A Guide for Businesses and Organizations to British Columbia's *Personal Information Protection Act*

December 30, 2003
(2nd Publication)

Contents

Why a Guide?

The Office of the Information and Privacy Commissioner for British Columbia (OIPC) has developed this guide to help you understand the *Personal Information Protection Act* (PIPA) overall, but especially the areas you are most likely to run across in your organization's activities.

The guide will not answer every question you might have, but it will give an overview of the most important rules in PIPA and how organizations can operate to comply with those rules. You can find other PIPA implementation tools on the website of the Corporate Privacy and Information Access Branch ("CPIAB") of British Columbia's Ministry of Management Services, noted below. Further information, useful tools and links to other resources can also be found at the OIPC's website, www.oipc.bc.ca.

Some words or phrases in this guide are *in italics*. They are explained either in the paragraph after they are used or in the glossary at the end of the guide. When you are trying to decide if or how PIPA applies, it is important to pay attention to the definitions in PIPA, since those definitions prevail over the glossary definitions.

This document has been prepared based on the guide to Alberta's *Personal Information Protection Act* prepared by the Office of the Information and Privacy Commissioner for Alberta and the Information Management & Privacy Branch of Alberta's Ministry of Government Services. They have generously allowed the OIPC to adapt that guide for British Columbia's *Personal Information Protection Act* and we are grateful to them for their support and collaborative approach to their work.

Contact information:

Office of the Information and Privacy Commissioner

Mailing Address:
PO Box 9038, Stn. Prov. Govt.
Victoria, B.C. V8W 9A4

Web Site: **www.oipc.bc.ca/private/**

E-mail: **info@oipc.bc.ca**

Telephone: (250) 387-5629 For toll-free access, call Enquiry BC at one of the numbers listed below and request a transfer to (250) 387-5629:

Vancouver: (604) 660-2421
Elsewhere in BC: (800) 663-7867

Corporate Privacy and Information Access Branch

Implementation Tools:
www.mser.gov.bc.ca/foi_pop/privacy/default.htm

PIPA Hot Line: (250) 356-1851

For information on PIPA, call the PIPA hotline at (250) 356-1851. For toll-free access, call Enquiry BC as noted to the left.

Legal Notice

Please note that the discussion in this guide of British Columbia's *Personal Information Protection Act* is for general information only. It is not intended to be, and cannot be relied upon as, legal advice or other advice. This document does not bind or fetter the Office of the Information and Privacy Commissioner for British Columbia in interpreting or applying PIPA. Only PIPA's provisions can be regarded as authoritative and PIPA's provisions prevail in all cases.

This guide has been prepared based on a similar guide prepared by the Office of the Information and Privacy Commissioner for Alberta and the Information Management & Privacy Branch of Alberta's Ministry of Government Services. The contents of this document are, however, the sole product and responsibility of the OIPC and neither of the organizations just mentioned bears any responsibility of any kind for this guide.

What does the *Personal Information Protection Act* do?

The *Personal Information Protection Act* (PIPA) describes how all organizations in British Columbia's private sector must handle personal information of customers, employees and others. PIPA comes into effect on January 1, 2004. PIPA creates common-sense rules about collecting, using and disclosing personal information. PIPA's purpose is stated this way in section 2:

> The purpose of this Act is to govern the collection, use and disclosure of personal information by organizations in a manner that recognizes both the right of individuals to protect their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

PIPA also gives individuals the right to access the personal information an organization has about them and to ask for the information to be corrected if they think their personal information is incorrect or incomplete.

Personal information means information that can identify an individual (for example, name, home address, home phone number, ID numbers), and information about an identifiable individual (for example, physical description, educational qualifications, blood type). Personal information includes *employee personal information* but does not include business *contact information* or *work product information*.

PIPA applies to *personal information*. It does not apply to general information used to operate the business of the organization. For PIPA to apply, the personal information in question needs to be about an individual who is "identifiable" directly from that information or is "identifiable" from that information combined with other information that is otherwise available. Non-identifiable or aggregate information such as statistical information about groups of individuals is not personal information.

PIPA allows personal information to be collected, used or disclosed for reasonable purposes. To understand what purposes are reasonable, consider the following examples:

Example

A customer renting a movie from a video store would consider it reasonable to provide a telephone number or an address. But could a video store ask for a social insurance number? That would not be reasonable.

Example

A customer paying cash to buy a battery for his flashlight would not consider it reasonable to be asked for his or her name, address or telephone number unless the purpose for doing so was explained to the customer and it was clear that the customer was not required to provide the information to complete the purchase.

Example

Susan is buying a new truck and applies to the dealer for financing. The dealer can ask Susan to provide personal information to process the loan, and can use and disclose the information as required to process the loan application. However, it would be unreasonable for the dealer to ask for personal information that is either irrelevant to the purchase or for processing the loan application, or to use or disclose the personal information for some other purpose without first obtaining Susan's consent to do so.

What organizations and types of information does PIPA regulate?

Organizations covered by PIPA

PIPA applies to all *organizations* and to all personal information held by organizations unless PIPA says that it does not apply. **[section 4(1)]**

An *organization* includes:

- a corporation
- a partnership
- an individual involved in a commercial activity (for example, an individual running a small renovation business that is not incorporated)
- an association that is not incorporated
- a trade union
- a *non-profit organization*, such as a charity, club, religious organization or amateur sport association
- a trust, except for a private trust for the benefit of friends or family of the individual who sets up the private trust.

Example

An amateur hockey team runs a raffle to buy equipment for the club. Ticket buyers provide their name, address and phone number on the ticket stub. The team later compiles a list of ticket purchasers and wishes to sell it to the local sports equipment store. The rules for collecting, using and disclosing personal information apply here. The team needs the ticket buyers' consent to sell their information to the sports equipment store.

An *organization* does not include a person who is acting in a personal or domestic way – that is, for purposes related solely to family or home activities – or is acting in the capacity of an employee.

Example

In her spare time, Jane Doe, researches her family history in British Columbia. She gathers information about relatives, many of whom live in British Columbia, from various sources. She is not an organization under PIPA, since her collection, use and disclosure of her customers' personal information is for purely personal purposes of genealogical research.

PIPA does not apply to certain public sector organizations

"Public bodies" regulated under the *Freedom of Information and Protection of Privacy Act* (FOIPP Act) are not organizations under PIPA. Public bodies include provincial government ministries, local governments, universities, colleges, public school boards, regional health authorities, hospitals and Crown corporations (other than BC Rail, to which PIPA applies). PIPA also does not apply to the court system or to a member of the Legislative Assembly acting in her or his capacity as a member.

PIPA does not apply to certain kinds of information

PIPA does not apply if you collect, use or disclose personal information:

- for personal, home or family purposes (for example, for Christmas card mailing-lists of family and friends)
- for artistic or literary purposes (for example, if a character in your novel is recognizably a friend of yours)
- for journalistic purposes (this protects freedom of expression for newspapers, but PIPA does apply to a newspaper's employee personal information, subscriber information and its marketing activities.

Example

Guy is writing an article that will be published in a trade journal. He can collect, use and disclose personal information without following PIPA's rules. PIPA does not apply since Guy's writing of the article is a journalistic use.

PIPA also does not apply in the following situations:

- PIPA does not apply to personal information if the FOIPP Act applies to the information. For example, a government ministry may have disclosed personal information to a contractor carrying out work for that ministry, but maintained control over that information through contractual measures. Because the information is still under the ministry's control, the FOIPP Act applies to the information.
- If the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) applies to personal information, PIPA does not apply. For example, personal information held by a federally regulated organization, such as a bank or telephone company, is regulated under PIPEDA, even though the company may be located in BC.
- PIPA does not apply if the information is personal information in court files.

Examples

An accounting firm handles payroll information for a municipality and several private-sector clients. It receives the names of employees, social insurance numbers, hours of work and rates of pay from its clients.

The municipality is covered by the FOIPP Act and maintains control, through contractual measures, over the payroll information it sends to the accounting firm. The FOIPP Act will, therefore, apply to this information. However, PIPA will apply to the payroll information the accounting firm receives from its private-sector clients.

TIP FOR BEST PRACTICE:

When working under contract for a public body, organizations should be clear whether the public body has control of personal information generated or provided under the contract. You should expressly cover this off in the contract.

How does PIPA affect *legal proceedings?*

Parties to legal proceedings have a right to get certain information by law (for example, through testimony in the pre-trial process known as examination for discovery). PIPA does not change that right and does not affect solicitor-client privilege. Lawyers must follow rules and laws about how certain information is handled. While PIPA does not affect those rules or laws, it will apply to how lawyers and law firms handle their clients' and employees' personal information in the course of their practices.

An organization cannot contract out of the PIPA rules

Your organization should not try to contract out of your PIPA responsibilities. Any attempt to contract out – with your customers, employees or others – is not likely to be upheld. A ruling under the FOIPP Act has confirmed that it is not possible to contract out of the similar rules under the FOIPP Act.

When does PIPEDA apply?

Both the federal Act, the *Personal Information Protection and Electronics Documents Act* ("PIPEDA"), and PIPA focus on protecting personal information.

PIPEDA has been in place for federally regulated businesses – such as banks, telephone companies, airlines, shipping companies and railways – since January 1, 2001. On January 1, 2004, PIPEDA will apply to every organization across Canada when collecting, using or disclosing personal information while carrying out a commercial activity within a province, unless a province passes an Act that is "substantially similar" to PIPEDA.

When PIPA comes into force on January 1, 2004, it will apply to provincially regulated businesses, non-profit organizations, trade unions and other organizations in British Columbia. However, PIPEDA will likely still apply to provincially regulated organizations when, in the course of a commercial activity, personal information crosses British Columbia's borders. It will also still apply to federally regulated industries in British Columbia.

It is possible that there will be circumstances where the issue of which legislation applies, PIPEDA or PIPA, will have to be resolved by the courts.

PIPA Guidelines for your organization

1. Be accountable for your information practices

Summary: Your organization's PIPA responsibilities

Your organization is legally responsible for all personal information in your custody or under your control—in other words, even information your contractor is using under its contract with your organization is your responsibility.

PIPA requires your organization to choose an individual to be responsible for compliance with PIPA. You should make the individual's name and contact information publicly available.

PIPA uses the "reasonable person test" for deciding whether an organization has carried out its PIPA responsibilities. The test refers to what a reasonable person would think appropriate in the circumstances.

Bottom Line: Your organization is legally responsible for all the personal information that is either in your *custody* or under your *control*. **[section 4(2)]**

Information Practices

Organizations are accountable for the personal information they collect, use and disclose. They are accountable for personal information in their *custody* or *control*. Organizations have *custody* of personal information when it is in their offices, facilities, file cabinets and computers, and so on.

Personal information is, generally, under the *control* of an organization when the organization can decide how to use or disclose the information, how to store it and how long to keep it. For example, if your business sends electronic information to another business to process or store it for your business, the information is still under your control even though you have sent it to your contractor. You must make sure that the other business protects it the same way that you must do. In other words, your organization must use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

Your organization must designate one or more individuals to make sure that your organization follows PIPA's rules. The designated individual can be called your "privacy officer". This individual may also be the contact person for answering questions about PIPA and for handling access requests and complaints under PIPA. Other individuals in your organization may be delegated to act in the place of the appointed individual.

Policies and Procedures

Your organization will need to develop, and put into practice, policies and procedures to protect personal information. In general, this should include:

- implementing procedures to protect personal information;
- establishing procedures to receive and respond to complaints and inquiries;
- training staff and communicating to staff information about the organization's policies and practices; and
- developing information to explain the organization's policies and procedures.

In particular, the policies and procedures should cover:

- what information you collect.
- why you collect personal information.
- how you obtain consent for collecting, using and disclosing personal information.
- what the limits are on your collecting, using and disclosing personal information.
- how you ensure that the personal information is correct, complete and current.
- how you ensure that adequate security measures are in place.
- how to develop or update a timetable for keeping or destroying information.
- how you process access requests.
- how you respond to inquiries and complaints.

To be accountable, your organization must do what a reasonable person would do in each particular situation. This means you should review your personal information-handling practices for both ongoing and new activities, and doing so on an ongoing basis in the future.

Identifying the purpose for which you are collecting personal information

In developing your organization's policies and procedures, it is important for you to identify the purposes for which your organization is collecting personal information. This will allow your organization to determine, as the policies and procedures are being developed, what information it needs to collect to fulfil its business purposes and to ensure that personal information is collected only for the purposes that have been identified.

In developing your organization's policies and procedures, and identifying the personal information you collect and why, you should remember the following general rules (bearing in mind that PIPA provides some exceptions as described elsewhere in this guide):

- you must limit the collection of personal information to that is which necessary for the purposes you identify;
- you can only collect, use or disclose personal information if it is reasonable having regard to the sensitivity of the personal information in the circumstances;
- you cannot require someone to consent to collection, use or disclosure of personal information beyond what is necessary to provide them with a product or service; and
- personal information should be collected by fair and lawful means.

These principles are the bedrock of good information practices and of compliance with PIPA.

You can use the following questions to help assess whether and ensure that your information practices comply with PIPA:

1. What personal information do we collect?

2. For what purposes do we collect it?

3. Do we collect only personal information that we really need for our purposes?

4. How do we collect it?

5. What do we use it for and are those uses reasonable and appropriate?

6. Where do we keep it and how is it secured?

7. Who, within the organization, has access to the information or uses it, and for what purposes? Are we limiting access on a real need-to-know basis?

8. Who is it disclosed to outside our organization and why? Should we be disclosing this information to these others for the purposes we now disclose it?

9. How long do we retain the personal information? When is it disposed of and how? Is it disposed of securely?

10. In light of PIPA, should we change any of these practices?

Complaint-handling procedures

An important aspect of accountability, and a PIPA requirement, is that you must have procedures in place to receive and respond to complaints or inquiries about your organization's policies and practices relating to the handling of personal information. The complaint procedures should be easily accessible and simple to use and your organization should inform individuals who make inquiries or lodge complaints of the existence of your complaint procedures. Finally, your organization should investigate all complaints and, if you find that a complaint is justified, should take appropriate measures in response (including, if necessary, amending your organization's policies and practices).

For guidance on how to develop fair and effective complaint handing procedures you can consult the model dispute process found on the OIPC's website, at http://www.oipc.bc.ca/advice/GUID-Complaint_Investigation.pdf. This tool was developed for public sector use, but may assist you in developing your own tool. You can also refer to the dispute process tool on CPIAB's website: http://www.mser.gov.bc.ca/foi_pop/privacy/default.htm. Last, although written for the public sector, the Office of the Ombudsman's Public Report No. 49, "Developing an Internal Complaint Mechanism", may also be of assistance. It is located at the Ombudsman's web site under "Publications and Reports": http://www.ombud.gov.bc.ca.

The following may also help you evaluate your practices.

TIPS FOR BEST PRACTICE:

- **Support the privacy officer –** Have senior management support the designated privacy officer and give him or her authority to deal with privacy issues related to your operations.

- **Advertise the identity of the privacy officer –** Make sure that all staff knows who the designated privacy officer is and include the privacy officer's contact information on your web site.

- **Analyze your own practices –** Identify the purposes for which your organization is collecting personal information and analyze your business's personal information handling practices. Make sure they meet fair information principles (see sections on collection, use, disclosure, protection).

- **Develop and implement privacy policies –** Implement polices and procedures to protect personal information, including complaint-handling procedures.

- **Insert privacy clauses in agreements –** Include a privacy protection clause in contracts to make sure that your contractor protects personal information the way your organization does.

- **Inform staff –** Inform and train staff on privacy policies and procedures.

- **Communicate your privacy policies –** Make information available explaining your policies and procedures (for example, in brochures and on web sites).

2. Obtain consent

Summary: Obtaining consent to collection of personal information

Your organization generally needs an individual's consent to collect his or her personal information (directly or from another source) and to use and disclose it. There are some exceptions to the need to get consent for these things.

PIPA considers consent to be given when an individual, knowing of the purpose for the collection of his or her information, voluntarily gives the information to you.

You should decide, however, whether getting express, written consent is desirable, notably for more sensitive personal information. When deciding on which type of consent you should obtain, consider what is reasonable for the individual, the circumstances of collection, your proposed uses or disclosures of the information, the sensitivity of the information, and whether you may need to prove that you obtained consent.

An individual can change or withdraw consent in some situations, but not if it interferes with a legal obligation.

Bottom Line: Unless PIPA says that you don't need consent, you **must** get consent to:

- collect personal information,
- collect personal information from a source other than the individual,
- use personal information, or
- disclose personal information. **[section 6]**

Types of Consent [sections 7 to 9]

Your organization should choose an appropriate form of consent in light of your proposed use or disclosure of the personal information and its sensitivity. You should also always consider what kind of consent an individual would reasonably expect, in the circumstances, given the sensitivity of the information and the uses or disclosures you plan for the information.

PIPA recognizes the following types of consent:

1. express consent
2. deemed consent
3. consent by not declining to give consent (also known as 'opt-out consent')

Express consent

Express consent signifies that an individual, knowing what personal information is being collected and for what purposes, willingly agrees to the information being collected, used and disclosed as notified. Express consent can be given in writing or verbally. If you rely on verbal consent, remember that you may have to prove later that the consent was actually given by the individual.

Some examples of express consent follow.

Example

Natalie signs up for a loyalty card at a grocery store to obtain lower prices and special offers. The consent form explains all the uses and disclosures of her personal information, and Natalie signs the form agreeing to those things.

Example

An organization provides family counselling for couples considering divorce. Hank and Celeste sign consent forms outlining how the organization will collect, use, and disclose this sensitive personal information.

Deemed consent

PIPA says that an individual is "deemed" to consent to collection, use or disclosure of personal information if the individual voluntarily provides it for a purpose that would, at the time, be considered obvious to a reasonable person.

PIPA does not require an organization to provide written or verbal notice of its intended uses or disclosures of personal information when collecting it in such a situation. This is because "deemed" consent only works in cases where those purposes would be considered so obvious that notification would be unnecessary.

Here are examples of when deemed consent can and cannot be used.

Example

Cory takes his suit in to the dry cleaner. The dry cleaner asks for his name and a phone number. Cory provides these voluntarily. Cory is deemed to have consented to the cleaner using his name and phone number to identify Cory when he returns to collect his suit, or to contact him if he forgets to pick it up.

Example

If the dry cleaner were part of a larger store, and the organization wished to use the information to market other services, it could not do so without telling Cory this and getting his consent after doing so. This is because the marketing use would not be obvious to a reasonable person bringing in dry cleaning.

Consent by not declining consent (by not opting-out)

In some cases, your organization can get consent by giving individuals a chance to decline consent. They can, in other words, opt out of your proposed uses or disclosures and thus decline to give consent. If they give you their personal information knowing what you intend to do with it, they have consented to the notified uses and disclosures.

A common method of opt-out consent is where a form contains a notice of what the organization intends to do with the personal information it collects and also a check-off box. If your organization tells people what you will use their names and addresses for, such as to send them information about your other products, they can check the box if they do *not* want you to use their information for this purpose. This is declining consent, which is also called 'opting out'. If an individual leaves the check-off box blank, they have consented to your sending them information about other products.

Your organization can only use this form of consent by meeting the conditions below:

- Your organization must let the individual know why it is going to collect, use or disclose the personal information (in other words, you have to tell people what your organization plans to do with the information).
- Your organization must do this through an easy-to-understand notice given before, or at the time, it collects, uses, or discloses the information.
- The individual must have had a reasonable chance to say "no" to the collection, use or disclosure. The chance must be reasonable in terms of the format, procedure and time for declining consent.
- The personal information must not be so sensitive that it would be unreasonable for the organization to use an opt-out form of consent to collect, use or disclose it.

The following examples illustrate acceptable methods for providing the opportunity to decline consent:

Example

Aaron enters a draw to win a computer. He provides his name and home e-mail address on the entry form. The form clearly says the company also will use this information to send him information about similar products from the company. The form provides a space to check if Aaron does not want to receive such information.

Example

Paulette signs up to take a Spanish course at a language academy. The registration form has a box indicating she will be on the mailing list for future course calendars unless she chooses to remain off the mailing list, which she can indicate by ticking a box.

Example

A magazine subscription form says that the company normally shares the names and addresses of subscribers with other companies. The form provides a toll free number that subscribers can call to remove their names from the list.

Withdrawing or changing consent

An individual can cancel or change his or her consent by giving the organization reasonable notice, as long as doing so does not break a legal duty or promise between the individual and the organization. **[section 9]**

The organization must let the individual know what the consequences of cancelling or changing consent will be. For example, if cancelling consent means that your organization will no longer honour an extended warranty, you must inform the customer of this consequence.

An individual should be able to put reasonable terms and conditions on his or her consent. For example, the individual may say that the an organization can use the personal information to supply one specific product to the individual, but not to use it in the future to market new related products.

Refusing to sell a product or service

Your organization can only require an individual to consent to your collection, use or disclosure of personal information, as a condition of your supplying the individual with a product or service, to the extent that you need that information to supply the product or service. **[section 7(2)]** Your organization cannot, in other words, force someone to give more personal information than you need as a condition of their getting the service or product they want.

Example

A store cannot refuse to sell Bruce a jacket for cash because he refused to provide his home phone number or other personal details, such as his annual income.

Example

Under PIPEDA, the federal Privacy Commissioner has ruled that it is unreasonable for a phone company to refuse to provide cell phone service because a customer would not provide his social insurance number. The social insurance number is optional for conducting a credit check.

Consent obtained by deception is invalid

Your organization cannot get consent from someone by using false or misleading means or by misleading the individual about why they are collecting, using or disclosing the information. If this happens, the individual's consent is not valid. **[section 7(3)]**

Example

Kyle receives a survey in the mail asking for his opinions on current events. It includes an optional section for Kyle's name and address, and a series of questions about household purchases over the last three months. The survey form indicates that the organization will send discount coupons tailored to each survey respondent as a thank-you for completing the survey. T he company then sells the information to marketers. Because they did not notify him of the intended sale of his information, the company did not have valid consent to sell Kyle's name and address for marketing purposes.

TIPS FOR BEST PRACTICE:

- **Obtain consent in writing or orally, in person, by phone, by mail, by the Internet etc.**
- **Make consent clauses easy to find, use clear and simple language and be as specific as possible about your intended uses and disclosures.**
- **Choose the type of consent you obtain by considering the reasonable expectations of the individual, the circumstances surrounding the collection, and the sensitivity of the information.**
- **You may wish to obtain express consent whenever possible, especially when the personal information is sensitive.**
- **The PIPA regulations require that, for an individual who is a minor, seriously ill, or mentally incapacitated, an organization must obtain consent from a legal representative, such as a legal guardian or a person having a power of attorney or who has been appointed a legal committee.**

3. Follow the rules for collecting personal information

Summary: Rules for collecting personal information

Collect personal information only for reasonable purposes and only collect the amount and type of information reasonably needed to carry out the purposes for collecting it. You need to give notice about why you are collecting personal information before, or at the time, you collect the information. Collect directly from the individual unless he or she agrees to someone else giving the information to you.

Bottom Line: An organization may collect personal information only for purposes that are reasonable and may only collect information that is reasonable for fulfilling out those purposes. **[section 11]**

Your organization can only collect personal information for purposes that a reasonable person would consider appropriate in the circumstances *and*, unless PIPA otherwise allows you to collect it, only to fulfill the purposes that you notify the individual of. **[section 11]** This rule, and the exceptions to it, are discussed below.

Your organization must limit the personal information it collects to what is necessary for fulfilling your organization's purposes for collecting it. Therefore, it is important that your organization clearly identify the purposes for which it is collecting personal information. You must limit both the amount and type of information collected. Doing so also benefits your organization because it lessens:

1. The risk of not properly using or disclosing personal information; and
2. The cost of collecting, storing, and retaining unnecessary information.

Even if an individual volunteers more personal information than is needed for your intended purposes, your organization cannot record, use or disclose the irrelevant information.

Your organization ideally should collect personal information directly from the individual the information is about. This helps to ensure that the information is accurate and maximizes the transparency of the transaction.

PIPA does not apply to collection of personal information before January 1, 2004

PIPA does not apply to the collection of personal information that was collected by your organization before January 1, 2004. **[section 3(2)(i)]** This means that you do not have to go back to individuals from whom you have already collected personal information before January 1, 2004 to obtain their consent after that date. Your organization may continue to use and disclose such information for reasonable purposes that fulfill the purposes for which it was collected without obtaining consent. However, if your organization wants to use such information for a new purpose, you need consent from the affected individuals.

PIPA's general rules about protecting personal information, about giving an individual access to his or her information and so on apply to all personal information held by your organization, including personal information collected before January 1, 2004.

Disclosing why personal information is collected (giving notice)

Your organization must, either before it collects personal information or at the time it collects it, let the individual know the purposes of the collection and the name of a person who can answer questions about it. **[section 10(1)]** You should define the purposes for collecting personal information as clearly and narrowly as possible, so the individual can understand how your organization will use or disclose the information. Avoid overly broad statements of purpose, since this can get you in trouble under the PIPA rule that collection, use and disclosure of personal information must be reasonable and appropriate in the particular circumstances.

Examples of specific collection purposes include opening customer accounts, verifying creditworthiness, providing benefits to employees, processing a magazine subscription, sending out club or association information to members, guaranteeing a travel reservation, identifying customer preferences; and establishing customer eligibility for special offers or discounts.

Your organization may put a personal information collection notice in writing (for example, on a form or a related section of a Web site) or give it verbally (for example, in person or during a phone call). When deciding whether to give notice in writing or verbally, consider the sensitivity of the personal information you are collecting and your proposed uses or disclosures of that information. Remember that you may have to prove that you gave notice by one method or another.

The following example of a collection notice gives some idea of what a written notice may look like.

Sample of a Personal Information Collection Notice

When you first become a customer of XYZ Company, or when you buy more products or services from us, we will collect your name, address and telephone number (or other necessary personal information) and will use it to:

- confirm your identity and credit history
- open an account with us
- establish your eligibility for special offers or discounts
- provide ongoing service

We may disclose your personal information:

1. to a person who we are satisfied is requesting the information on your behalf;
2. to other business units of XYZ Company to help serve you better;
3. to a credit reporting agency;
4. when permitted or required by law; or
5. to a public authority if, in our reasonable judgment, there appears to be an imminent danger which could be avoided by disclosing the information.

If you have any questions about the collection of your personal information, call us at _____ from _____ (give business hours).

Collecting personal information without consent

PIPA allows your organization to collect personal information about an individual without consent as set out in section 12(1):

- When a reasonable person would consider that it is clearly in the interests of the individual and consent cannot be obtained in a timely way. **[section 12(1)(a)]**

  Example: Getting a name and phone number to contact a family member in an emergency situation involving a relative of that family member.

- When collecting the personal information is necessary for the medical treatment of the individual and the individual is unable to give consent.

- If the collection is reasonable for the purposes of an *investigation* or legal *proceeding.*

  Example: A landlord investigating an apparent breach of a lease.

- When the personal information is collected by observation at a performance, sports meet or similar event that is open to the public and at which the individual voluntarily attends.

  Example: A sports scout gathers information about a hockey player's performance for recruitment purposes.

- If the personal information is publicly available. (Publicly available information will be defined in the PIPA regulation.)

- If the information is used to decide whether an individual is suitable for an honour, award or other similar benefit, including an honorary degree, scholarship or bursary (but not for a job or a promotion).

  Example: A Chamber of Commerce gathers biographical information to provide an achievement award to a member.

- When a credit reporting agency collects personal information to create a credit report, but only if the individual had consented to that disclosure to the original collector of the information.

  Example: A customer who applies for a loan from her credit union consents to its disclosing her personal information to a credit reporting agency.

- When another Act or regulation requires or allows for collecting information without consent.

  Example: Collecting an employee's social insurance number as required by the *Income Tax Act* (Canada) to issue a T4-slip.

- When the personal information was disclosed to the organization under the following sections of PIPA:

    - ♦ Section 18 permits disclosure of personal information without consent in specific circumstances.
    - ♦ Section 19 permits disclosure of employee personal information without consent for specific purposes outlined in Guideline 6 of this Guide.
    - ♦ Section 20 permits limited disclosure of personal information without consent to facilitate the sale of a business or its assets. These circumstances are also outlined below.
    - ♦ Section 21 permits disclosure of personal information without consent, under specified conditions, for research or statistical purposes.
    - ♦ Section 22 permits disclosure of personal information without consent, under specified conditions, for archival or historical purposes.

- If you need the information to collect a debt owing to your organization or to repay the individual money you owe.

    Example: A company collecting an individual's new address from Canada Post to collect a debt.

Collecting personal information indirectly or from another organization

PIPA allows an organization to collect personal information from a source other than the individual whose information is collected in cases where you do not need consent to collection (for example, where the information is necessary for the individual's medical treatment; the information is reasonable for an investigation and direct collection would compromise the availability or accuracy of the information). An organization may collect personal information from another organization without consent in order to carry out work for that organization that is solely for the purpose for which the personal information was originally collected. **[section 12(2)]**

In cases where consent to collection is required, you can collect an individual's personal information from another source if you have her or his consent. In deciding whether to get written or verbal consent to indirect collection, remember that you may have to show that you received consent for the indirect collection. It is important to note that your organization also must satisfy the organization that discloses information to you that the individual consented according to PIPA's rules, as in the following example.

Example

Jim wants to move to a new apartment. He can give the prospective landlord permission to contact his current landlord to obtain a reference. The current landlord needs to be satisfied that Jim actually did consent to the reference before disclosing the information. Therefore, Jim should let his current landlord know that he will be using the current landlord as a reference.

4. Follow the rules for using personal information

Summary: Rules for using personal information

Use personal information only for reasonable purposes that fulfill the purposes your organization identified at the time you collected the personal information. As well, only use the amount and type of information needed to carry out those purposes. PIPA permits using personal information without consent for limited and specific circumstances

Bottom Line: An organization may only use personal information for purposes that are reasonable and that are necessary to carry out the purposes your organization identified at the time it collected the information. **[section 14]**

Your organization can only use personal information for purposes that a reasonable person would consider appropriate in the circumstances *and*, unless PIPA otherwise allows you to use it otherwise, only to fulfill the purposes that you notify the individual of. **[section 14]** This rule and the exceptions to it, are discussed below.

Sometimes it is hard to decide what is a 'use' and what is a *'disclosure'* of personal information. The following explanations may help.

A 'use' of personal information usually means using it within your organization to carry out your organization's purpose for collecting the information. For example, your organization may use personal information in order to provide the individual with a product or service or to evaluate whether an individual is eligible for a benefit. For instance a shipping department's use of customer information that was collected by the billing department would be a valid use of the customer's name and address.

A *'disclosure'* of personal information involves your organization's showing, sending, or giving someone's personal information to someone else, including another organization, government or individual. To continue the example above, providing the customer's name and address when requested by Canada Customs and Revenue Agency would be a valid disclosure of personal information.

Using personal information without consent

PIPA allows your organization to use, without consent, personal information collected before January 1, 2004 for reasonable purposes that fulfill the purposes for which it was originally collected. If at any time your organization wants to use personal information collected before January 1, 2004 for a purpose other than the purpose for which you originally collected it, you will need to get consent for that new use (unless consent is not necessary under section 15, as discussed below). However, if the purpose was not documented, or was unclear, at the time of collection, it may be preferable to obtain explicit consent before using the personal information.

PIPA allows your organization to use personal information about an individual without consent in certain situations listed in section 15. The situations listed in section 15 are the same as those listed above for collection of information without consent, which you should refer to. Section 15 also allows the following further uses without consent:

- When a credit reporting agency is permitted under PIPA to collect the personal information without consent and uses that personal information only to create a credit report and for no other purpose. **[section 15(1)(k)]**

- If your organization uses the information to respond to an emergency that threatens the life, health or security of an individual or the public. **[section 15(1)(l)]**

  Example: If an individual makes a threat against another person, using the information to prevent the person from being injured.

5. Follow the rules for disclosing personal information

Summary: Rules for disclosing personal information

Disclose information only for reasonable purposes that your organization identified at the time of collection. As well, only disclose the amount and type of information needed to carry out those purposes. PIPA permits disclosing personal information without consent for limited and specific circumstances

Bottom Line: An organization may only disclose personal information for purposes that are reasonable and that are necessary to carry out the purposes it identified at the time of collection. **[section 17]**

Your organization can only disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances *and*, unless PIPA otherwise allows you to disclose it, only to fulfill the purposes for which it was collected. [**section 17]** This rule and the exceptions to it, are discussed below.

Disclosing personal information without consent

PIPA allows your organization to disclose, without consent, personal information collected before January 1, 2004 for purposes that are reasonable and that fulfill the purpose for which it was originally collected. If at any time your organization wants to disclose personal information collected before January 1, 2004 for a purpose other than the purpose for which you originally collected it, you will need to get consent for that new disclosure (unless consent is not necessary under section 18, as discussed below). However, if the purpose was not documented, or was unclear, at the time of collection, it may be preferable to obtain explicit consent before disclosing the personal information.

PIPA also allows your organization to disclose personal information about an individual without consent in certain situations listed in section 18. With one exception, the situations listed in section 18 are the same as those listed above for use of information without consent, which you should refer to. The exception is that section 18 does not allow disclosure of personal information for credit reporting purposes. You should also note that section 18 allows the following further disclosures without consent:

- When a treaty requires or allows for disclosure without consent and the treaty is made under an act or regulation of British Columbia or Canada.

- When the disclosure is necessary to comply with a subpoena, warrant or order by a court or other agency with jurisdiction to compel the production of personal information.

  Example: Disclosing personal information when a court order is served on an organization.

- When the disclosure is to a public body or a law enforcement agency in Canada to assist an investigation of an offence under the laws of Canada or a province of Canada.

  Example: To the Workers' Compensation Board carrying out an investigation of a workplace accident or to police investigating a robbery.

- If the information is disclosed to respond to an emergency that threatens the health or safety of an individual or the public and if notice of the disclosure is mailed to the last known address of the individual to whom the personal information relates.

  Example: If an individual makes a serious threat against another person, the information may be disclosed to prevent the person from being injured, as long as you notify the individual about the disclosure.

- When disclosure is needed to contact next of kin or a friend of an injured, ill or deceased individual.

  Example: Contact information disclosed so that the family may be contacted.

- If the disclosure is to a lawyer representing your organization.

- If the disclosure is to an archival institution if the collection of the personal information is reasonable for research or archival purposes.

- When another Act or regulation requires or allows the disclosure without consent.

  Example: Disclosing an employee's social insurance number as required by the *Income Tax Act* to prepare a T4-slip.

6. Follow special rules for employee personal information

Summary: Employee personal information

PIPA has special rules for "employee personal information" and considers employees to include volunteers. Your organization may collect, use and disclose employee personal information without consent if it is reasonable for starting, managing or ending an employment or volunteer relationship with the individual involved. However, you need to give notice to the employee that you are doing so.

Bottom Line: An organization may collect, use and disclose employee personal information for reasonable purposes related to managing or recruiting personnel without consent as long as it notifies the employee.

PIPA defines the terms "employee", "employee personal information", "contact information" and "work product information". You should refer to the definitions for precise understanding of those terms, but the following descriptions give a sense of what they mean.

An *employee* is someone employed by the organization or someone who performs a service for the organization and includes:

- an apprentice
- a volunteer
- a work experience or co-op student

Employee personal information refers to personal information that is reasonably needed to establish, *manage,* or end a work, or volunteer work, relationship. It does not include personal information about employees held by an organization that is not related to those things. Employee personal information is therefore a distinct category of personal information and PIPA treats it differently in some ways, as discussed below. Employee personal information does not include business *contact information* or *work product information*.

Contact information refers to an individual's name and position or title, business telephone number, business address, business e-mail, business fax number and other business contact information.

Work product information refers to information prepared by individuals or employees in the context of their work or business, but does not include personal information about other individuals. For example, a work-related report prepared and signed by an employee would be work product information but, if the report contained personal information about the organization's customers, that portion of the report would remain the personal information of the customers.

Managing personnel means human resource management activities relating to the duties and responsibilities of employees, not contractors or consultants. It can also refer to administering personnel, and includes activities such as payroll, performance evaluation, discipline, reward and promotion, and succession planning.

Your organization can collect, use, and disclose *employee personal information* without consent:

- where, as discussed above, PIPA allows collection, use or disclosure of personal information without consent or deems consent to be given; or
- if the collection, use or disclosure is reasonable for the purposes of establishing, managing or terminating an employment relationship between your organization and the individual, but the individual must be given notice as described in the next paragraph.

If PIPA does not allow collection, use or disclosure of personal information without consent or deem consent to be given, the individual is entitled to prior notice that your organization is collecting, using or disclosing employee personal information about that individual and the purpose for doing so.

Whether or not your organization needs consent, your collection, use and disclosure of employee personal information must be reasonable for the purpose of establishing, managing or terminating an employment relationship with the individual.

As with other personal information, if your organization uses an individual's employee personal information to make a decision that directly affects the employee, you must retain that information for at least one year after using it, so that the individual has a reasonable opportunity to obtain access to it. In other cases, your organization must destroy *documents* containing employee personal information once the purpose for which the employee personal information was collected is no longer being served by retention of the employee personal information and retention is not necessary for legal or business purposes.

Example

Earl has a medical condition that has kept him from working for several weeks. Earl's doctor has informed him that he should expect to be away from work for several weeks more. Earl's employer has a long-term disability plan that requires that proof of disability must be provided to the carrier of the plan. The terms of the plan also allow the carrier to confirm to the employer that an employee is disabled and unable to return to work and the expected length of absence from work.

Earl qualifies for, and wants to apply for, long-term disability benefits. It is reasonable for his employer to require Earl to sign a consent form authorizing his physician to disclose medical information to the carrier and for the carrier to inform Earl's employer for the expected duration of his absence for medical reasons. The carrier must not disclose to his employer any of Earl's medical information except as permitted by the terms of the plan and of the consent form.

7. Follow the special rules for business transactions

Summary: Business transactions and personal information

When buying or selling a business, your organization may collect, use and disclose information without consent when those involved agree to do so only for the transaction and when they need the information to decide whether to buy or sell.

Once the transaction is completed, the organization receiving the personal information may continue to use and disclose it, but the information can only be used and disclosed for the purpose for which it was collected. Further, the information must relate solely to the carrying on of the business. Also, the organization receiving the personal information must notify employees, and others whose personal information has been disclosed, that the business transaction has taken place and that their personal information was disclosed as part of the transaction.

If the transaction does not proceed, the organization that received the personal information must destroy or return it.

Bottom Line: Your organization may collect, use and disclose personal information for business transaction purposes without consent under certain conditions, if it meets the conditions specified in PIPA. **[section 20]**

A *business transaction* is defined in section 20 of PIPA to mean the purchase, sale, lease, merger, amalgamation, acquisition or disposal of an organization (or part of an organization) or any business or activity or business asset of an organization. The transaction may include the taking of a security interest (for example, a mortgage) in the organization and includes a prospective transaction (one that may occur in future). Section 20 does not apply where personal information is the only asset being purchased, sold, leased, etc. Substantial assets other than personal information must be part of the business transaction.

Your organization can collect, use and disclose personal information without consent to a prospective party for the purposes of deciding whether to proceed with a *business transaction* if:

1. The prospective party needs the information to decide whether to go ahead with the transaction; and

2. The prospective party has entered into an agreement to use or disclose the personal information *solely* for purposes related to the prospective transaction.

If the transaction does go ahead, the organization that originally held the personal information may disclose, without consent**,** personal information of employees, customers, directors, officers and shareholders of the organization to another party to the transaction on the condition that:

1. The organization receiving the personal information must use or disclose it only for the same purposes for which it was collected, used or disclosed by the organization providing the personal information;

2. The disclosure is only of personal information that relates directly to the part of the organization or its business assets that is covered by the business transaction; and

3. The employees, customers, directors, officers and shareholders whose personal information is disclosed are notified that the business transaction has taken place and that the personal information about them has been disclosed.

If the transaction does not go ahead, the organization that received the information for the transaction must return or destroy it.

Your organization should disclose, or receive, personal information for business transaction purposes only in accordance with a written agreement between the parties to the transaction that expressly incorporates the above rules.

Example

ABC Corporation is considering buying XYZ Enterprises, a video rental store. To decide whether to go ahead with the purchase, ABC wants to see some of XYZ's business documents that contain personal information about customers and employees. XYZ may provide these documents without consent of the individuals, as along as ABC has entered into an agreement to protect the information and not to use it for purposes other than the purchase of XYZ. If the deal goes through, ABC may continue to use the personal information for the original purposes for which it was collected once those whose personal information was received are notified. If the deal does not proceed, ABC must return the personal information to XZY or destroy it.

As noted earlier, section 20 does not apply where personal information is the only substantial asset being purchased, sold, leased, transferred, disposed or disclosed, as the following example illustrates.

Example

A company that specializes in helping couples to plan their weddings decides to establish a dating service to stimulate business. It incorporates a second company to do so. The dating service company grows quite large and successful by collecting, with consent, very personal information from individuals to assist them to meet other compatible individuals.

However, complaints from the small minority of dissatisfied customers of the dating service company are distressing to the principals of the company, who are used to dealing primarily with blissfully happy couples. They decide to sell the now lucrative dating service *data-base* but discover that they are precluded from doing so without obtaining the consent of the now numerous customers of the dating service company.

8. Follow the rules for giving individuals access to their own personal information

Summary: Requests to obtain one's own personal information

Individuals have a right to be given access to their own personal information, to know how their information is or has been used, and to know to whom and in what situations your organization has disclosed the information. Organizations may charge a minimal fee for access, but cannot charge a fee to their employees for giving access to employee personal information.

Your organization has a duty to help individuals with their requests and to respond within 30 business days. You can extend the response time in certain cases.

In some circumstances, you can or must refuse access to someone's personal information, including where disclosure would harm someone else, would harm an investigation or legal proceeding, when access would disclose someone else's personal information, or would disclose confidential business information.

If an individual is not satisfied with what you disclose, he or she may ask the OIPC to review your response.

PIPA regulations may be issued to authorize another person to act on behalf of the individual in some cases, for example, a parent on behalf of a young child.

Bottom Line: Your organization must give individuals access to their own information and respond openly, completely, and accurately. There are a few exceptions to giving access.

Overview of an individual's right of access to his or her information

An individual has the right to ask for access to his or her own personal information in the *custody* or under the *control* of an organization. **[section 23]**

A request for access must be in writing and must give enough information so the organization can, with reasonable effort, find the information. An individual who makes a request is called an *applicant*. An applicant may ask to see the information or receive a copy of it. Applicants do not have to say why they are asking for the information.

The organization must respond to an applicant within 30 business days after receiving the request. In some cases PIPA allows more time to respond to a request.

Unless your organization does not have personal information about the applicant or PIPA allows or requires it to refuse access to information, your organization must:

- give the applicant access to his or her personal information,
- tell the applicant what the information has been, or is being, used for, and
- tell the applicant to whom, and in what situations, the information is being, or has been, disclosed by the organization.

Your organization may not have any record of the persons or organizations to whom it has disclosed an individual's personal information before January 1, 2004. If this is the case, the organization should tell the individual who, or what organization, it may have disclosed the information to.

Can you charge fees for access?

Your organization may charge an applicant a "minimal fee" for responding to a request for access to the applicant's personal information. **[section 32(2)]** You must give an applicant a written estimate of the total fee for your organization to respond *before* you process the request. You may require the applicant to pay a deposit before processing the request. **[section 32(3)]**

Your organization may *not* charge any fees for a request for access to an applicant's *employee personal information*. **[section 32(1)]**

TIPS FOR BEST PRACTICE:

- A fee could include actual, out-of-pocket, costs such as copying and postage, but not a handling or processing fee.
- If the request involves only a few pages of *documents* that are easy to locate, the fee should be small.
- If the request involves a large number of *documents*, and it takes a long time to locate and produce the *documents*, the fee could be larger, remembering that your are limited to charging a "minimal fee" for access to personal information and no fee at all for someone's employee personal information.

Who can request personal information?

At this time no regulations have been made to give other people the right to access personal information on behalf of minors or deceased people. If such regulations are made, this guide will be revised accordingly.

How do you respond to a request for personal information?

Section 28 says that your organization must:

- make a reasonable effort to help an applicant who seeks access to her or his own personal information;
- respond to an applicant as accurately and completely as reasonably possible.

If the applicant asks, and if it is reasonable to do so, you must explain any term, code or abbreviation used in a *document.*

If someone's personal information is in electronic form, your organization should provide a paper copy of the information wherever it is reasonably possible to do so.

How long do you have to respond to a request for personal information?

You must make every reasonable effort to respond to an access request within 30 business days after your organization received the request. **[section 29]** Section 31 of PIPA allows you to take an extra 30 business days to respond if:

- the applicant does not give enough information to allow you to find the personal information or the document requested;
- a large amount of personal information is requested or has to be searched and meeting the time limit would unreasonably interfere with your organization's operations; or
- you have to consult with another organization or *public body* to decide if access should be given.

You may also ask the *Commissioner* for a longer extension than 30 business days. **[section 31]**

If you take extra time for your response, you must tell the applicant, at the time you take the time extension:

- why you are taking more time,
- when you will respond to the request, and
- that the applicant can complain to the Commissioner about your organization taking more time. **[section 31]**

If you do not respond to the applicant in the required time, including where the response time is extended as described above, the applicant can complain about this to the Commissioner.

What must your response to an access request say?

When you respond to a request, you must tell the applicant:

- if you have a document that contains the individual's personal information;
- whether you will give access to all or part of the document; and
- if access will be given, where, when and how it will be given. **[section 28]**

If you refuse access to all or part of a *document*, you must tell the applicant:

- the reasons for refusing access and the sections of PIPA that allow, or require you, to refuse to give access;
- the name of the person in the organization who can answer questions about the refusal; and
- that the applicant may ask the Commissioner to review your organization's decision to refuse access. **[section 30]**

When can your organization refuse to give someone their personal information?

Your organization is entitled to refuse access in a number of situations: **[section 23(3)]**

- When the personal information is protected by solicitor-client privilege (for example, a letter from your organization's lawyer containing legal advice about a lawsuit the applicant has brought against your organization).
- When disclosure of the personal information would reveal confidential commercial information that could, in a reasonable person's opinion, harm the competitive position of your organization.
- When the personal information was collected for an *investigation* or *legal proceeding* that has not concluded (including any appeals).
- When the organization is a credit reporting agency and the personal information was last disclosed by the agency in a credit report more than 12 months earlier.
- When the information was collected by a mediator or arbitrator in conducting a mediation or arbitration where the mediator or arbitrator was appointed under a collective agreement, a law or by a court.

Example

Joe, a former employee of ABC Corporation, asked for access to his personnel file. Joe and ABC Corporation were involved in a dispute before the Workers' Compensation Appeal Tribunal. ABC Corporation reviewed the applicant's file and refused to give him access to the following personal information on his file:

- information prepared by company lawyers about the WCB dispute and the grievance Joe filed (information protected by solicitor-client privilege); and
- information about ABC Corporation's ongoing investigation into Joe's fitness to work (information collected for the investigation).

Your organization may, in some cases, be required to refuse access to someone's personal information. You must refuse access to personal information the disclosure of which:

- Could reasonably be expected to threaten the safety or physical or mental health of another individual;
- Could reasonably be expected to cause immediate or grave harm to the safety or to the physical or mental health of the individual who made the request;
- Would reveal personal information about another individual; or
- Would identify the individual who gave you an opinion about another individual, and the individual giving the opinion does not give his or her consent to disclose his or her identity. You can hold back the identity of the person who wrote the opinion while still giving access to the opinion itself, unless the applicant could figure out who gave the opinion by reading it. **[section 23(4)]**

If any of the information in a *document* meets these criteria, that information has to be removed. The remaining information would then be given to the individual. **[section 23(5)]** This process is referred to as "severing" the information from the document. It is intended give the applicant the personal information to which he or she is entitled, while protecting the personal information of others and avoiding harm by releasing information as specified above.

Example

Mary applies for a promotion in her company. Three employees of the company are asked by a human resources consultant to give their opinions about Mary's work habits and leadership ability. The human resources consultant makes notes of their comments on the competition file. After Mary does not get the promotion, she asks for access to her file, including the notes made by the human resources consultant.

The company reviews Mary's file and asks the three employees if they will consent to the release of their names. One employee gives her consent but two employees, who have had an ongoing feud with Mary, do not give their consent. The company gives Mary partial access to her file, including the comments of the three employees and the name of the one employee who consented to the release of her identity. The company removes the names of the two employees who did not give consent. It also removes information that would reveal the identity of the each individual who gave opinions about Mary and did not consent to disclosing his or her identity.

TIPS FOR BEST PRACTICE:

- Try to keep personal information about each individual in one file or place, to make it easier to find it for an access request. Alternatively, keep a record of where all such information can be found.
- Never disclose personal information unless you are sure of the identity of the applicant and the applicant's right of access.
- When disclosing personal information to an applicant, ensure that it contains no information that section 23(4) PIPA *requires* you to withhold.

9. Follow the rules for correcting personal information

Summary: Correcting personal information

Individuals have a right to ask your organization to correct their personal information if they believe that your records contain factual errors or omissions.

You must correct any factual error or omission and inform other organizations to which you have disclosed the incorrect information.

If you decide there is no factual error or omission, you must annotate the record with the requested correction that you did not make.

If an individual is not satisfied with your decision, she or he can ask the *Commissioner* to review the matter.

Bottom Line: Your organization is responsible for making reasonable efforts to ensure that personal information is accurate and complete and to correct personal information if it is not.

Requests for corrections to personal information

An individual who believes there is an error or omission in his or her personal information under the *control* of your organization can ask you to correct it. **[section 24]**

The individual must make a written request for correction and give you enough background information so that your organization, with reasonable effort, can identify the correction being sought. Your organization cannot charge a fee for handling requests for correction.

How to respond to a request for correction

Your organization must decide, on reasonable grounds, if it should correct the information. If you decide the information should be corrected, then it must be done as soon as possible. Your organization must send corrected information to every organization to which it disclosed the wrong information during the year before the correction date. **[section 23(2)]**

If your organization decides that the information is correct and therefore decides not to make the requested correction, you must annotate (make a note to) the personal information saying that the correction was requested but not made. **[section 24(3)]**

If your organization receives a notice from another organization that an individual's personal information previously disclosed to you has been corrected, your organization must correct that personal information that is under its *control*. **[section 24(4)]**

Example

Joy recently discovered that XYZ Company's documents incorrectly say that she is married. She sends a request for correction to show her status as single. XYZ should correct its documents, and, if it has disclosed that information, notify other organizations that received it within the preceding year.

Example

Randy recently returned to work after a few weeks off with a broken leg. The company doctor sent a note to his supervisor saying that Randy should not have to stand for more than three hours a day. Randy was copied on the note. Randy went to his own doctor who advised that he should not stand for more than one hour a day. Randy asked the company to correct the company doctor's note on file to say that Randy cannot stand for more than one hour a day. The company is not required to correct the doctor's professional opinion, but must add Randy's request to make the correction to the file.

10. Follow the rules for accuracy, protection and retention of personal information

Summary: Accuracy, protection and retention of personal information

If your organization is likely to use personal information to make a decision affecting an individual, take all reasonable steps to ensure the information is accurate and complete.

Use reasonable safeguards to protect personal information from theft, modification, unauthorized access, collection, use, disclosure and destruction. Safeguards should be appropriate to the sensitivity of the information.

Only keep information for as long as reasonable to carry out business or legal purposes. Use care in disposing of, or destroying, information.

Bottom Line: Take care of all personal information that you create, receive, or keep. Ensure it is accurate, appropriately protected, and retained for reasonable purposes.

Accuracy

Your organization must make a reasonable effort to ensure that personal information collected by or on behalf of your organization is accurate and complete *if* your organization is likely to use that personal information to make a decision that affects the individual to whom the personal information relates or your organization is likely to disclose the personal information to another organization. **[section 33]**

This rule helps prevent the use of wrong information to make a decision about an individual and the disclosure of wrong personal information that could be used by other organizations.

One way to decide if you need to update personal information is to consider whether use or disclosure of the information you have about an individual could conceivably lead to some harm or to a wrong decision being made about the individual because the personal information is incomplete or out of date.

What is reasonable depends on the circumstances. For example, you should be careful when you get personal information from someone other than the individual. The information may not be correct or you may not have the whole story. Also, what is reasonable will depend on what the information is going to be used for and how that might affect the individual.

Your obligation to protect personal information

Your organization must make "reasonable security arrangements" to protect personal information from "unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks". **[section 34]** These risks include the following:

- Someone being able to read, or collect, use, copy or disclose, personal information when he or she is not supposed to be able to do those things;
- Someone stealing or losing personal information; or
- Someone changing, destroying or improperly disposing of personal information.

The safeguards you implement should be appropriate to the sensitivity of the information. For example, a reasonable person would likely expect a higher level of security for patient records in a medical practice than for a social club's membership address list.

Examples of physical safeguards include:

- Locking file cabinets and areas where files are stored when no one is there;
- Allowing only employees who need access to the storage areas or filing cabinets to have access to them;
- Clearing files and documents containing personal information off your desk at the end of the day;
- Shredding papers containing personal information rather than placing them in a garbage can or recycling bin; and
- Completely erasing the hard-drive of any computers you sell or discard that contain personal information, and also, ideally, physically destroying the hard-drive.

Examples of administrative safeguards include:

- Regularly training and reminding employees about your policies for protecting personal information and PIPA's requirement to safeguard personal information, and the disciplinary consequences of not following the rules.
- Having employees enter into a confidentiality agreement regarding personal information.

Examples of technical safeguards include:

- Positioning computer monitors so that personal information displayed on them cannot be seen by unauthorized personnel or by visitors
- Using computer screensavers so unauthorized personnel or visitors cannot see personal information.

- Ensuring your computers and network are secure from intrusion, including by using firewalls and, where appropriate for sensitive personal information, by encrypting personal information to prevent unauthorized access.

- Using strong and secure passwords to make sure that only authorized workers have access to information on computers, and changing the passwords reasonably often.

- Erasing or destroying computer hard drives before you discard them, sell them or donate them. Be aware, in particular with regard to sensitive personal information, that it may not be possible to erase the information sufficiently that it cannot be restored by someone with the technical expertise to do so. The best practice in such case would be to destroy the hard drive physically.

- Modifying machines and cash registers that accept credit card payments so credit card numbers are removed or blotted out from a store's receipts.

How long must you retain personal information?

Section 35 of PIPA requires your organization to destroy documents containing personal information, or make the information anonymous, as soon as it is reasonable to assume that:

- the purpose for which the personal information was collected is no longer being service by keeping the personal information; and

- it is no longer necessary to keep the personal information for legal or business purposes.

If your organization uses an individual's personal information to make a decision that directly affects the individual, you must keep that information for at least one year after using it, so the individual has a reasonable opportunity to obtain access to it. **[section 35]**

Your organization may already have its own retention periods or schedules for *documents*, based on financial, legal, regulatory, operational, audit or archival requirements. These retention periods can still be followed subject to the above PIPA rule.

Even if an individual has changed or taken back his or her consent for collecting, using or disclosing information, your organization can keep that information if there are legal reasons to do so **[section 9(5)]**.

How will PIPA be enforced?

Summary: Oversight of PIPA

Individuals may complain to the OIPC if they consider their personal information has not been collected, used or disclosed as required by PIPA, that their personal information is not accurate or complete, or that their request for access or correction has not been handled properly.

The OIPC can investigate complaints made to it. It can also initiate its own investigation where reasonable grounds exist to believe an organization is not complying with PIPA. The OIPC will generally require a would-be complainant to first try to work out a solution directly with the organization involved, without OIPC involvement. The OIPC will try to mediate a settlement of any complaint that it does accept. It may hold a formal inquiry into a complaint that has not settled. The OIPC can compel testimony, order production of evidence and enter premises to investigate a matter.

The OIPC can issue binding orders and can publish its orders. Organizations have 30 business days to comply with an order unless they ask the BC Supreme Court to overturn the order before the 30-day period expires.

PIPA creates various offences, including using deception or coercion to collect personal information contrary to PIPA; disposing of personal information with an intent to evade a request for access to that personal information; obstructing the OIPC; and failure to comply with an OIPC order. There are fines of up to $10,000 for individuals and up to $100,000 for organizations.

Bottom Line: The OIPC has significant powers to investigate and deal with complaints and can order your organization to comply with its findings. In addition, individuals may sue you for damages they actually suffer due to your failure to comply with PIPA, if the OIPC has issued an order finding your organization in breach of PIPA.

The Commissioner can investigate complaints and hold inquiries

The Information and Privacy Commissioner is the same Commissioner as under the FOIPP Act. The *Commissioner* has the power to review the actions and decisions of organizations under PIPA. For example, the Commissioner can review or investigate: **[section 36(2)]**

- Any decision, action or failure to act by an organization that has been asked to give access to or to correct personal information;
- A claim by an individual that his or her personal information has been improperly collected, used or disclosed; or
- A complaint against an organization not properly helping an applicant, about the time taken to respond to a request, or about the fees charged.

The Commissioner can:

- Send the individual to another grievance, complaint or review process (for example, the organization should have its own complaint process); **[section 38(4)]**
- Try to settle a complaint using mediation; **[section 49]**
- Hold an inquiry; **[section 50]**
- Issue binding orders; and **[section 52]**
- Authorize an organization not to respond to an individual's request for access to or correction of her or his personal information. **[section 37]**

Complaint Handling Procedures

PIPA is founded on the basis that it is good business practice for organizations to implement and follow sound personal information protection practices, including resolving complaints from those affected by the organization's practices. In most cases, before accepting a request for review or a complaint, the OIPC will ensure that the individual who wishes to complain or seeks a review has first tried to resolve the matter directly with the organization involved. This will involve the OIPC referring would-be complainants back to the organization if they have not already gone there. These OIPC referrals back to the organization will be to the organization's designated privacy officer.

It is therefore important that your organization have procedures in place to receive and respond to complaints or inquiries about its policies and practices relating to the handling of personal information. The complaint procedures should be easily accessible and simple to use and your organization should inform individuals who make inquiries or lodge complaints of the existence of relevant complaint procedures. Finally, your organization should investigate all complaints and, if a complaint is found to be justified, should take appropriate measures (including, if necessary, amending its policies and practices).

Duty to comply with Commissioner's orders

An organization must comply with an order not later than 30 business days from the day the order is given to the organization. **[section 52]** The exception is when an organization or individual applies for judicial review, in the BC Supreme Court, of the order. The organization or individual must apply for judicial review no later than 30 business days after the day on which the organization or individual seeking judicial review was given a copy of the order. The order is then stayed until the BC Supreme Court deals with the application.

Example

Trevor Young is employed by Company X, which has a management agreement with Company Y. One part of the agreement between the Companies is that Company Y can have access to the personnel files and training records of employees of Company X for management purposes, including the investigation of incidents. Trevor was the subject of an investigation and, during a meeting about the incident, he realized that Company Y had a copy of his personnel file.

Trevor complains to the OIPC that Company X had disclosed his personal information to Company Y improperly. Before the OIPC opens a file, it will ask Trevor if he has been to Company X about his complaint. If he has not, he may be asked to do that. If he has, the OIPC will open a file on the complaint. Someone from the OIPC will contact Trevor and Company X and try to help them work things out between them. If this cannot be done, the Commissioner may hold an inquiry.

Most complaints are resolved without an inquiry. An inquiry can be held in writing or in person, but is almost always held in writing. The Commissioner can issue a binding order following an inquiry.

An employee can refuse to contravene PIPA or can blow the whistle on an organization

An employee of an organization, acting in good faith, is protected from any punitive action by the organization if the employee does something to avoid or prevent a contravention of PIPA. The employee can also refuse to do something he or she believes is contrary to PIPA. **[section 54]**

An employee, acting in good faith, can tell the OIPC about a situation he or she reasonably believes to be a contravention of PIPA. The OIPC will then investigate the claim and will not disclose the identity of the employee. The "whistleblower" is protected from the organization's taking any negative action such as firing or suspending the employee. **[section 55]**

An individual or organization can be convicted of an offence under PIPA

It is an offence under PIPA to do any of the following things:

- Use deception or coercion to collect personal information in contravention of PIPA;
- Dispose of personal information with an intent to evade a request for access to the personal information;
- Obstruct or mislead the *Commissioner* or one of his staff;
- Retaliate against an employee for doing, or refusing to do, something to avoid or prevent a contravention of PIPA.
- Not follow an order. **[section 56(1)]**

PIPA provides for fines of up to $10,000 for individuals and up to $100,000 for organizations for offences committed.

A person or organization is not liable to prosecution for an offence against PIPA or any other Act because the person or organization complies with a requirement of the Commissioner under PIPA. **[section 56(3)]**

An individual can sue for damages

An individual can sue an organization for damages for "actual harm" the individual has suffered as a result of the organization's breach of its obligations under PIPA. Such a lawsuit can only be brought, however, if the Commissioner has made an order against the organization and it has become final by not being taken to the BC Supreme Court. Such a lawsuit can also be brought if the organization has been convicted of an offence under PIPA. **[section 57]**

GLOSSARY

Definitions of terms used in this Guide

Please note that, in any case of discrepancy or variation between the definitions below and those found in PIPA, the PIPA definitions take precedence over those below.

Applicant means an individual who requests access to personal information or a correction of personal information. **[section 25]**

Business transaction means the purchase, sale, lease, merger or amalgamation or any other type of acquisition, disposal or financing of an organization or a portion of an organization or of any of the business or assets of an organization. **[section 20(1)]**

Commissioner means the Information and Privacy Commissioner appointed under the *Freedom of Information and Protection of Privacy Act.* **[section 1]**

Contact information means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual. **[section 1]**

Control includes an organization's authority or ability to decide how to use, disclose and store personal information, how long to keep it and how to dispose of it. For example, personal information in the custody of a contractor providing services to the organization may still be under the control of the organization through the terms of its contract with the service provider.

Custody includes the keeping of personal information by an organization in its offices, facilities, file cabinets or computers.

Disclosure includes the showing, sending or giving of personal information to some other organization, government or person .

Document includes a thing on or by which information is stored, and a document in electronic or similar form. **[section 1]**

Domestic means related to home or family. **[section 1]**

Employee means an individual employed by an organization and includes a volunteer working under an unpaid volunteer work relationship. **[section 1]**

Employee personal information means personal information about an individual that is collected, used or disclosed solely for the purposes reasonably required to establish, manage or terminate an employment relationship between the organization and that individual, but does not include personal information that is not about an individual's employment. **[section 1]**

FOIPP Act means the *Freedom of Information and Protection of Privacy Act*, the Act that governs access to information and protection of personal information in the British Columbia public sector.

Investigation means an investigation related to

- a breach of an agreement,
- a contravention of an enactment of Canada or a province of Canada,
- circumstances or conduct that may result in a remedy or relief being available at law,
- the prevention of fraud, or
- trading in a security (as defined in section 1 of the British Columbia *Securities Act*) if the investigation is conducted by or on behalf of an organization recognized by the British Columbia Securities Commission to be appropriate for carrying out investigations of trading in securities, if the investigation is undertaken on a reasonably held belief that the breach, contravention, circumstance, conduct, fraud or improper trading practice has occurred or is likely to occur. **[section 1]**

Managing personnel means the carrying out of that part of human resource management relating to the duties and responsibilities of employees, not of contractors or consultants, and can also refer to administering personnel and includes activities such as payroll and succession planning.

Non-profit organization includes a charity, club, religious organization, community league or amateur sport association.

Organization includes:

- a person
- a corporation,
- a partnership,
- an individual acting in a commercial way , but not an individual acting in a personal or domestic capacity or acting as an employee,
- an association that is not incorporated,
- a trade union,
- a not-for-profit organization, and
- a trust (except for a private trust for the benefit of friends or family of the individual who sets up the private trust). **[section 1]**

Personal information means information about an identifiable individual. [**section 1]**

PIPA means the British Columbia *Personal Information Protection Act*.

PIPEDA means the federal *Personal Information Protection and Electronic Documents Act*.

Proceeding means a civil, criminal or administrative proceeding related to an allegation of:

- a breach of an agreement,
- a contravention of an enactment of Canada or of a province of Canada, or
- a wrong or breach of duty for which there is a remedy available under an enactment, at common law or in equity. **[section 1]**

Public body means a public body as defined in the *Freedom of Information and Protection of Privacy Act*, such as a government ministry, a regulatory agency, an administrative tribunal, a regional health authority, a local government, a public school board, public post-secondary institution or a professional regulatory organization. **[section 1]**

Work product information means information prepared by individuals or employees as part of their work responsibilities or activities related to their employment or business, but does not include personal information about an individual who did not prepare or collect the personal information. **[section 1]**