

**Getting Ready for Privacy Legislation**

---

**CHECKLISTS**

---

**Privacy Requirements and Policies for  
Health Practitioners**

**PUBLISHED BY THE COLLEGE OF OCCUPATIONAL  
THERAPISTS OF ONTARIO  
SEPTEMBER 2003**

**This booklet is not intended to provide legal advice. It provides some practical suggestions for how some organizations can review their information handling practices and develop a Privacy Policy. The *Personal Information Protection and Electronic Documents Act* is open to interpretation in a number of areas and is enforced by the federal Information and Privacy Commissioner. Thus, the descriptions provided below are based on current information and may change as experience with the legislation and its enforcement develops. Some provisions in the Act are simplified for the purpose of identifying issues for consideration. For legal advice, please speak to your own lawyer.**

Adapted from the work of:  
Richard Steinecke  
Steinecke Maciura LeBlanc  
Barristers & Solicitors

Original Work Copyright © 2003 by Steinecke Maciura LeBlanc  
Used with permission

## INDEX

	<b>Page</b>
Introduction .....	2
Step 1 – Designating Your Organization’s Information Officer.....	2
(a) Identifying Your “Organization” .....	2
(b) Selecting your Information Officer.....	2
Step 2 – Information and Activities Covered by the Privacy Plan .....	2
(a) Commercial Activities .....	2
(b) Inventory of Personal Information Collected .....	3
Step 3 – Collecting Personal Information.....	3
(a) Principles of Identifying Purposes and Obtaining Consent.....	3
(b) Primary Purpose and Consent / Other Legal Authority Checklist.....	3
(c) Related and Secondary Purposes Checklists .....	12
(d) Principles of Use and Disclosure .....	18
Step 4 – Safeguards, Retention and Destruction .....	19
(a) Safeguarding Personal Information .....	19
(b) Retention and Destruction of Personal Information .....	23
Step 5 – Access, Correction, Complaints and Openness .....	24
(a) Access Rights .....	24
(b) Correction Requests .....	24
(c) Complaints System .....	25
(d) Openness .....	26
Step 6 – Implementing Your Privacy Plan .....	26

## Introduction

Completing the checklists will assist an organization to comply with the requirements of PIPEDA. Boxes “” are to be ticked off when appropriate and blanks “\_\_\_\_\_” are to be filled in where they apply to your organization. See the accompanying Guide for assistance in completing this Checklist document.

### Step 1 – Designating Your Organization’s Information Officer

Date of Privacy Plan: \_\_\_\_\_

#### (a) Identifying Your “Organization” *(See Guide)*

Name of Organization: \_\_\_\_\_

List any consultants and agencies included within this organization:

---

---

---

#### (b) Selecting your Information Officer *(See Guide)*

Name of Information Officer: \_\_\_\_\_

### Step 2 – Information and Activities Covered by the Privacy Plan

The Personal Information Protection and Electronic Documents Act (PIPEDA) applies to any “commercial activities” of the organization that involve “personal information”. It is important to first identify what commercial activities your organization engages in and what personal information it collects, uses and discloses in the course of those activities. Only then can you go to the next step to assess whether your current information practices require change.

#### (a) Commercial Activities *(See Guide)*

Prudent organizations will act on the assumption that PIPEDA applies to the following unless and until an official interpretation says otherwise (check off the ones that apply to you):

- where the organization is for profit, all activities involving personal information are likely captured, unless an exception listed below applies

- where the organization is not-for-profit, activities that are commercial in nature, including:
  - selling or bartering personal information about clients or members
  - commercial ventures (e.g., space usage or rental, seminars and conferences, sales, auctions or bazaars, operating a product or gift outlet), listed below:
    - \_\_\_\_\_
    - \_\_\_\_\_
    - \_\_\_\_\_

The following activities are probably exempt from PIPEDA (check off the ones that apply to you):

- information about an employee of the organization (unless the organization is federally regulated, e.g., bank, railway, airline, broadcasting)
- the activities of a federal or a provincial government or their agencies
- information used strictly for personal or household purposes (e.g., your personal phone and address directory so long as they are not also used for work)
- information used strictly for journalistic, artistic or literary purposes (e.g., writing a newspaper article or book about another person).

**(b) Inventory of Personal Information Collected**  
*(See Guide)*

See the Guide for a discussion of the type of information that is considered personal information. If your organization collects personal information in the course of its commercial activities, continue on with the Guide. If your organization does not collect personal information in the course of its commercial activities, you are not covered by the privacy act. Check which of the following applies to you.

- Our organization collects personal information in the course of its commercial activities
- Our organization does not collect personal information in the course of its commercial activities

**Step 3 – Collecting Personal Information**

**(a) Principles of Identifying Purposes and Obtaining Consent**  
*(See Guide)*

See the Guide for a discussion of these principles. You will need to know the difference between a primary purpose and a secondary/related purpose for the use of personal information before completing sections (b) and (c) below.

**(b) Primary Purpose and Consent / Other Legal Authority Checklist**  
*(See Guide)*

PIPEDA applies to the collecting of personal information about any individual, not just clients of the organization. All of these purposes need to be identified. For each category of individuals about whom the organization collects personal information identify the primary purposes for collecting it on the following pages of this checklist. This will require you to think about the real reason why you collect the information in the first place.

**CLIENTS**

*(See examples of primary purposes on Form 3, at the back of the Guide)*

Primary Purpose #1 \_\_\_\_\_

Brief Description of the Purpose \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Primary Purpose #2 \_\_\_\_\_

Brief Description of the Purpose \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Authority to collect information for this purpose (check all that apply):

- Consent
  - Implied consent
  - Verbal consent that will be documented
  - Written consent
- Collection in interests of person and timely consent not possible
- Investigation of breach of law/contract and consent would compromise
- Solely for journalistic, artistic or literary purpose
- Publicly available information specified in regulation

Identify personal information below that is reasonably necessary to achieve the purpose:

PERSONAL CHARACTERISTICS

- Name
- Home contact information
- Identification number (e.g., credit card, social insurance, health, website cookies)
- Insurance benefit coverage
- Gender
- Age
- Colour
- Language
- Ethnic or country of origin
- Education or training
- Marital status, sexual history or sexual orientation
- Income
- Social status
- Other \_\_\_\_\_
- Other \_\_\_\_\_
- Other \_\_\_\_\_
- Other \_\_\_\_\_
- Other \_\_\_\_\_

HEALTH

- Health history
- Health measurements, samples or examination results
- Health conditions, assessment results, diagnoses
- Health services provided to or received by the person
- Health information collected in the course of providing services
- Prognosis or other opinions formed during assessment and treatment
- Compliance with assessment and treatment

- Reasons for discharge and discharge condition and recommendations
- Other \_\_\_\_\_
- Other \_\_\_\_\_
- Other \_\_\_\_\_
- Other \_\_\_\_\_
- Other \_\_\_\_\_

ACTIVITIES AND VIEWS

- Transaction history with the organization
- Occupation/profession
- Opinions expressed by the person
- Community involvements
- Religion
- Work hours
- Criminal History
- Credit or loan data
- Website cookies
- Existence of a dispute with the organization
- Intentions (e.g., to buy goods or services, to change jobs)
- Involvement with organization (e.g., they are a client)
- Letters written to the organization by the person
- Views, evaluations or opinions by organization about the person
- Other \_\_\_\_\_
- Other \_\_\_\_\_
- Other \_\_\_\_\_
- Other \_\_\_\_\_
- Other \_\_\_\_\_

**GENERAL PUBLIC**

*(See examples of primary purposes on Form 3, at the back of the Guide)*

Primary Purpose #1 \_\_\_\_\_

Brief Description of the Purpose \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Primary Purpose #2 \_\_\_\_\_

Brief Description of the Purpose \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Authority to collect information for this purpose (check all that apply):

- Consent
  - Implied consent
  - Verbal consent that will be documented
  - Written consent
- Collection in interests of person and timely consent not possible
- Investigation of breach of law/contract and consent would compromise
- Solely for journalistic, artistic or literary purpose
- Publicly available information specified in regulation

Identify personal information below that is reasonably necessary to achieve the purpose:

PERSONAL CHARACTERISTICS

- Name
- Home contact information
- Identification number (e.g., credit card, social insurance, health, website cookies)
- Insurance benefit coverage
- Gender
- Age
- Colour
- Language
- Ethnic or country of origin
- Education or training
- Marital status, sexual history or sexual orientation
- Income
- Social status
- Other \_\_\_\_\_
- Other \_\_\_\_\_
- Other \_\_\_\_\_
- Other \_\_\_\_\_
- Other \_\_\_\_\_

HEALTH

- Health history
- Health measurements, samples or examination results
- Health conditions, assessment results, diagnoses
- Health services provided to or received by the person
- Health information collected in the course of providing services
- Prognosis or other opinions formed during assessment and treatment
- Compliance with assessment and treatment

- Reasons for discharge and discharge condition and recommendations
- Other \_\_\_\_\_
- Other \_\_\_\_\_
- Other \_\_\_\_\_
- Other \_\_\_\_\_
- Other \_\_\_\_\_

ACTIVITIES AND VIEWS

- Transaction history with the organization
- Occupation/profession
- Opinions expressed by the person
- Community involvements
- Religion
- Work hours
- Criminal History
- Credit or loan data
- Website cookies
- Existence of a dispute with the organization
- Intentions (e.g., to buy goods or services, to change jobs)
- Involvement with organization (e.g., they are a client)
- Letters written to the organization by the person
- Views, evaluations or opinions by organization about the person
- Other \_\_\_\_\_
- Other \_\_\_\_\_
- Other \_\_\_\_\_
- Other \_\_\_\_\_
- Other \_\_\_\_\_

**CONTRACT STAFF**

(Non-employee Staff, Volunteers, Students)

(See examples of primary purposes on Form 3, at the back of the Guide)

PRIMARY PURPOSE #1 \_\_\_\_\_

BRIEF DESCRIPTION OF THE PURPOSE \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

PRIMARY PURPOSE #2 \_\_\_\_\_

BRIEF DESCRIPTION OF THE PURPOSE \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

Authority to collect information for this purpose (check all that apply):

- Consent
  - Implied consent
  - Verbal consent that will be documented
  - Written consent
- 
- Collection in interests of person and timely consent not possible
- Investigation of breach of law/contract and consent would compromise
- Solely for journalistic, artistic or literary purpose
- Publicly available information specified in regulation

Identify personal information below that is reasonably necessary to achieve the purpose:

PERSONAL CHARACTERISTICS

- Name
- Home contact information
- Identification number (e.g., credit card, social insurance, health, website cookies)
- Insurance benefit coverage
- Gender
- Age
- Colour
- Language
- Ethnic or country of origin
- Education or training
- Marital status, sexual history or sexual orientation
- Income
- Social status
- Other \_\_\_\_\_
- Other \_\_\_\_\_
- Other \_\_\_\_\_
- Other \_\_\_\_\_
- Other \_\_\_\_\_

HEALTH

- Health history
- Health measurements, samples or examination results
- Health conditions, assessment results, diagnoses
- Health services provided to or received by the person
- Health information collected in the course of providing services
- Prognosis or other opinions formed during assessment and treatment
- Compliance with assessment and treatment

- Reasons for discharge and discharge condition and recommendations
- Other \_\_\_\_\_
- Other \_\_\_\_\_
- Other \_\_\_\_\_
- Other \_\_\_\_\_
- Other \_\_\_\_\_

ACTIVITIES AND VIEWS

- Transaction history with the organization
- Occupation/profession
- Opinions expressed by the person
- Community involvements
- Religion
- Work hours
- Criminal History
- Credit or loan data
- Website cookies
- Existence of a dispute with the organization
- Intentions (e.g., to buy goods or services, to change jobs)
- Involvement with organization (e.g., they are a client)
- Letters written to the organization by the person
- Views, evaluations or opinions by organization about the person
- Other \_\_\_\_\_
- Other \_\_\_\_\_
- Other \_\_\_\_\_
- Other \_\_\_\_\_
- Other \_\_\_\_\_

**OTHER CATEGORY OF INDIVIDUALS** \_\_\_\_\_

**PRIMARY PURPOSE #1** \_\_\_\_\_

**BRIEF DESCRIPTION OF THE PURPOSE** \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

**PRIMARY PURPOSE #2** \_\_\_\_\_

**BRIEF DESCRIPTION OF THE PURPOSE** \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

Authority to collect information for this purpose (check all that apply):

- Consent
  - Implied consent
  - Verbal consent that will be documented
  - Written consent
- Collection in interests of person and timely consent not possible
- Investigation of breach of law/contract and consent would compromise
- Solely for journalistic, artistic or literary purpose
- Publicly available information specified in regulation

Identify personal information below that is reasonably necessary to achieve the purpose:

PERSONAL CHARACTERISTICS

- Name
- Home contact information
- Identification number (e.g., credit card, social insurance, health, website cookies)
- Insurance benefit coverage
- Gender
- Age
- Colour
- Language
- Ethnic or country of origin
- Education or training
- Marital status, sexual history or sexual orientation
- Income
- Social status
- Other \_\_\_\_\_
- Other \_\_\_\_\_
- Other \_\_\_\_\_
- Other \_\_\_\_\_
- Other \_\_\_\_\_

HEALTH

- Health history
- Health measurements, samples or examination results
- Health conditions, assessment results, diagnoses
- Health services provided to or received by the person
- Health information collected in the course of providing services
- Prognosis or other opinions formed during assessment and treatment
- Compliance with assessment and treatment

- Reasons for discharge and discharge condition and recommendations
- Other \_\_\_\_\_
- Other \_\_\_\_\_
- Other \_\_\_\_\_
- Other \_\_\_\_\_
- Other \_\_\_\_\_

ACTIVITIES AND VIEWS

- Transaction history with the organization
- Occupation/profession
- Opinions expressed by the person
- Community involvements
- Religion
- Work hours
- Criminal History
- Credit or loan data
- Website cookies
- Existence of a dispute with the organization
- Intentions (e.g., to buy goods or services, to change jobs)
- Involvement with organization (e.g., they are a client)
- Letters written to the organization by the person
- Views, evaluations or opinions by organization about the person
- Other \_\_\_\_\_
- Other \_\_\_\_\_
- Other \_\_\_\_\_
- Other \_\_\_\_\_
- Other \_\_\_\_\_

**(c) Related and Secondary Purposes Checklists**

*(See Guide)*

For each related or secondary purpose for which the organization collects personal information, complete a separate checklist below.

The first few samples are pre-completed. These apply to common purposes that recur for many organizations. Make any changes required for your organization. Some of the pre-completed samples (e.g., special offers and promotions) may not apply at all to your organization. These pre-completed sample provisions are followed by some blank forms for you to complete for any other related or secondary purposes your organization might have.

**Related and Secondary Purpose #1: Invoicing and Collection**

**Brief Description:** To invoice clients for goods/services that are not paid for at the time and to collect unpaid accounts.

**Personal Information Collected** (that is not already collected as a part of the primary purpose):

- Home address
- Employer
- Credit check
- Description of service/product provided
- Other:

---

---

---

**Limitations in Collection:** Appropriate only for clients who have not paid at the time of the service or delivery of good or who pay by personal cheque.

**Authority to Collect** information for this purpose:

- Implied consent (rarely appropriate for related or secondary purposes)
- Verbal consent that will be documented
- Written consent
- Collection in interests of person and timely consent not possible
- Investigation of breach of law/contract and consent would compromise (if payment not made)
- Solely for journalistic, artistic or literary purpose
- Publicly available information specified in regulation

**Related and Secondary Purpose #2: Recall Visits**

**Brief Description:** To advise clients that their product or service should be reviewed (e.g., to ensure a product is still functioning properly and appropriate for their then current needs and to consider modifications or replacement).

**Personal Information Collected** (that is not already collected as a part of the primary purpose):

- Home contact information
- Employer
- Other:

---

---

---

**Limitations in Collection:** Appropriate for all clients.

**Authority to Collect** information for this purpose:

- Implied consent (rarely appropriate for related or secondary purposes)
- Verbal consent that will be documented
- Written consent
- Collection in interests of person and timely consent not possible
- Investigation of breach of law/contract and consent would compromise
- Solely for journalistic, artistic or literary purpose
- Publicly available information specified in regulation

**Related and Secondary Purpose #3: Special Events and Opportunities**

**Brief Description:** To advise clients and others of special events and opportunities (e.g., a seminar or conference) that we have available.

**Personal Information Collected** (that is not already collected as a part of the primary purpose):

- Home contact information
- Employer
- Other:

---

---

---

**Limitations in Collection:** Appropriate for all clients and members of the public.

**Authority to Collect** information for this purpose:

- Implied consent (rarely appropriate for related or secondary purposes)
- Verbal consent that will be documented
- Written consent
- Collection in interests of person and timely consent not possible
- Investigation of breach of law/contract and consent would compromise
- Solely for journalistic, artistic or literary purpose
- Publicly available information specified in regulation

#### **Related and Secondary Purpose #4:** Quality Control and Risk Management

**Brief Description:** Our organization reviews client and other files for the purpose of ensuring that we provide high quality services, including assessing the performance of our staff. In addition, external consultants (e.g., auditors, lawyers, practice consultants, voluntary accreditation programs) may on our behalf do audits and continuing quality improvement reviews of our organization, including reviewing client files and interviewing our staff.

**Personal Information Collected** (that is not already collected as a part of the primary purpose): Usually none. In rare cases, our organization or our consultants may make inquiries to verify that the information we have about you is accurate.

**Limitations in Collection:** Appropriate for all categories of individuals from whom we collect personal information.

**Authority to Collect** information for this purpose:

- Implied consent (rarely appropriate for related or secondary purposes)
- Verbal consent that will be documented
- Written consent
- Collection in interests of person and timely consent not possible
- Investigation of breach of law/contract and consent would compromise
- Solely for journalistic, artistic or literary purpose
- Publicly available information specified in regulation

## **Related and Secondary Purpose #5: External Regulation**

**Brief Description:** Our organization, or its professional staff, is regulated by \_\_\_\_\_ who may inspect our records and interview our staff as a part of their regulatory activities in the public interest. In addition, as professionals, we will report serious misconduct, incompetence or incapacity of other practitioners, whether they belong to other organizations or our own. Also, our organization believes that it should report information suggesting serious illegal behaviour to the authorities. External regulators have their own strict privacy obligations. Sometimes these reports include personal information about our clients, or other individuals, to support the concern (e.g., improper services). Also, like all organizations, various government agencies (e.g., Canada Customs and Revenue Agency, Information and Privacy Commissioner, Human Rights Commission, etc.) have the authority to review our files and interview our staff as a part of their mandates. In these circumstances, we may consult with professionals (e.g., lawyers, accountants) who will investigate the matter and report back to us.

**Personal Information Collected** (that is not already collected as a part of the primary purpose): Usually none. In rare cases, our organization or our consultants may make inquiries to verify that the information we have about you is accurate.

**Limitations in Collection:** Appropriate for all categories of individuals from whom we collect personal information.

**Authority to Collect** information for this purpose:

- Implied consent (rarely appropriate for related or secondary purposes)
- Verbal consent that will be documented
- Written consent
- Collection in interests of person and timely consent not possible
- Investigation of breach of law/contract and consent would compromise
- Solely for journalistic, artistic or literary purpose
- Publicly available information specified in regulation

**Related and Secondary Purpose #6: Third Party Billing**

**Brief Description:** The cost of some goods/services provided by the organization to clients is paid for by third parties (e.g., private insurance, government funding). These third party payers often have your consent or legislative authority to direct us to collect and disclose to them certain information in order to demonstrate client entitlement to this funding.

**Personal Information Collected** (that is not already collected as a part of the primary purpose): \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

**Limitations in Collection:** Appropriate only for clients receiving goods/services paid for by third parties.

**Authority to Collect** information for this purpose:

- Implied consent (rarely appropriate for related or secondary purposes)
- Verbal consent that will be documented
- Written consent
- Collection in interests of person and timely consent not possible
- Investigation of breach of law/contract and consent would compromise
- Solely for journalistic, artistic or literary purpose
- Publicly available information specified in regulation

**Related and Secondary Purpose #7: Responding to Questions**

**Brief Description:** Clients or other individuals we deal with may have questions about our goods/services after they have been received. We also provide ongoing services for many of our clients over a period of months or years for which previous records are helpful. We retain our client information for a minimum of ten years after the last contact to enable us to respond to those questions and provide these services. We destroy our information ten years after the last entry (or, where we know, after the individual turns 18) at the first reasonable opportunity in order to reduce the risk of accidental or inadvertent disclosure.

**Personal Information Collected** (that is not already collected as a part of the primary purpose): \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

**Limitations in Collection:** NA. This is a use of information that is already collected.

**Authority to Collect** information for this purpose: NA. This is a use of information that is already collected.

**Related and Secondary Purpose #8: Security Camera**

**Brief Description:** The organization uses a security camera to safeguard its staff and clients, the premises and its records. The images are stored for a period of \_\_\_\_\_ before being destroyed. The information is not used for any other purpose.

**Personal Information Collected** (that is not already collected as a part of the primary purpose): videotaped image of persons visiting the office.

**Limitations in Collection:** only those who visit our office.

**Authority to Collect** information for this purpose:

- Implied consent (through sign in the waiting area)
- Verbal consent that will be documented
- Written consent
- Collection in interests of person and timely consent not possible
- Investigation of breach of law/contract and consent would compromise
- Solely for journalistic, artistic or literary purpose
- Publicly available information specified in regulation

**Related and Secondary Purpose #9: Sale of Business**

**Brief Description:** If the organization or its assets were to be sold, the purchaser would want to conduct a “due diligence” review of the organization’s records to ensure that it is a viable business that has been honestly portrayed to the purchaser. The purchaser would not be able to remove or record personal information. Before being provided access to the files, the purchaser must provide a written promise to keep all personal information confidential. Only reputable purchasers who have already agreed to buy the organization’s business or its assets would be provided access to personal information, and only for the purpose of completing their due diligence search prior to closing the purchase.

**Personal Information Collected** (that is not already collected as a part of the primary purpose). This due diligence may involve some review of our accounting and service files. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

**Limitations in Collection:** NA. This is a use of information that is already collected.

**Authority to Collect** information for this purpose:

- Implied consent (rarely appropriate for related or secondary purposes)
- Verbal consent that will be documented
- Written consent
- Collection in interests of person and timely consent not possible
- Investigation of breach of law/contract and consent would compromise
- Solely for journalistic, artistic or literary purpose
- Publicly available information specified in regulation

**Related and Secondary Purpose #10:** \_\_\_\_\_

**Brief Description:** \_\_\_\_\_

\_\_\_\_\_

**Personal Information Collected** (that is not already collected as a part of the primary purpose): \_\_\_\_\_

\_\_\_\_\_

**Limitations in Collection:** \_\_\_\_\_.

**Authority to Collect** information for this purpose:

- Implied consent (rarely appropriate for related or secondary purposes)
- Verbal consent that will be documented
- Written consent
- Collection in interests of person and timely consent not possible
- Investigation of breach of law/contract and consent would compromise
- Solely for journalistic, artistic or literary purpose
- Publicly available information specified in regulation

**(d) Principles of Use and Disclosure**

See the Guide for a discussion of these principles and then double check that the above information is accurate and complete.

## Step 4 – Safeguards, Retention and Destruction

### (a) Safeguarding Personal Information

(See Guide)

Complete the checklist below. Place a “√” in the box if the organization currently uses the safeguard. Place an “X” in the box if the organization should begin to use the safeguards. It is not necessary to employ every safeguard listed; a selection of safeguards is offered but not all are appropriate for every case. (Indeed, some of the options listed are inconsistent alternatives.) In addition to the generic safeguards described below, special safeguards may be required for extremely sensitive information.

#### Location of Paper Information

- office areas restricted to staff
  - policy that no non-staff permitted without continuous monitoring
  - policy that all files be locked away before non-staff are permitted entry (e.g., after hours)
  - policy that all non-staff who require access (e.g., cleaners) must sign confidentiality agreements
  - other: \_\_\_\_\_
- office areas open to non-staff
  - policy that area be supervised at all times
  - policy that all files containing personal information be locked away when staff are not present (e.g., after hours)
  - other: \_\_\_\_\_
- while in transit to another location
  - policy that in personal custody of staff at all times during transit
  - policy that must be locked away out of sight while unattended (e.g., trunk of car, locked room or filing cabinet when information taken home)
  - other: \_\_\_\_\_
- home office
  - policy that must be locked away in a desk, filing cabinet or separate room while unattended and that no other person has a key
  - other: \_\_\_\_\_

#### Location of Electronic Information

- office areas restricted to staff
  - policy that no non-staff permitted without continuous monitoring
  - for larger organizations, use security badges and sign in sheets
  - policy that all non-staff who require access (e.g., cleaners) must sign confidentiality agreements
  - password protection for each terminal
  - password protection for screen saver on each terminal

- for more sophisticated networks, unique user identifiers, audit trails, and intrusion detection systems
- for wireless networks, consult an expert for appropriate safeguards for your context
- other: \_\_\_\_\_
- office areas open to non-staff
  - policy that area be supervised at all times
  - policy that no personal information can be left on screen when staff leave terminal
  - password protection for each terminal
  - password protection for screen saver on each terminal
  - other: \_\_\_\_\_
- while portable computer in transit to another location
  - policy that in personal custody of staff at all times during transit
  - policy that must be locked away out of sight while unattended (e.g., trunk of car, locked room or filing cabinet when information taken home)
  - password protection for portable computer
  - other: \_\_\_\_\_
- cell phones
  - use digital cell phones only, as those conversations are more difficult to intercept
  - do not use identifying information in cell phone conversations
  - other: \_\_\_\_\_
- home office
  - policy that must be locked away in a desk, filing cabinet or separate room while unattended and that no other person has a key
  - password protection for portable computer
  - other: \_\_\_\_\_

#### Transfer of Paper Information

- in sealed envelope, marked private and confidential, sent by Canada Post or reputable courier
- in sealed envelope, marked private and confidential, delivered by staff
- in sealed envelope to be picked up by person who asks for it by name of recipient (files kept out of sight in reception area until picked up)
- other: \_\_\_\_\_

#### Transfer of Electronic Information

- through a direct line that is password protected
- through email or other internet communication in one of the following circumstances:
  - with the consent of the person to whom the personal information relates (e.g., the client requests email communication)
  - where the message is anonymized

- encryption is used
- through fax with a cover sheet identifying the recipient with privacy clause on it and one of the following safeguards:
  - the fax number has been approved by the recipient
  - the recipient has advised that the fax machine is securely located and there is no basis to doubt the assurance
  - in the context the privacy of the recipient of the fax can reasonably be inferred (e.g., it is to an organization that is expected to keep information private like a legal, accounting or health care office)
  - the recipient has a Privacy Policy
  - your incoming fax machine is securely located
- through a disk, CD or other storage medium that is treated with the same safeguards as a transfer of paper information
- website use of personal information is:
  - encrypted
  - appropriate website cookies policy
  - Other: \_\_\_\_\_
- other: \_\_\_\_\_

#### General Safeguards

- staff (including temporary workers) are trained in the following:
  - the importance of the privacy of personal information
  - access to personal information within the organization is on a need-to-know basis
  - the organization's Privacy Policy on information handling, including obtaining consent before collecting, only using information for the purpose for which the consent was provided, the organization's safeguards, access and correction rights, the complaints process and the name of the Information Officer for the organization
  - sensitivity in collecting or using personal information verbally where others might overhear
  - when providing copies of personal information internally or externally, to remove or mask unnecessary personal information
  - to recognize and avoid being "pumped" for information
  - to ensure that any personal information is not accidentally discarded in the regular garbage or blue box disposal system, but rather is shredded
  - to avoid discussing personal information in public places (e.g., elevators, restaurants, washrooms, public transit)
  - that a breach of the organization's policies will result in discipline up to and including dismissal
- regular (at least annual) review and updating of staff through a continuing education program
- privacy and security agreements with the following consultants and outsourced providers
  - temporary workers

- cleaners
- information technology
- marketers
- legal
- bookkeeping and accounting
- file storage
- credit card companies
- website manager
- office security
- building maintenance
- landlord
- other: \_\_\_\_\_
- other: \_\_\_\_\_
- other: \_\_\_\_\_
- regular and systematic monitoring of compliance with the organization's policies by the Information Officer or his or her delegate (which should be documented)
- regular reminders to staff to change their passwords
- regular and systematic auditing of the electronic safeguards by an external company (which should be documented)
- a policy to notify individuals where their personal information is misused or misappropriated
- review physical layout and procedures appropriate to the context (e.g., use rooms rather than cubicles or curtains for sensitive interviews, keep people in the waiting room for as short a time as possible, security system)
- other: \_\_\_\_\_

**(b) Retention and Destruction of Personal Information**

*(See Guide)*

Retention Policy for Client Files (from last use):

- minimum retention period: \_\_\_\_\_  
(working notes and unnecessary copies can be destroyed earlier so long as the main record containing the information is retained)
- maximum retention period: \_\_\_\_\_

Retention Policy for General Correspondence (not related to a specific client) Newsletters, Seminars and Marketing Activities (from last use):

- minimum retention period: \_\_\_\_\_  
(working notes and unnecessary copies can be destroyed earlier so long as the main record containing the information is retained)
- maximum retention period: \_\_\_\_\_

Retention Policy for Client and Contact Directories:

- minimum retention period: upon request by client or contact to remove information, or \_\_\_\_\_  
(working notes and unnecessary copies can be destroyed earlier so long as the main record containing the information is retained)
- maximum retention period: indefinitely (impractical to regularly and systematically replace information, especially since most of the information is often business contact information)

Retention Policy for \_\_\_\_\_ Files:

- minimum retention period: \_\_\_\_\_  
(working notes and unnecessary copies can be destroyed earlier so long as the main record containing the information is retained)
- maximum retention period: \_\_\_\_\_

Retention Policy for \_\_\_\_\_ Files:

- minimum retention period: \_\_\_\_\_  
(working notes and unnecessary copies can be destroyed earlier so long as the main record containing the information is retained)
- maximum retention period: \_\_\_\_\_

Destruction of personal information

- shredding (paper files)
- deletion (electronic records where hard drive or storage vehicle is retained)
- physical destruction (where hard drive or storage vehicle for electronic information is being discarded)
- return all or part of the file to client
- other: \_\_\_\_\_

## **Step 5 – Access, Correction, Complaints and Openness**

### **(a) Access Rights** *(See Guide)*

Complete the checklist below. Place a “✓” in the box if the organization currently follows the access requirement. Place an “X” in the box if the organization needs to make a change in the area.

- staff know where to refer a request or inquiry for access if they are not able to answer it themselves
- the organization provides access upon request within 30 days unless a ground of refusal exists
  - the organization provides access to not just the personal information held, but also to how the organization has used and disclosed it (thus, reasonable records should be kept)
    - the organization keeps reasonable records of any unusual uses or disclosure of personal information (e.g., systematically filing a cover letter, fax sheet or email in the relevant file)
- the organization either charges no fee or has a fee schedule of minimal fees to handle such a request
- the organization's grounds for refusing an access request are consistent with those mentioned above
  - the organization provides reasons for any refusal of a request and describes any recourse that is available
- the organization confirms the identity of the individual requesting the information before disclosing it
- the organization takes reasonable and necessary steps to ensure that the individual requesting it can understand the information (e.g., explain short forms or codes, provide it in an alternative format where the requester has a sensory disability)

### **(b) Correction Requests**

*(See Guide)*

Complete the checklist below. Place a “✓” in the box if the organization currently follows the correction requirement. Place an “X” in the box if the organization needs to make a change in the area.

- the organization has a process for handling correction requests that is fair to the individual, the organization (e.g., where the request relates to an expression of opinion by the organization) and the person making the entry (e.g., consulting with the person making the entry)
- corrections are made without obliterating the original entry or, failing that, a notice of the disagreement is filed with the record
- corrections or notice of the disagreement are sent to third parties who have received the erroneous information unless doing so is not appropriate
- the individual is given a timely response to a request to correct, along with reasons for any refusal to do so and notice of any recourse

**(c) Complaints System**  
(See Guide)

Complete the following checklist for your organization's complaints system:

- the designated individual to receive complaints is:
  - the Information Officer
  - other: \_\_\_\_\_
- the designated individual to investigate complaints is:
  - the Information Officer
  - the individual designated by the Information Officer to investigate that particular complaint
  - other: \_\_\_\_\_
- the designated individual to decide the complaint is:
  - the Information Officer
  - the individual designated by the Information Officer to investigate that particular complaint
  - the CEO/President/Senior Partner of the organization
  - other: \_\_\_\_\_
- the individual who decides the complaint has the authority to do the following:
  - to ensure compliance with the organization's policies in respect of the complaint
  - to change the organization's information handling policies (after consultation with other leaders of the organization)
  - to award a refund, credit or financial compensation to the individual (after consultation with other leaders of the organization)
  - other: \_\_\_\_\_
- external bodies that a complainant can go to for recourse are as follows:
  - the following regulatory body(ies) for the organization or members of the organization: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_
  - the federal Information and Privacy Commissioner
  - other: \_\_\_\_\_

**(d) Openness**  
(See Guide)

Complete the following checklist to select the ways that would be appropriate for your organization to make its Privacy Policy available to the public (again, it is not necessary to use each of these measures):

- staff are trained to provide the Privacy Policy document to anyone who requests it
- the Privacy Policy document will be posted in the reception area(s) of our organization
- the Privacy Policy document will be posted on our organization's website
- the Privacy Policy document will be sent to our ongoing clients
- the Privacy Policy document will be provided to each new client at the time the consent form is signed
- a brochure summarizing the Privacy Policy document will be sent to our ongoing clients
- a brochure summarizing the Privacy Policy document is provided to each new client at the time the consent form is signed
- other: \_\_\_\_\_

**Step 6 – Implementing Your Privacy Plan**

It is now time to prepare your organization's Consent Form and Privacy Policy. Use the samples found at the end of the Guide to assist you. The information needed to complete these documents should be found in the above checklists.

Once this is done, use the following checklist to track the implementation of your organization's privacy plan.

Initial

- Consent form (Form 1) prepared
- Privacy Policy document (Form 2) prepared
- Initial staff training completed
- Contracts with external consultants and outsourcing providers completed and returned with signatures
- Privacy Policy document posted publicly

Ongoing

- Monitoring compliance with Privacy Policy document (prepare a report annually) is scheduled
- External information technology audit (annual) is scheduled
- Refresher training session for all staff (annual) is scheduled
- Review and update of Privacy Policy document (annual) is scheduled