment			Evidence	Actions
	Met	Not Met	Partially Met		
You take reasonable measures to ensure that personal information is accurate, complete and up-to-date prior to using the information to make decisions.					
You only update personal information if the process is necessary to fulfill the purposes for which the information was collected.					
Your privacy management framework addresses the accuracy, completeness and currency of personal information which includes a process through which individuals can challenge the accuracy of information.					
Your privacy management framework specifies when updates are appropriate based on the defined purposes and uses of the information as well as the interests of the individual.					
You record when and where key information was collected, including dates of corrections or updates to such information.					
You conduct periodic spot-checks, assessments or audits of information holdings and databases to ensure that key information is accurate, complete and up-to-date.					

CHECKLIST FOR PRINCIPLE 7 – SAFEGUARDS

Statement	Assessment			Evidence	Actions
	Met	Not Met	Partially Met		
You have adopted physical, technical and administrative safeguards to protect personal information against loss or theft as well as unauthorized access, disclosure, copying, use or modification.					
You choose security safeguards that are commensurate with the sensitivity of the information and the means used to transmit it.					
You protect all personal information regardless of the format in which it is held.					
You make your employees aware of the importance of maintaining the confidentiality of personal information.					
You have implemented processes to prevent unauthorized access to personal information during the disposal or destruction of information.					
You have implemented and adhere to your various information security policies and practices.					
You have established an information security breach policy and commit to investigating the root cause of such breaches.					
You have developed and implemented policies and practices including appropriate safeguards for all uses of personal information outside the office.					

CHECKLIST FOR PRINCIPLE 8 – OPENNESS

Statement	Assessment			Evidence	Actions
	Met	Not Met	Partially Met		
You make information regarding policies and procedures related to the management of personal information available to individuals.					
You explain to customers why you collect, how you use and when you will disclose their personal information.					
You make information available to clients and customers regarding who within the organization can address questions or complaints regarding the handling of personal information.					
You make the name/title and address of the person accountable for the organization's privacy policies available on request.					
You describe to your clients how they can obtain access to or correct their personal information.					
You provide individuals with a description of what personal information you hold and what you disclose to other organizations.					

CHECKLIST FOR PRINCIPLE 9 – INDIVIDUAL ACCESS

Statement	Assessment			Evidence	Actions
	Met	Not Met	Partially Met		
You have adopted policies and procedures for responding to requests for personal information under PIPEDA.					
You have advised staff of the need to direct requests for access to information to the staff member responsible for processing these requests.					
You inform individuals of the existence, use and disclosure of their personal information on receipt of a written request.					
You provide individuals with access to personal information on receipt of a written request.					
You limit refusal to provide access to information to exceptions described in Section 9 of PIPEDA.					
You provide an account of the uses of information on request.					
You provide an account of all third parties to whom information has been disclosed (or a listing of the types of third parties to whom such information is generally disclosed) on receipt of a request for such a list from an individual.					
You assist those individuals who indicate they need help to complete a request for information.					
You respond to a request for information at minimal or no cost to the individual.					
You respond to a request for information in not more than 30 days unless you notify the requestor within that time period of your need to extend the time limit for response, indicate the extended time limit and inform the requester of his or her right to complain to the OPC.					
You rely on time limit extensions only in cases where responding within the original 30 days would unreasonably interfere with your activities, when additional time is needed to conduct consultations, or when additional time is needed to convert personal information to an alternative format.					
You provide access to information in a format which is legible and will provide an explanation of abbreviations or codes on request from an individual.					
You advise requestors of the reasons for refusal and recourse available to them when refusing to provide information.					
You allow individuals to challenge the accuracy of personal information and amend information when an individual demonstrates that information is inaccurate or incomplete.					
You forward corrected personal information to third parties who would have received the original information.					

CHECKLIST FOR PRINCIPLE 10 – CHALLENGING COMPLIANCE

Statement	Assessment			Evidence	Actions
	Met	Not Met	Partially Met		
You enable individuals to address compliance challenges to the designated individual responsible for PIPEDA.					
You have policies and procedures in place for receiving and responding to complaints or inquiries about your personal information handling policies and practices.					
You advise individuals or complainants of the existence of all relevant complaint processes, including the right to make a complaint to a regulatory body.					
You investigate all complaints you receive about your personal information handling policies and practices.					
You modify your actions if a complaint is substantiated, and take steps to minimize the likelihood that the issue will recur.					

APPENDIX A

OVERVIEW OF PIPEDA

Organizations subject to the *Personal Information Protection and Electronic Documents Act* (PIPEDA) should be familiar with the *Act*. This self-assessment tool should be used in conjunction with the *Act*. Information about PIPEDA can be found on the OPC Web site at <http://www.privcom.gc.ca/>.

The purpose of PIPEDA is to support and promote electronic commerce by protecting personal information. Part I of the *Act* establishes reasonable rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals. Other parts of the *Act* provide for electronic alternatives and facilitate the use of electronic documents and publications for various purposes.

Organizations covered by the *Act* must obtain an individual's consent when they collect, use or disclose the individual's personal information. The individual has a right to access personal information held by an organization and to challenge its accuracy, if need be. Personal information can only be used for the purposes for which it was collected. If an organization is going to use it for another purpose, consent must be obtained again. Individuals should also be assured that their information will be protected by specific safeguards, including measures such as locked cabinets, computer passwords or encryption.

An organization is responsible for the protection of personal information and the fair handling of it at all times, throughout the organization and in dealings with third parties.

WHAT ORGANIZATIONS ARE SUBJECT TO PIPEDA?

In the Course of Commercial Activities

PIPEDA applies to every organization that collects, uses or discloses personal information in the course of commercial activities. PIPEDA defines commercial activity as:

any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists.

The term organization includes “an association, a partnership, a person and a trade union.” The definition of organization is intended to be broad and inclusive.

The federal government may exempt organizations and/or activities in provinces that are deemed to have adopted substantially similar privacy legislation. In those provinces that have passed substantially similar legislation, PIPEDA will continue to apply to the federally regulated private sector — such as banks, airlines, telephone and broadcasting companies, and railways — and to personal information in inter-provincial and international transactions by all organizations engaged in commercial activities. To date, Quebec, British Columbia, Alberta, and, in matters relating to health care, Ontario, have promulgated legislation deemed substantially similar to the federal law.

Municipalities, Universities, Schools and Hospitals

The *Constitution Act, 1867* gives the provinces authority over municipal institutions, education and hospitals. PIPEDA is based on the federal government’s jurisdiction over “the regulation of trade and commerce.”

While municipalities, educational institutions and hospitals may occasionally provide services on a fee basis, they are not, on the whole, engaged in trade and commerce as contemplated by the Canadian Constitution. Furthermore, these institutions are completely or largely dependent on municipally or provincially levied taxes and provincial grants.

As a result, the OPC is of the view that, as a general rule, PIPEDA does not apply to the core activities of municipalities, universities, schools, and hospitals. By core activities we mean those activities that are central to the mandate and responsibilities of these institutions.

Providing a service for a fee does not necessarily trigger the application of the *Act* if the service is part of the institution’s core activities. For example, charging a fee for a private room or charging extra for a fiberglass cast does not automatically make a hospital or even that transaction subject to the *Act*. Similarly, a municipality can charge a per bag fee to collect garbage, or charge for the use of a playing field or arena, without becoming subject to the *Act*.

A municipality, university, school or hospital may become subject to the *Act* when it engages in a non-core commercial activity, unless substantially similar provincial legislation applies. For example, if a university sold or bartered an alumni list, that activity would be considered a commercial activity and that particular transaction would be subject to the *Act*. As well, personal information collected by a university or a hospital in the course of operating a parking garage would probably be subject to the *Act* since this would not be considered a core activity.

A coffee shop in a hospital or university, a TV rental service in a hospital, a university bookstore or any other business operated by a third party within one of these institutions would be subject to the *Act* just as a coffee shop in a shopping mall is subject to the *Act*, unless substantially similar provincial legislation applies.

Private educational institutions and private hospitals are in a different situation. Generally speaking, many of these institutions are more clearly engaged in commercial activities and we would recommend that they operate on the assumption that they are subject to PIPEDA, unless substantially similar provincial legislation applies.

The Health Care Sector

The core activities of public hospitals or publicly funded long-term care facilities are not subject to PIPEDA. However, health care providers in private practice such as doctors, dentists and chiropractors are engaged in a commercial activity and thus subject to the *Act*, unless substantially similar provincial legislation applies. For additional information on the application of PIPEDA to the health care sector see http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/h_gv00207e.html. Alberta, Saskatchewan, Manitoba and Ontario have enacted personal health information legislation that applies to the health care sector, including hospitals. Quebec’s *Act respecting health services and social services* also contains important provisions regarding personal health information.

Provincial Legislation

In many provinces, personal information collected by municipalities, universities, schools and hospitals is protected by provincial legislation. Typically, this is public sector legislation, often a *Freedom of Information and Protection of Privacy Act*. In some cases, health information protection acts and private sector acts may also apply. For additional information on relevant provincial legislation see http://www.privcom.gc.ca/prov/index_e.asp.

The Territories

The situation in the three Territories is somewhat more complex. PIPEDA applies to all federal works, undertakings and businesses (FWUBs) and to the personal information of employees of FWUBs. A FWUB is “any work, undertaking or business that is within the legislative authority of Parliament.”

Since all organizations in the Territories are considered to be FWUBs, PIPEDA applies to information about employees of municipalities, universities, schools and hospitals in the Territories.

However, PIPEDA does not apply to patient or student information in publicly-funded hospitals or schools in the Territories because they are not considered to be engaged in commercial activities.

APPENDIX B

PRIVACY SELF-ASSESSMENT

What Is Privacy Self-Assessment?

The OPC views privacy self-assessment as a process whereby an organization initiates an evaluation for the purpose of benchmarking and improving its own privacy systems and practices over time. This includes assessing the organization against a defined set of expectations to determine the degree to which they are met. In measuring compliance, gaps and/or risks may be identified for the purpose of guiding and following up remedial action.

There are three basic ways an organization might carry out such evaluations:

1. The business unit itself analyzes and assesses its degree of compliance against the privacy standard. This is commonly referred to as “self-assessment” since it is done by responsible operating managers. This might be done with assistance of a facilitator;
2. Another party within the organization, but independent of the business unit under review, is engaged to assess the extent of compliance with the standard (e.g., an internal auditor). A combination of (1) and (2) might also be undertaken; and/or
3. An external third party conducts an independent assessment (e.g., an external auditor).

There are also a variety of approaches an organization might take in terms of scope and frequency of assessment. Whatever the approach, we advise doing self-assessment on a planned continuous/cyclical basis.

The approaches include:

- conducting a single assessment exercise across the organization at one point in time. This approach might prove most efficient if your organization is relatively small; or
- creating a schedule whereby business units are assessed according to a risk-based schedule (e.g., assessing the riskiest units first where, for example, there is a large volume of financial or health information being acquired, stored and processed); or
- a pilot project might be conducted in a small unit first to validate and adjust the approach as needed, before tackling larger or riskier units.

What Are the Benefits of Self-Assessment?

The OPC believes organizations should be proactive in ensuring compliance with privacy laws. Along with other characteristics (such as a privacy policy), self-assessing demonstrates a responsible privacy management culture within an organization. Ultimately, sound life cycle management of personal information is intimately tied to an organization’s reputation and branding, business relationships, legal liability, customer loyalty and business growth. Self-assessment is in an organization’s self-interest.

It is important to appreciate that a self-assessment tool should be applied as part of a well-structured privacy program. Self-assessments done on a routine or periodic basis are valuable tools that help an organization respond to changing factors in their environment; factors that may keep the organization from meeting stated objectives.

During the research for developing this guide, the OPC learned of some privacy assessment/risk management tools being used within organizations such as IBM Canada and the Workplace Safety & Insurance Board. There are models out there and self-assessment is indeed possible. More significantly, they indicate that self-assessment is a constructive way of changing behavior and increasing privacy awareness. Moreover, it can yield business benefits by diagnosing business processes. Self-assessment also distributes accountability for privacy and can enhance the role of a Chief Privacy Officer.

How to Prepare for your Self-Assessment

This compliance exercise entails not only ensuring that privacy controls have been designed, but also gathering evidence that these controls have been effectively implemented. For example, to test the effective implementation of a policy stating that express consent is required for the collection of personal information, evidence that such consent has been obtained should be gathered on a sample basis. The more evidence that is gathered on your organization's compliance, the better you will be able to identify and evaluate privacy risks.

Assessments need to be carefully planned in order to be successful. They will require time and resources to complete. More importantly, the organization should be prepared to consider assessment results and invest in appropriate courses of action to address unacceptable risks and strengthen its privacy management capabilities. No self-assessment is of much use unless identified gaps (weaknesses) are subject to a management action plan and such plans are followed up by management.

There are a few preparatory activities that need to be completed before starting the self assessment exercise. All of these activities, in and of themselves, will help to reduce information gaps during the actual self-assessment. These activities include: developing an assessment plan; conducting a personal information inventory; and conducting a policy and procedure inventory and review.

Developing an Assessment Plan

Develop a plan that describes the business area(s) to be assessed, a brief description of the services that the business area provides, the principle(s) they will be assessed against and the timeline for assessment. For each of the areas, determine whether you are assessing the:

- “design effectiveness” of the privacy controls, judging whether the control is designed to meet the stated objective;
- “implementation effectiveness”, evaluating whether the controls are implemented as they should be; and/or
- “operating effectiveness”, evaluating whether controls have been implemented and are operating effectively over a certain period of time.

In order to evaluate whether a privacy control has been designed effectively, you need to know the requirement that the control is intended to achieve. For example, if an overarching privacy policy is supposed to articulate the organization's commitment to the 10 principles of *PIPEDA*, then the policy should be evaluated to determine if it meets that requirement. If it does, it has been designed effectively. In order to understand whether a control is implemented effectively, the organization must understand the objective of the control. If automated security access controls within an application are intended to enforce limiting the disclosure of personal information, you may need to do a few tests to determine if only those with a “need to know” can access personal information.

If the assessment plan includes evaluating all of these aspects of your privacy policy, procedures, processes and governance structures, provide for a sufficient amount of time, depending on the volume of material to review/analyze.

Conducting a Personal Information Inventory

This high-level inventory should be completed by each business area that will be involved in the assessment exercise. Use a table or spreadsheet to create an inventory about of the type of personal information collected and where it is kept within the organization. For example, the inventory may identify the name of an application (e.g., PeopleSoft), the series of hardcopy or electronic files within the application (e.g., HR staffing files, pay and benefits files, evaluation files). The inventory should describe, at a high level, the type of the personal information (e.g. medical, financial, HR), how it is collected, used, disclosed, maintained, and disposed of or archived.

Depending on the number of business processes and information systems within your organization involved in the collection, use or disclosure of personal information, this task can become a very significant undertaking. Starting with a pilot project of a more manageable scale might prove more feasible in those situations. Another way to understand personal information holdings of an organization is to develop business process diagrams for each major organizational activity being assessed, that would show a high level flow of personal information throughout its lifecycle.

While such work may be significant and done for privacy purposes, it would also likely be of value for security and business delivery purposes. Indeed, having a collective handle on what personal information is collected and why and how it is secured, stored, transmitted, used and disposed of is often a vital corporate need. Personal information is a corporate asset, often a key asset.

To effectively complete the Personal Information Inventory, use the following questions as a guide:

- What does PIPEDA mean by the term “personal information”, and how does that definition apply in the context of my organization?
- What personal information does our organization collect?
- How and in what situations do we collect it?
- Why do we collect it?
- Who in the organization uses personal information?
- Who has access to it?
- Where do we store it?
- In what formats (e.g., electronic, paper, audiotape) do we keep it?
- How do we keep it secure?
- What personal information do we disclose to other organizations, and why?
- To what other organizations do we disclose the information and how?
- How long do we keep personal information?
- How long do we need to keep it?
- When and how do we dispose of it?

Note: When PIPEDA uses the term “reasonable” it asks “is the information being used in a manner in which a reasonable person would consider appropriate?”

Conducting a Policy and Procedure Inventory

Make a list of the policies and procedures that are relevant to the management of personal information. These will include privacy policies and procedures, but they also may include security, records and information management, data management and confidentiality policies and procedures. You may wish to divide your policies and procedures into those that apply to the whole organization and those that are business unit/business process specific.

There are multiple ways in which to carry out the self-assessment process. Depending on the scope of the assessment, the plan can be executed using a:

-
- Privacy Compliance Assessment Committee structure. Considering the complex and multi-faceted nature of privacy, a committee might be required to ensure privacy issues are comprehensively analyzed. Committee members could, for example, represent various business units, such as Information Technology,
- Legal and Communications/Marketing;
 - Lead facilitator to support Business Unit Assessment Teams; or,
 - Privacy Compliance Assessment Project Manager along with a consistent Compliance Assessment Team.

Once the planning phase has been completed, it is important to review the plan with management. Ongoing and visible support of management will be a critical success factor for the Assessment. There should also be a Communications Plan in place that specifies how the results of each Assessment will be reviewed with the business unit, how the overall report will be presented and key messages to release throughout the project.

APPENDIX C

OTHER GUIDANCE AVAILABLE FROM THE OPC

This self-assessment tool has been designed primarily with medium to large organizations in mind. OPC has developed an E-learning tool for small retail businesses that would be of assistance to such organizations. This can be found on the OPC Web site at <http://www.privcom.gc.ca/>.

You may find the following guidance and fact sheets to be of assistance and complimentary to this self-assessment tool:

- Compliance Framework of the OPC
- Privacy Breach Guidelines
- Questions and Answers regarding the application of PIPEDA
- Determining the appropriate form of consent under PIPEDA
- Faxing Personal Information
- Best Practices for dealing with pre-PIPEDA personal information (grandfathering)
- Best Practices for the use of Social Insurance Numbers in the private sector
- Guidelines for Recording Customer Telephone Calls
- Organizations' Guide to Complaint Investigations under PIPEDA
- Application of PIPEDA to Charitable and Non-Profit Organizations
- Application of PIPEDA to Employee Records
- Privacy in the Workplace
- Complying with PIPEDA
- Privacy Questionnaire: Is your Business Ready?
- An Overview of PIPEDA for Businesses and Organizations
- Information on PIPEDA for Health Care Sector Organizations

You may also wish to refer complaint investigations as made public by the OPC in its Annual Reports or posted at <http://www.privcom.gc.ca/>.