

Protecting Personal Information

A Workbook for Non-Profit Organizations

Discussion Draft, March 2010



**Government
of Alberta** ■

The Office of the Information and Privacy Commissioner of Alberta and Access and Privacy, Service Alberta, have published other resources to help organizations and individuals understand their rights and obligations under the *Personal Information Protection Act*. These resources are available on their respective websites:

www.oipc.ab.ca and pipa.alberta.ca.

The *Personal Information Protection Act* and regulation are available for purchase from the Alberta Queen's Printer at www.qp.alberta.ca or call 780-427-4952 (toll free: dial 310-0000 first). Links to the Act and regulation can be found on the legislation page at pipa.alberta.ca.

This Workbook was prepared to help organizations to interpret the *Personal Information Protection Act*. This document is an administrative tool intended to assist in understanding the Act. It is not intended as, nor is it a substitute for, legal advice. For the exact wording and interpretation of the Act, please read the Act in its entirety.

This document is not binding on the Office of the Information and Privacy Commissioner of Alberta.

Discussion Draft
March 2010

For more information contact:

PIPA Information Line, Service Alberta

Email: pspinfo@gov.ab.ca

Phone: 780-644-PIPA (7472) (Toll free: dial 310-0000 first)

Message for Directors and Officers Leading Non-Profit Organizations

In Alberta, more than 19,000 non-profit organizations play an important role in the lives of the province's citizens. Thousands of Albertans interact with non-profit organizations in many ways, receiving services from some, being a member of others, and volunteering as well. Many activities of non-profit organizations involve collecting personal information about volunteers, employees, members and clients.

Albertans are increasingly concerned about privacy and are well informed. They expect to have a say in how personal information about themselves and their family members is used, and the circumstances under which it is disclosed. They are concerned about identity theft and privacy breaches. They want accountability when they feel their personal information has been handled carelessly.

Sound privacy practices are often promoted to businesses as providing an edge over the competition. But all organizations benefit from the positive image, and enhanced loyalty from members, clients and employees, when good practices protect personal information. This workbook outlines best practices that non-profit organizations can follow to protect personal information. The workbook is based on Alberta's privacy legislation. Where a practice is required under the legislation, this is noted in the text for those organizations that are currently subject to the legislation.

Alberta's *Personal Information Protection Act* (PIPA) applies to many non-profits only when they are engaged in a commercial activity. If a non-profit organization is incorporated under the *Societies Act* or the *Agricultural Societies Act*, or is registered under Part 9 of the *Companies Act*, PIPA applies only to personal information involved in commercial activities.

This workbook has been developed to assist leaders in non-profit organizations in implementing best practices to protect personal information. The workbook has been developed with smaller organizations in mind. It also provides an excellent starting point for larger organizations, as well as a good review for those non-profit organizations that are fully subject to PIPA.

Protecting personal information – it makes good sense!

Contents

Getting Started.....	1
1. Know your status	2
2. Know what you have.....	3
3. Know why you have it	4
4. Choose a privacy contact person	8
5. Get consent	9
6. Employees and volunteers	13
7. Safeguard personal information	14
Access Requests	17
Other Privacy Acts	18
Understanding the Language of Privacy	19
Sample Privacy Policy.....	20
Sample Privacy Statement	25
Other Resources.....	26

Getting Started

This workbook will guide you through the process of documenting the personal information your organization collects and the purposes for collecting it. The workbook will assist you in adding appropriate notice and consent statements to your organization's forms. You will also find information on an individual's right to access his or her personal information from organizations that are subject to PIPA and information on other useful resources.

For brevity, in this workbook the term "staff" will be used to mean paid employees and volunteers. The term "client" will be used to refer to clients, customers and donors, as well as members, of the non-profit organization.

The workbook outlines requirements for non-profit organizations that are required to comply with PIPA. It also includes best practices that organizations may voluntarily decide to follow to protect the personal information of staff and clients.

After completing this workbook you should be able to write a consent statement and notice for the forms your organization uses to collect personal information. You should also be able to draft a privacy policy or privacy statement that covers the personal information of clients and staff. You will have assessed your organization's practices for keeping information safe and know how to improve protection of personal information.

1. Know your status

The majority of non-profit organizations in Alberta are not required to comply with PIPA. It is important to know whether your organization is subject to the Act. If your organization is subject to the Act, then it must comply with PIPA when collecting, using, disclosing, and safeguarding personal information. It must also respond to requests from individuals to access records containing personal information about them, and do this within the time frames set out in the Act.

If your organization is not required to comply with the Act, you may nevertheless choose to adopt certain best practices to protect the personal information in your care.



Worksheet 1

Is your organization subject to PIPA?

1. Is your organization
 - incorporated under Alberta's *Societies Act*,
 - incorporated under Alberta's *Agricultural Societies Act*, or
 - registered under Part 9 of Alberta's *Companies Act*?

☐ YES. Go to question 2.

☐ NO. Your organization is fully subject to PIPA. (Go to next page.)
2. Does your organization
 - operate a private school (as defined by the *School Act*),
 - operate an early childhood services program (as defined by the *School Act*), or
 - operate a private college (as defined by the *Post-secondary Learning Act*)?

☐ YES. Your organization is subject to PIPA for the collection, use and disclosure of personal information for that operation.

☐ NO. Go to question 3.
3. Does your organization sell, barter or lease a membership list, donor list, or other fund-raising or client, volunteer or employee list?
- ☐ YES. Your organization is subject to PIPA for the collection, use and disclosure of personal information on that list.

☐ NO. Go to question 4.
4. Does your organization engage in any other "commercial activity"? For example, are you operating a day care centre or a fitness centre, or offering training or selling products for fees like those charged by the for-profit sector?
- ☐ YES. Your organization is subject to PIPA for the collection, use and disclosure of the personal information connected to the commercial activity.

☐ NO. Your organization is not subject to PIPA. Your organization may choose to adopt best practices to protect the personal information of your clients and staff.

2. Know what you have

The next step is to determine what kind of personal information your organization normally collects. All organizations should know the kind of personal information they collect.

Personal information is information about a particular individual. Name, contact information, birth date, work history and identification numbers are all examples of personal information.

Use the box below to create a list of the personal information your organization collects about employees, volunteers and clients.



Worksheet 2

Personal information list

- ☐ Name
- ☐ Contact information
- ☐ Birth date, age
- ☐ Credit card information
- ☐ Past work experience
- ☐ Criminal background check
- ☐ Social Insurance Number
- ☐ Driving record
- ☐ Contact information for referees
- ☐ Contact information for a parent/spouse to be used in an emergency
- ☐ Provincial health care number
- ☐ Medical information
- ☐ Driver's licence number
- ☐ Other: _____
- ☐ Other: _____



Some of the personal information listed above is sensitive information, which could be used by criminals to commit identity theft. Particular care should be given to ensure the security of this information. Security measures are discussed later on in the workbook. The best security measure of all is not to collect the information if you do not need it.



When completing steps 2 and 3, refer to the forms your organization used to collect personal information in the first place. The forms will serve as a reminder of the activities carried out by your organization that involve the collection, use and disclosure of personal information.

3. Know why you have it

Under PIPA, organizations may only collect, use and disclose personal information for purposes that are reasonable. In simpler terms, you need a good reason to collect the information. Even organizations not subject to PIPA should have a *good reason* to collect personal information.

Your organization will have a reasonable purpose – or a good reason – for collecting personal information if the organization needs the information for a service or activity. For example, if your organization runs fitness classes, certain personal information is necessary to register the participants and operate the classes.

Use the box below to create a list of your organization's purposes for collecting personal information.



Worksheet 3A

Purposes for collecting personal information

- ☐ Maintaining a membership list to administer membership benefits
- ☐ Mailing a newsletter
- ☐ Registering a participant
- ☐ Processing payment for a product or service
- ☐ Providing a receipt for a payment or donation
- ☐ Assessing or evaluating qualifications of potential staff
- ☐ Assigning duties to staff
- ☐ Determining eligibility for insurance coverage (vehicle, liability, bonding)
- ☐ Contacting a family member in case of an emergency
- ☐ Ensuring the health and safety of participants (e.g. collecting medical information, such as information about allergies, for children attending a camp)
- ☐ Deducting income tax and making other payroll deductions (for paid employees)
- ☐ Other: _____
- ☐ Other: _____
- ☐ Other: _____
- ☐ Other: _____
- ☐ Other: _____
- ☐ Other: _____
- ☐ Other: _____
- ☐ Other: _____

Now that you know what personal information you collect, and the purposes for collecting personal information, you should look at whether the information and purposes match each other.

If your organization collects personal information for several programs, it might be easiest to match the information to each program. Here is an example from a community league that runs a sports league for children, and runs a raffle for fundraising.

Activity	Personal information (Describe information)	Purpose (List why you need it)
Registering participants, administering teams	Name of child Name of parent/guardian Contact information	Creating team lists, contact lists for coaches
	Birth date of child	Placing a child on an age-appropriate team
Fundraising (raffle)	Name Telephone number Address	Contacting the winners



Worksheet 3B

Match it up

Activity	Personal Information (Describe information)	Purpose (List why you need it)

Is there any personal information that you collect where you could not identify a good reason for collecting it? If you cannot link the information to a purpose, consider whether you should be collecting it. PIPA requires organizations to collect only what they reasonably need.

If you have determined that you do not really need the information, what do you do? Stop collecting it. Change your forms so you're not asking for the information, or cross out that section of the form until the form is revised.

You may also want to remove unnecessary information from current files. This is especially important if the information is sensitive (e.g. Social Insurance Numbers, medical information). Most organizations clean up their files periodically and it is acceptable to plan to remove unnecessary information during the periodic clean-ups.

Before you get rid of the personal information, make sure you have proper processes for securely destroying the information: shred paper files (use a cross-cut shredder) and permanently delete electronic files. The section of this workbook on safeguards will make some suggestions for destroying records.



Worksheet 3C

List the "leftovers"

Activity	Personal Information (Describe information)	Action Plan
		<input type="checkbox"/> Delete from form <input type="checkbox"/> Delete from current file
		<input type="checkbox"/> Delete from form <input type="checkbox"/> Delete from current file
		<input type="checkbox"/> Delete from form <input type="checkbox"/> Delete from current file
		<input type="checkbox"/> Delete from form <input type="checkbox"/> Delete from current file
		<input type="checkbox"/> Delete from form <input type="checkbox"/> Delete from current file

Organizations subject to PIPA can keep personal information for as long as the information is needed for legal or business purposes. Personal information that your organization no longer needs (e.g. contact information for former clients or staff) must be securely destroyed after a reasonable amount of time – one year is a good guideline, but you might have legal reasons for keeping certain information (such as financial or tax records) for a longer time. Disposing of information that is no longer needed is a good practice for any organization.

How will your organization determine when to get rid of personal information that is no longer needed? One way is to have a dedicated spot – file cabinet for paper files, or a specific place on your hard drive or network – for "inactive" information to go. Date the file according to when you "shelved" it. If the information remains inactive (e.g. for a year), then destroy it using your safe-destruction processes. Set a schedule for reviewing the inactive file for "past due" dates.



Worksheet 3D

Plan to dispose of the “leftovers”

“Inactive” File	Action Plan
File location/name (e.g. “Old members” - paper file)	Review date: _____ Destroy after ____ months (e.g. 12, 18) Destruction method: _____
File location/name	Review date: _____ Destroy after ____ months Destruction method: _____
File location/name	Review date: _____ Destroy after ____ months Destruction method: _____
File location/name	Review date: _____ Destroy after ____ months Destruction method: _____
File location/name	Review date: _____ Destroy after ____ months Destruction method: _____
File location/name	Review date: _____ Destroy after ____ months Destruction method: _____
File location/name	Review date: _____ Destroy after ____ months Destruction method: _____
File location/name	Review date: _____ Destroy after ____ months Destruction method: _____

4. Choose a privacy contact person

When an organization subject to PIPA collects personal information from an individual, the organization must provide a contact person to whom questions can be directed about the collection. An organization that is not subject to PIPA should consider having a privacy contact person as a best practice.

In a small organization, it may be easiest to make one person responsible for receiving questions about the personal information your organization collects.

The “privacy contact person” can be a paid employee, a volunteer or a board member. Many individuals have some experience with privacy issues, through their roles as employees, customers, or as parents interacting with the school system. The contact person needs to have a basic understanding of the organization’s privacy practices in order to respond appropriately to questions from the public.

Also, employees and volunteers should know who the privacy contact person is, so that they can direct questions to that person.

Most organizations assign the privacy contact duties to a particular position in their organization (e.g. CEO, board secretary, office manager) rather than naming a particular person. If you do this, you do not have to update your privacy contact information whenever you have a change in personnel.



Worksheet 4 Our privacy contact

Privacy contact person for _____ [insert name of your organization]

Position title _____

Phone _____

Fax [optional] _____

Email [optional] _____



The phone number can be a home, business or cell number; callers should be able to leave a message if the phone is not answered.

5. Get consent

Organizations subject to PIPA need consent to collect, use and disclose personal information about clients, unless the Act says otherwise. The consent process for these organizations is explained below. The use of consent by organizations not subject to PIPA is discussed on page 10. Consent is not normally required when dealing with the personal information of employees and volunteers; this is discussed on page 13.

Organizations subject to PIPA

When obtaining consent under PIPA, you must notify your clients of the information you collect, and how you use it. You must also give your clients the name and contact information of your privacy contact person in case they have questions. This notice can be included on a membership application or registration form, or may be given orally.

Obtaining express consent is the highest standard. You may obtain express consent in writing or orally. If the information is sensitive, it is a good idea to get consent in writing or to make a note that you asked for and received oral consent. Sensitive information includes: Social Insurance Numbers, medical information, financial information, reference checks, and date of birth together with name and address.

Your organization may, at times, collect information for one purpose and want to use it for another purpose later on. If so, you must obtain consent for that other purpose. For example, a sports facility collects an individual's contact information at the time of registration; the facility might want to use that information to promote other unrelated programs. The facility will need to obtain consent for that second purpose.

If your organization wants to disclose personal information outside of the organization for an unrelated purpose, the organization will need consent to do so.

You can often obtain consent for all these different purposes at the same time – when you initially collect the information.

In some situations, it is obvious what information is being collected and why. For example, if a client hands you a credit card to pay for her sports facility membership fee, you do not need to tell her that you are collecting her credit card information to process the payment! In this situation, there is implied consent to use the credit card information for that purpose. When can you rely on implied consent?

You *may* use implied consent if:

- a client voluntarily gives you information, and
- the reason you need the information is obvious, and
- it is reasonable in that situation to volunteer the information



You need to obtain consent for each purpose. Obtaining consent to use personal information for enrolment does not allow you to use the same information for marketing purposes later on – even if it is the same information.

Organizations *not* subject to PIPA

Organizations that are not subject to PIPA do not have to follow the consent rules in PIPA when collecting personal information. It may not be practical for these organizations to follow the same consent process as organizations subject to PIPA. As a best practice, organizations not subject to PIPA may want to provide an explanation or notice to clients of how the organization *normally* uses and discloses the personal information it collects.

An organization considering implementing a consent process should obtain legal advice before doing so. Your organization might need to use or disclose personal information for unexpected purposes, or purposes unrelated to the normal operations of your organization, that were not listed on your consent form or notice.

Organizations subject to PIPA have the benefit of the provisions in PIPA for circumstances where it would be unreasonable or impractical to obtain consent (e.g. when collecting a debt, disclosing information to a government department, notifying others in an emergency, or carrying out an investigation). Organizations not subject to PIPA cannot rely on these provisions; for this reason, there may be situations where obtaining consent would be problematic.

At the same time, there may be situations where it could be appropriate to obtain consent, particularly when the disclosure of personal information is for a discretionary purpose, that is, not necessary for the program or service for which the information was collected. For example, an organization may wish to disclose the mailing addresses of its team members to a sports retailer that wants to provide a discount coupon to team members in exchange for receiving the mailing addresses for marketing purposes. Because this disclosure is optional, the team organization may wish to obtain written consent to disclose the addresses to the retailer.

Your legal advisor can assist you in determining when your organization should consider obtaining consent and what needs to be included in a consent form.



Worksheet 5A

Forms your organization uses to collect personal information

Notice of the purposes for which an organization collects personal information, and a consent statement, if needed, can be included in the forms the organization uses to collect personal information.

List the forms your organization uses to collect personal information.

- ☐ Membership application
- ☐ Registration form for [specify] _____
- ☐ Other: _____
- ☐ Other: _____
- ☐ Other: _____
- ☐ Other: _____
- ☐ Other: _____



Worksheet 5B

Sample notice and consent statements

A consent form states what information will be collected, sets out the purpose(s) for collecting it, and asks the individual to positively authorize the collection for those specific purposes.

Select the purposes that apply to your organization's activities. Sample wording is provided but should be modified to reflect your organization's way of doing business.

☐ **Maintain the membership list/provide member benefits**

We require the above information to ensure that our membership list is current and to send you information about our programs and services, as well as renewal notices. Membership in our local branch requires membership in the provincial chapter; we will pass on your information to the provincial chapter.

☐ **Register participants for training**

We require the above information for registration and administration of this training session. Information may be used for program evaluation.

☐ **Register individuals in a sports program**

We require the above information to register you/your child in the sports program. The information will be used to place you/your child into the appropriate category and team, to create team contact lists for coaches and participants, and to maintain an emergency contact list for coaches.

☐ **Medical concerns**

The medical information you have provided about your child will be given to the volunteers supervising the children, to assist them in recognizing a medical emergency and to call for necessary assistance.

☐ **Driving record**

The driver's abstract will be provided to our organization's insurance provider in order to provide insurance coverage on the person driving the organization's vehicles.

☐ **Other purposes**

[Add the information for your privacy contact person and obtain a signature]

For further information, contact _____ [Privacy contact person]

I consent to the collection of my/my child's personal information for the purposes stated above.

Signature _____

Name (print) _____

Date _____



A child under the age of 18 can provide consent if he or she understands the nature and consequences of giving consent; otherwise a parent or guardian can provide consent.

Sample notice for sports registration used by a community league

The information collected above will be used to register the participant in the organization's sports league. The information will be used by staff and the coach to assign the participant to a team, to contact parents/guardians concerning the game schedule and changes, and to contact individuals as necessary in the case of an emergency.

For further information, contact our office manager at 780-555-5555 or privacy@league.ca

☐ Please include my name, my child's name and contact information in the team list that will be distributed to other parents.

Sample script used by staff of a community league for accepting registrations over the telephone

The personal information that I will be asking you for will be used to register the participant in the organization's sports league. The information will be used by staff and the coach to assign the participant to a team, to contact parents/guardians concerning the game schedule and changes, and to contact individuals as necessary in the case of an emergency.

[Collect personal information]

If you need any additional information about our privacy policies, you can contact our office manager at 780-555-5555 or privacy@league.ca

For the convenience of parents, the organization compiles a team list that includes the parent's name, your child's name and contact information to distribute to other parents. Would you like your information to be included in the team list? Yes/No

Name of person giving consent _____ Parent/Guardian ☐

Name of staff member _____

Date information collected _____

6. Employees and volunteers

An organization subject to PIPA does not have to obtain consent from employees or volunteers to collect, use or disclose their personal employee information. Notice is enough if the information is related to establishing, managing, or terminating the employment or volunteer relationship. Notice should be given before the information is collected. Giving notice means telling your employees and volunteers what information you collect, use or disclose and why.

Under PIPA, your organization can collect, use or disclose that information without consent, with two conditions:

- the purpose is related to the employees' or volunteers' work (consent is required for other purposes); and
- you tell (provide notice to) your employees or volunteers about the collection, use or disclosure, along with the purposes.

If the information is not reasonably required for employment or volunteer work purposes, the organization must follow the rules in PIPA regarding consent.

An example of an employee notice is provided in the sample privacy policy at the end of the workbook.

An organization that is not subject to PIPA may decide, as a best practice, to give notice of its purposes for collecting, using or disclosing the personal information of employees and volunteers when the organization *needs* to collect, use or disclose that information (i.e. it is not optional). For example, an organization must report certain information of employees to the Canada Revenue Agency, or to the organization's insurance benefit provider. In these circumstances, the notice would inform the employee or volunteer why the personal information was being disclosed and to whom.

In other circumstances, an organization may decide to allow employees and volunteers to choose whether their personal information is collected, used or disclosed for a particular purpose. For example, the organization may give employees a choice about whether to be added to another organization's mailing list or whether to have their photographs posted on the organization's website.



Worksheet 6

Purposes for collecting personal employee information

- ☐ Assessing or evaluating qualifications of potential staff
- ☐ Deducting income tax and making other payroll deductions (for paid employees)
- ☐ Establishing training and development requirements
- ☐ Other: _____
- ☐ Other: _____
- ☐ Other: _____
- ☐ Other: _____
- ☐ Other: _____

7. Safeguard personal information

Organizations subject to PIPA must protect the personal information the organization has about clients and staff by using reasonable safeguards. Organizations not subject to PIPA should also, as a best practice, protect the personal information of their clients and staff.

In determining what safeguards are reasonable for your organization, you will want to consider how sensitive the information is. All personal information should be protected from loss, theft, and inappropriate use or disclosure, but information like credit card numbers, Social Insurance Numbers, Alberta health care numbers, driver's licence numbers and birth dates can be used to cause harm if they are lost or stolen.

Common-sense security practices

- File cabinets should be locked when unattended. Computers should have password protection to limit access to files containing information about staff and clients. More sensitive information will require additional safeguards.
- Limit access to personal information. Only those staff who need access to the information should have a key to the file cabinet or know computer passwords.
- The best safeguard is to not collect or keep more information than you need. For example, if you need to verify a child's age for a program, consider making a note on the registration form stating that the age was verified by viewing a birth certificate (or relevant document) instead of keeping a copy of the certificate on file.



Many of the security tips in the next worksheet will also ensure the security of your organization's business assets and records (e.g. computers and financial accounts).



Worksheet 7

Security practices

- ☐ **We keep records in paper files**
 - ☐ Locked file cabinets and desk drawers protect information in paper files.
 - ☐ Keys are only provided to staff who need access to the files to perform their work.
 - ☐ Paper files are cross-cut shredded (or otherwise destroyed) before being disposed of.



The Edmonton Police Service found thousands of credit and debit card receipts from one retail store in the possession of known criminals. The store had failed to shred or otherwise destroy the receipts before throwing them into the back-alley dumpster. Since the store's point of sale equipment did not truncate – or black out – some of the credit and debit card numbers, the thieves were able to use some of the information to commit fraud (IPC Investigation Report 2006-IR-003).

- ☐ **We keep records in electronic form**
 - ☐ Computers are password-protected.
 - ☐ Staff must log in to access personal information.
 - ☐ Personal information is accessible only to those who need it.
 - ☐ Computers are physically secured (e.g. secured to a desk by a cable lock) and doors are locked.
 - ☐ Firewalls and anti-virus software are kept up-to-date, to protect against invasive malware.
 - ☐ Networks have adequate encryption according to current encryption standards (this will protect personal information, along with any other confidential information of your organization).
- ☐ **We send or receive personal information via fax or email**
 - ☐ Cover sheets are used to instruct a recipient to contact the organization if a fax is received in error.
 - ☐ Frequently used numbers are programmed into the fax machine to avoid dialling errors.
 - ☐ We call in advance of sending a fax containing sensitive information to ensure the intended recipient knows it is coming, and then to confirm the fax was received.
 - ☐ We only use secure email to send or receive personal information, especially when the information is sensitive.

- ☐ **We store personal information on portable media devices (e.g. laptops or flash drives)**
 - ☐ Personal information is stored on portable devices like laptops, flash drives and CDs or DVDs only when necessary; only as much personal information is stored as is necessary for the task.
 - ☐ Portable media devices are password-protected and encrypted according to current encryption standards.
 - ☐ Portable media devices are not left unattended and are securely locked away when not in use.
- ☐ **Our volunteers/employees sometimes take files containing personal information home to work on**
 - ☐ Our policy is to only take home records if necessary and with approval.
 - ☐ Staff must make sure the records are kept locked up and are not accessible to other household members.
- ☐ **Our staff members are aware of their obligation to protect privacy**
 - ☐ Our board members, employees and volunteers receive information about their obligation to protect personal information.
 - ☐ Our board members, employees and volunteers know who our privacy contact is.
- ☐ **We accept credit or debit cards for payment**
 - ☐ Point of sale machines truncate, or black out, part of the credit or debit card numbers on the receipt.
 - ☐ Our copies of credit and debit card receipts are shredded (or otherwise destroyed) when they are no longer needed.
- ☐ **We post membership, team lists, team schedules, etc. on our website**
 - ☐ Consent is obtained to post names, photographs, and other personal information on our website.



One option is to set up a separate password-protected web page for each team, with only coaches and team members having the password.



Safeguarding tips to implement

- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____

Access Requests

Under PIPA, individuals have the right to request access to their own personal information held by your organization. An individual who makes a request is called an applicant. The applicant must make a request in writing, and may ask to see the information or receive a copy of it.

Many organizations that are subject to PIPA never receive a formal request from an individual to obtain access to his or her own personal information. Most requests are handled on a routine basis. Formal requests tend to be made under PIPA when an individual has a dispute with an organization or needs copies of records for another purpose.

An individual cannot use the Act to obtain general records about the organization or about another individual. However, a guardian can request information on behalf of a dependent child or adult, and any person can make a request on behalf of another individual with that individual's consent.

If you are processing a written request under PIPA, talking to the applicant may help you clarify what the applicant wants – this can simplify the process. You can also ask the applicant what programs she has participated in – this can help you know where to look for records.

Under PIPA you may charge an applicant a reasonable fee (e.g. photocopying costs) for access to the requested information. However, you may not charge a fee for an access request made by employees or volunteers for their work-related information. Your organization must respond to an applicant within 45 calendar days of receiving the request. When you respond to a request, you must tell the applicant: whether you have a record of the information, whether you will give access to all or part of the record, and where, when, and how access will be given.

Your organization can, and sometimes must, refuse to give an applicant access to his or her personal information under PIPA. If you refuse access to all or part of the record, you must tell the applicant the reason(s) for refusing access. An individual can also make a request to correct his or her personal information. For more information on responding to an access request, see PIPA Advisory 3 - Access Requests - Responding to a Request, available at www.oipc.ab.ca.

Depending on the nature of your business, an organization may decide, as a best practice, to provide an individual with copies of his or her own personal information without receiving a request under PIPA. This may be important for an individual who needs copies of records about him- or herself to prove eligibility for benefits or admission to a program, or to exercise other rights.

It is important that the organization does not release the personal information of another individual when providing access to records. The organization may want to assign the responsibility for receiving and processing access requests to particular persons (or positions) who are able to review and sever the records before they are released.

It is a good idea to ask that access requests be made in writing and to verify the identity of the individual picking up the records to protect against releasing the records to the wrong person.

Other Privacy Acts

It is common for organizations to work together to offer joint programs. Often each organization will maintain its own records related to its area of the program. However, sometimes organizations will need to share personal information about their clients in order to run the joint program. If your organization needs to share personal information with another organization, you will want to ensure that the other organization handles the information responsibly.

Most organizations in Alberta are subject to privacy legislation:

- most private-sector organizations are subject to PIPA,
- public bodies (government departments, municipalities, schools, etc.) are subject to the *Freedom of Information and Protection of Privacy Act* (the FOIP Act), and
- health care providers are subject to the *Health Information Act* (HIA).

A non-profit organization that works under contract to a public body is not subject to the FOIP Act. The public body remains responsible for complying with the FOIP Act, and will “pass along” its obligation for protecting personal information through the contract. The records held by the non-profit organization under the contract are not subject to PIPA; they remain under the control of the public body. If a privacy complaint is made, the public body is accountable. Any questions on how to protect the personal information should be directed to the public body.

Similarly, a non-profit organization would not be subject to the *Health Information Act* unless named in the HIA as a custodian, or if it has signed an agreement to become an information manager.

Understanding the Language of Privacy

Personal information is information that can be used to identify a particular individual (for example, name, address, phone number) and information about an individual (for example, physical description, educational background).

Business contact information includes an individual's name, position, title, business telephone number, business address, and email address. PIPA allows this information to be disclosed without consent to allow an individual to be contacted as a representative of their organization, for example, as a member of the board.

Commercial activity includes selling, bartering or leasing membership and donor lists, and operating certain private schools, private colleges and pre-schools. It also includes other activities of a commercial nature, which often means providing a service that is offered at a price competitive with the private sector, such as training courses or day care.

Express consent is explicit permission from an individual to collect, use or disclose his personal information for the stated purpose. Express consent may be given orally or in writing.

Opt-in consent is a form of express consent. A common form of opt-in consent is checking a box to indicate that consent is given.

Implied consent is a form of consent given without an express oral or written statement of consent, such as when a person volunteers information to you and the reason you are collecting the information would be obvious to that person. For example, when an individual hands you his credit card, it is obvious that you will use the information stored in the card to process payment for the product or service you are providing.

Notice is given to an individual when you inform him about the information you collect and how it will be used. A notice (or notice statement) under PIPA must say who your privacy contact person is.

Collect, use and disclose: PIPA uses the terms *collecting*, *using* and *disclosing* personal information.

Collecting means gathering, acquiring, recording, photographing or obtaining personal information from any source.

Using personal information means processing or employing information for a particular purpose.

Disclosing information means showing, telling, sending, or giving the personal information to an outside party. Umbrella associations and partners are all outside parties; transferring personal information to any other organization is a disclosure.

Reasonable: PIPA often refers to what is *reasonable*; this means what a reasonable person would think is appropriate in the situation. Typically, the amount of personal information collected must be reasonable for the transaction. It might be *reasonable* to look at a driver's licence to verify an individual's age; it may not be reasonable to take a copy of the licence.

Employees, volunteers: All paid employees, volunteers, interns, and work-experience students are treated in the same manner under PIPA. Organizations often need to collect, use and disclose personal information about these individuals for *work* or *volunteer* work purposes. They can do this without consent if they provide notice. Organizations not subject to PIPA may choose to provide notice.

Sample Privacy Policy:

An organization subject to PIPA

Name of your Organization

Personal Information Protection Policy

Is this for members, clients, customers, volunteers, employees? Choose the words appropriate for your organization.

Include some examples of personal information that your organization collects.

Fill this in with the purposes you identified.

Choose an example that fits your organization. When are your clients likely to volunteer personal information?



You do not need to obtain consent to use personal information collected before the Act applied, but it is a good practice to seek consent when you update that information.

Name of your organization is committed to safeguarding the personal information entrusted to us by our clients. We manage your personal information in accordance with Alberta's *Personal Information Protection Act* and other applicable laws. This policy outlines the principles and practices we follow in protecting your personal information.

This policy applies to Name of your organization and to any person providing services on our behalf. A copy of this policy is provided to any client on request.

What is personal information?

Personal information means information about an identifiable individual. This includes an individual's name, home address and phone number, age, sex, marital or family status, an identifying number, financial information, educational history, etc.

What personal information do we collect?

We collect only the personal information that we need for the purposes of providing services to our clients, including personal information needed to:

- deliver requested products and services
- enrol a client in a program
- send out association membership information

We normally collect client personal information directly from our clients. We may collect your information from other persons with your consent or as authorized by law.

We inform our clients, before or at the time of collecting personal information, of the purposes for which we are collecting the information. The only time we don't provide this notification is when a client volunteers information for an obvious purpose (for example, producing a credit card to pay a membership fee when the information will be used only to process the payment).

Consent

We ask for consent to collect, use or disclose client personal information, except in specific circumstances where collection, use or disclosure without consent is authorized or required by law. We may assume your consent in cases where you volunteer information for an obvious purpose.

We assume your consent to continue to use and, where applicable, disclose personal information that we have already collected, for the purpose for which the information was collected.

Fill in as appropriate for your organization.

Include this paragraph only if you use opt-out consent.

Choose examples relevant to your organization.

List one of your purposes.

Use this section if your organization's policy includes personal employee information.

Fill this in with the purposes you identified.

We ask for your express consent for some purposes and may not be able to provide certain services if you are unwilling to provide consent to the collection, use or disclosure of certain personal information. Where express consent is needed, we will normally ask clients to provide their consent orally (in person, by telephone), or in writing (by signing a consent form).

In cases that do not involve sensitive personal information, we may rely on "opt-out" consent. For example, we may disclose your contact information to other organizations that we believe may be of interest to you, unless you request that we do not disclose your information. You can do this by checking the appropriate box on our application form or by telephoning our local number/toll-free number.

A client may withdraw consent to the use and disclosure of personal information at any time, unless the personal information is necessary for us to fulfil our legal obligations. We will respect your decision, but we may not be able to provide you with certain products and services if we do not have the necessary personal information.

We may collect, use or disclose client personal information without consent only as authorized by law. For example, we may not request consent when the collection, use or disclosure is to determine suitability for an honour or award, or in an emergency that threatens life, health or safety.

How do we use and disclose personal information?

We use and disclose client personal information only for the purpose for which the information was collected, except as authorized by law. For example, we may use client contact information to deliver goods.

If we wish to use or disclose your personal information for any new business purpose, we will ask for your consent. We may not seek consent if the law allows this (e.g. the law allows organizations to use personal information without consent for the purpose of collecting a debt).

What is personal employee information?

Personal employee information is personal information about an employee or volunteer which is collected, used or disclosed solely for the purposes of establishing, managing or terminating an employment relationship or a volunteer work relationship. Personal employee information may, in some circumstances, include a Social Insurance Number, a performance review, etc.

We can collect, use and disclose your personal employee information without your consent only for the purposes of establishing, managing or ending the employment or volunteer relationship. We will provide current employees and volunteers with prior notice about what information we collect, use or disclose and our purpose for doing so.

What personal employee information do we collect, use and disclose?

We collect, use and disclose personal employee information to meet the following purposes:

- Determining eligibility for employment or volunteer work, including verifying qualifications and references
- Establishing training and development requirements

Fill this in as appropriate for your organization.

- Assessing performance and managing performance issues if they arise
- Administering pay and benefits (paid employees only)
- Processing employee work-related claims (e.g. benefits, workers' compensation, insurance claims) (paid employees only)
- Complying with requirements of funding bodies (e.g. lottery grants)
- Complying with applicable laws (e.g. *Canada Income Tax Act*, Alberta Employment Standards Code)

We only collect, use and disclose the amount and type of personal employee information that is reasonable to meet the above purposes. The following is a list of personal employee information that we may collect, use and disclose to meet those purposes.

- Contact information such as your name, home address, telephone number
- Criminal background checks
- Employment or volunteer information such as your resume (including educational background, work history and references), reference information and interview notes, letters of offer and acceptance of employment, policy acknowledgement forms, background verification information, workplace performance evaluations, emergency contacts, etc.
- Benefit information such as forms relating to applications or changes to health and insurance benefits including medical and dental care, life insurance, short and long term disability, etc. (paid employees only)
- Financial information, such as pay cheque deposit information and tax-related information, including Social Insurance Numbers (paid employees only)
- Other personal information required for the purposes of our employment or volunteer relationship

We will inform our employees and volunteers of any new purpose for which we will collect, use, or disclose personal employee information, or we will obtain your consent, before or at the time the information is collected.

Choose an example that fits your organization.

We will obtain your consent to collect, use and disclose your personal information for purposes unrelated to the employment or volunteer relationship (e.g. such as providing you with information about our workplace charity program).

What information do we provide for employment/volunteer references?

In some cases, after your employment or volunteer relationship with us ends, we will be contacted by other organizations and asked to provide a reference for you. It is our policy not to disclose personal information about our employees and volunteers to other organizations who request references without consent. The personal information we normally provide in a reference includes:

- Confirmation that an individual was an employee or volunteer, including the position, and date range of the employment or volunteering
- General information about an individual's job duties and information about the employee or volunteer's ability to perform job duties and success in the employment or volunteer relationship



Remember you will be held to what you say in your policy, so your policy must reflect your actual practices.

Include examples of your practices.

Fill this in with information for your privacy contact person.

How do we safeguard personal information?

We make every reasonable effort to ensure that personal information is accurate and complete. We rely on individuals to notify us if there is a change to their personal information that may affect their relationship with our organization. If you are aware of an error in our information about you, please let us know and we will correct it on request wherever possible. In some cases we may ask for a written request for correction.

We protect personal information in a manner appropriate for the sensitivity of the information. We make every reasonable effort to prevent any loss, misuse, disclosure or modification of personal information, as well as any unauthorized access to personal information.

We use appropriate security measures when destroying personal information, including shredding paper records and permanently deleting electronic records.

We retain personal information only as long as is reasonable to fulfil the purposes for which the information was collected or for legal or business purposes.

Access to records containing personal information

Individuals have a right to access their own personal information in a record that is in the custody or under the control of **Name of organization**, subject to some exceptions. For example, organizations are required under the *Personal Information Protection Act* to refuse to provide access to information that would reveal personal information about another individual.

If we refuse a request in whole or in part, we will provide the reasons for the refusal. In some cases where exceptions to access apply, we may withhold that information and provide you with the remainder of the record.

You may make a request for access to your personal information by writing to **Name or position title of individual in your organization designated to ensure compliance with PIPA**. You must provide sufficient information in your request to allow us to identify the information you are seeking.

You may also request information about our use of your personal information and any disclosure of that information to persons outside our organization. In addition, you may request a correction of an error or omission in your personal information.

We will respond to your request within 45 calendar days, unless an extension is granted. We may charge a reasonable fee to provide information, but not to make a correction. We do not charge fees when the request is for personal employee information. We will advise you of any fees that may apply before beginning to process your request.

Fill this in with information for
your privacy contact person.

Questions and complaints

If you have a question or concern about any collection, use or disclosure of personal information by **Name of organization**, or about a request for access to your own personal information, please contact **Name or position title of individual in your organization designated to ensure compliance with PIPA**.

If you are not satisfied with the response you receive, you should contact the Information and Privacy Commissioner of Alberta:

Office of the Information and Privacy Commissioner of Alberta
Suite 2460, 801 - 6 Avenue, SW
Calgary, Alberta T2P 3W2

Phone: 403-297-2728

Email: generalinfo@oipc.ab.ca

Toll Free: 1-888-878-4044

Website: www.oipc.ab.ca

Sample Privacy Statement: An organization not subject to PIPA

Name of your Organization Personal Information Protection

Is this for members, clients, customers, volunteers, employees? Choose the words appropriate for your organization.

Include some examples of personal information that your organization collects.

Fill this in with the purposes you identified.

Choose an example that fits your organization. When are your clients likely to volunteer personal information?



Remember you will be held to what you say in your policy, so your policy must reflect your actual practices.

Include examples of your practices.

Fill this in with information for your privacy contact person.

Name of your organization is committed to safeguarding the personal information entrusted to us by our clients. This privacy statement outlines the practices we follow in protecting personal information.

This privacy statement applies to Name of your organization and to any person providing services on our behalf. A copy of this privacy statement is provided to any client on request.

What is personal information?

Personal information means information about an identifiable individual. This includes an individual's name, home address and phone number, age, sex, marital or family status, an identifying number, financial information, educational history, etc.

What personal information do we collect?

We collect only the personal information that we need for the purposes of providing services to our clients, including personal information needed to:

- deliver requested products and services
- enrol a client in a program
- send out association membership information

We normally collect client information directly from our clients. We may collect your information from other persons with your consent or as authorized by law.

We inform our clients, before or at the time of collecting personal information, of the purposes for which we are collecting the information. The only time we don't provide this notification is when a client volunteers information for an obvious purpose (for example, producing a credit card to pay a membership fee when the information will be used only to process the payment).

How do we safeguard personal information?

We make every reasonable effort to ensure that personal information is accurate and complete. We rely on individuals to notify us if there is a change to their personal information that may affect their relationship with our organization. If you are aware of an error in our information about you, please let us know and we will correct it on request wherever possible. In some cases we may ask for a written request for correction.

We protect personal information in a manner appropriate for the sensitivity of the information. We make every reasonable effort to prevent any loss, misuse, disclosure or modification of personal information, as well as any unauthorized access to personal information.

We use appropriate security measures when destroying personal information, including shredding paper records and permanently deleting electronic records.

Questions and complaints

If you have a question or concern about any collection, use or disclosure of personal information by Name of organization, or about a request for access to your own personal information, please contact Name or position title of individual to respond to questions.

Other Resources

Access and Privacy, Service Alberta

Website: pipa.alberta.ca

PIPA Information Line, Service Alberta

Email: pspinfo@gov.ab.ca

Phone: 780-644-PIPA (7472) (Toll free dial 310-0000 first)

Selected publications

A Guide for Organizations and Businesses

A Summary for Organizations

Frequently Asked Questions

Information Sheet 1: Non-Profit

Organizations

Information Sheet 2: Investigations

Information Sheet 3: Personal Information

Information Sheet 4: Personal Information

Collected Before 2004

Information Sheet 5: Personal Employee

Information

Information Sheet 7: Personal Information of
Deceased Persons

Information Sheet 8: Collection, Use and
Disclosure of Personal Information for
Archival and Research Purposes

Information Sheet 9: Publicly Available

Information

PIPA on a Page

PIPA Pointers

Office of the Information and Privacy Commissioner

Email: generalinfo@oipc.ab.ca

Phone: 403-297-2728 (Toll free dial 1-888-878-4044)

Website: www.oipc.ab.ca

Selected publications

A PIPA Guide for Organizations: Understanding
the Role of the OIPC

Questions and Answers

Frequently Asked Questions for Minor Sports

Associations

Photo Identification Guidance

SIN Tips

Video Surveillance Guidelines

A Guide for Organizations and Businesses

PIPA Advisory 1 – Consent

PIPA Advisory 2 – Access Requests – An

Overview

PIPA Advisory 3 – Access Requests –
Responding to a Request

PIPA Advisory 5 – Access Requests – Fees

PIPA Advisory 6 – Access Requests – Time

Limits

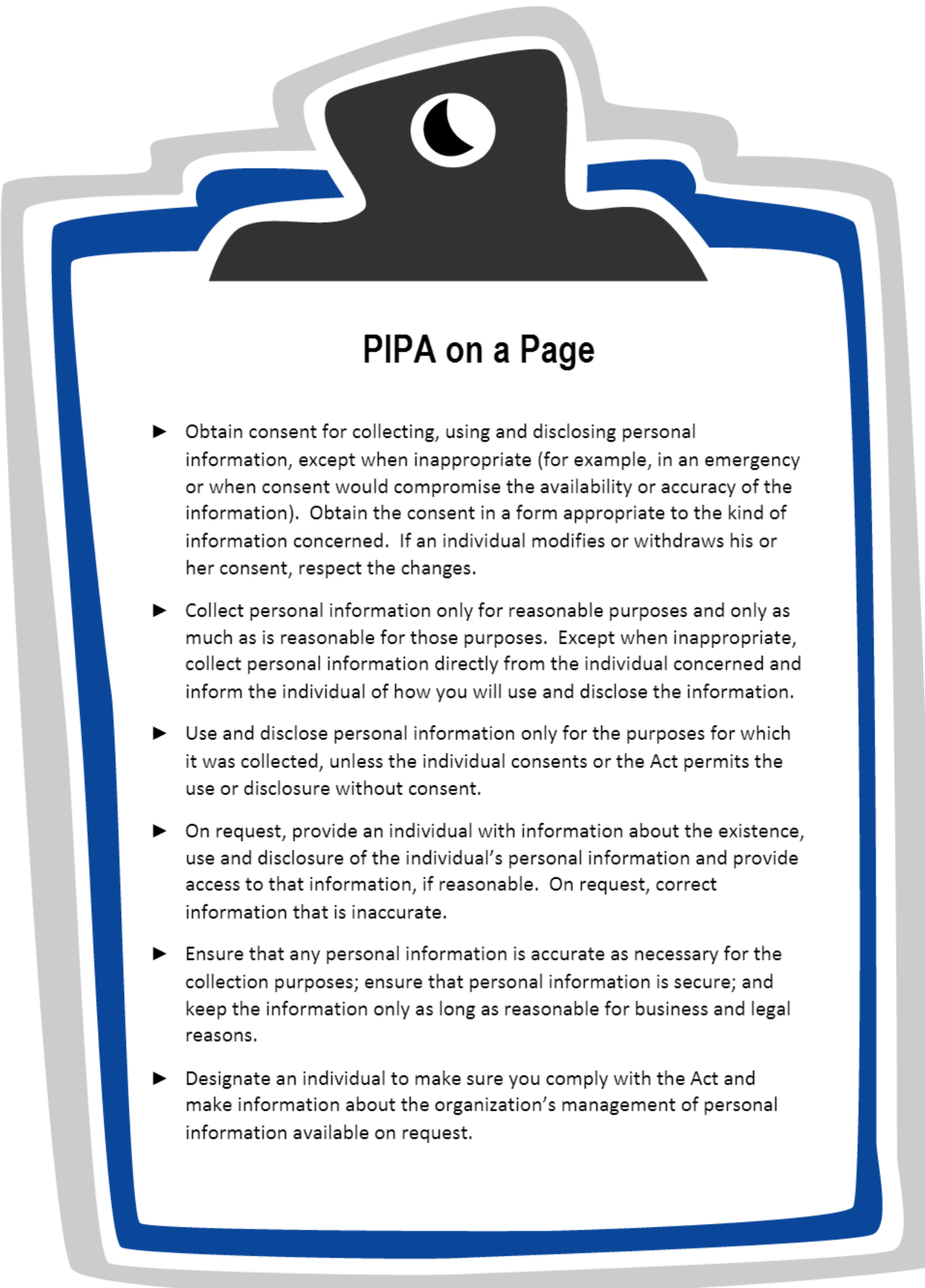
PIPA Advisory 7 – Access Requests – Exceptions
to Access

PIPA Advisory 8 – Reasonable Safeguards

Reporting a Privacy Breach to the OIPC

Key Steps in Responding to Privacy Breaches

Notes



PIPA on a Page

- ▶ Obtain consent for collecting, using and disclosing personal information, except when inappropriate (for example, in an emergency or when consent would compromise the availability or accuracy of the information). Obtain the consent in a form appropriate to the kind of information concerned. If an individual modifies or withdraws his or her consent, respect the changes.
- ▶ Collect personal information only for reasonable purposes and only as much as is reasonable for those purposes. Except when inappropriate, collect personal information directly from the individual concerned and inform the individual of how you will use and disclose the information.
- ▶ Use and disclose personal information only for the purposes for which it was collected, unless the individual consents or the Act permits the use or disclosure without consent.
- ▶ On request, provide an individual with information about the existence, use and disclosure of the individual's personal information and provide access to that information, if reasonable. On request, correct information that is inaccurate.
- ▶ Ensure that any personal information is accurate as necessary for the collection purposes; ensure that personal information is secure; and keep the information only as long as reasonable for business and legal reasons.
- ▶ Designate an individual to make sure you comply with the Act and make information about the organization's management of personal information available on request.