April 2012 (4th Publication)

A Guide to B.C.'s Personal Information Protection Act

for Businesses and Organizations

Office of the Information & Privacy Commissioner
for British Columbia

Protecting privacy. Promoting transparency.

Contents

Why a Guide?

The Office of the Information and Privacy Commissioner for British Columbia ("OIPC") developed this guide for businesses and other organizations to help you understand the *Personal information Protection Act* ("PIPA"), especially the areas of PIPA you are most likely to run across when operating your business or organization.

The guide will not answer every question you might have, but it will give you an overview of the major rules in PIPA and how you can operate to comply with those rules. You will find further resources about PIPA on the OIPC website.

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.

Many of the explanations in this guide are followed by references to sections in PIPA, which are noted in parentheses.[1] Some of the explanations and examples in this guide are based on decisions of the Commissioner on PIPA rules, which are called Orders.[2] The relevant Orders are also noted in parenthesis throughout this guide.

This document is 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.

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 should not take the place of legal advice. This guide 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 are authoritative and prevail in all cases.

This guide is 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 product and responsibility of the OIPC and neither of the Albertan organizations bears any responsibility of any kind for this guide.

1 The Personal information Protection Act, S.B.C. 2003, c. 63 is available at: http://www.bclaws.ca/
2 All PIPA Orders in this guide are available at: http://www.oipc.bc.ca/

What does the Personal information Protection Act do?

EXAMPLES

WHAT IS REASONABLE?

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

» A store has experienced a number of fraudulent returns of goods and has experienced losses from the return of stolen goods. To detect and deter the fraudulent returns, the store introduces a policy to ask customers to provide their names, addresses and telephone numbers when they return merchandise, which will only be disclosed to the police for fraud or theft investigations. The store's policy is reasonable in the circumstances. (Order P05-01)

The *Personal information Protection Act* (PIPA) is an Act about privacy in the private sector. PIPA describes how all private sector organizations must handle the *personal information* of its employees and the public (your customers) and creates common-sense rules about collecting, using and disclosing that *personal information*. PIPA intends to balance the following two principles:

- An individual's right to protect his or her *personal information*, and
- An organization's need to collect, use or disclose *personal information* for reasonable purposes (section 2 of PIPA).[4]

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

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

PIPA allows *personal information* to be collected, used or disclosed for reasonable purposes (section 4(2)). Under PIPA, reasonable means what a reasonable person would think is appropriate in the situation. What is reasonable will depend on factors such as the kind or amount of *personal information* you collect, how you plan to use that information, and where or to whom you plan to disclose that information (Order P05-01).[5]

4 The relevant PIPA section for this principle is section 2 of *PIPA*. You will see references to PIPA's sections following explanations throughout this guide.
5 These principles are taken from an *Order* (decision) of the *Commissioner*. You will see references to *Orders* following examples and explanations throughout this guide. You can find copies of these *Orders* on the OIPC website at: http://www.oipc.bc.ca/

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 3(1)).

An *organization* includes:

- a corporation, including a strata corporation,
- a partnership,
- a doctor's office,
- an association that is not incorporated,
- a co-operative association, including a housing co-op,
- a society,
- a church or other religious organization,
- a charity,
- a sports club,
- a trade union,
- a partnership,
- a political party,
- an individual involved in a commercial activity (for example, an individual running a small renovation business that is not incorporated), and
- a trust.

An *organization* does not include a person who is acting in a personal or *domestic* way (for purposes related solely to family or home activities).

Organizations not covered by PIPA

"Public bodies" regulated under the *Freedom of Information and Protection of Privacy Act* (FIPPA) are not organizations under PIPA. *Public bodies* include provincial government ministries, local governments, universities, colleges, public school boards, regional health authorities, hospitals, self-regulating professional bodies and Crown corporations (other than BC Rail, to which PIPA applies). PIPA also does not apply to personal information found in many court documents (section 3(2)).

Information covered by PIPA

PIPA applies to *personal information*. PIPA defines *personal information* as information about an identifiable individual, which means a person can be identified by the information, either directly (e.g. name, image, job title) or in combination with other information. For example, a health report about an unnamed individual would contain personal information if the individual could be identified through a street address, personal health number, phone number or other information that could link the information to the affected individual (section 1).

EXAMPLES

INFORMATION NOT COVERED BY PIPA

» In her spare time, Roberta, researches her family history. 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 this personal information is for purely personal purposes.

EXAMPLES

IS IT COVERED BY PIPA?

» Hassan 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 Hassan's writing of the article is for a journalistic purpose.

» 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 FIPPA and maintains control over the personal information through a contract. FIPPA applies to the payroll information the municipality sends to the accounting firm. However, PIPA will apply to the payroll information the accounting firm receives from its private-sector clients.

Personal information includes *employee personal information* but does not include business *contact information* or *work product information*. Non-identifiable or aggregate information, such as statistical information about groups of individuals, is not *personal information*.

PIPA does not apply to general information used to operate the business of an organization.

PIPA applies to *personal information* whether the information is recorded or not. For example, viewing a driver's license for the purpose of determining whether a customer is of legal drinking age is collection under PIPA (Order P10-01).

Information not covered by PIPA

PIPA does not apply if you collect, use or disclose *personal information* for the following purposes:

- personal, home or family purposes, for example, holiday card mailing-lists of family and friends (section 3(2)(a)),
- artistic or literary purposes, for example, if a character in your novel is recognizably a friend of yours (section 3(2)(b)), or
- journalistic purposes, to protect freedom of expression for the press (section 3(2)(b)). For example, personal information in newspapers is not covered by PIPA, however, a newspaper's *employee personal information* and subscribers' *personal information* is covered by PIPA.

PIPA also does not apply to *personal information* in certain circumstances, such as the following:

- PIPA does not apply to *personal information* if FIPPA applies. For example, a government ministry may have disclosed *personal information* to a private sector contractor carrying out work for that ministry, but maintained control over that information through contractual measures. FIPPA applies because the *personal information* is still under the ministry's control (section 3(2)(d)).
- PIPA does not apply to *personal information* if the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) applies to that information. For example, personal information held by a federally-regulated organization, such as a bank or telephone company, is regulated under PIPEDA even if the company is located in BC (section 3(2)(c)).
- PIPA does not apply to the collection, use or disclosure by a member or officer of the Legislative Assembly of *personal information* relating to his or her functions (section 3(2)(g)).

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. This should be expressly laid out in the contract.

How does PIPA affect legal proceedings?

Lawyers must follow rules and laws about how certain information is handled. Also, parties to legal *proceedings* have a right to get certain information by law. PIPA does not change that right and does not affect solicitor-client privilege (sections 3(3) and 3(4)). However, PIPA does apply to how lawyers and law firms handle their clients' and employees' *personal information* in the course of their practices.

Personal information in court documents or documents created by judges and the courts are not covered by PIPA (section 3(2)(e)). The same applies to documents containing *personal information* relating to a prosecution if those proceedings have not completed (section 3(2)(h)).

When does the *Personal Information Protection and Electronic Documents Act* apply?

PIPEDA is a federal act that protects *personal information* in provinces and territories that do not have their own private-sector privacy laws.

PIPEDA applies in BC in two circumstances. First, PIPEDA applies to federally-regulated businesses, for example banks, telephone companies, airlines, shipping companies and railways. Second, PIPEDA may apply to BC-based organizations when the *personal information* of residents from other provinces has been affected.

An organization cannot contract out of the PIPA rules

Your organization cannot contract out of its PIPA responsibilities. A ruling under FIPPA has confirmed that it is not possible to contract out of the similar rules under FIPPA (Order F00-47).

PIPA "trumps" other Acts of British Columbia

If a section of PIPA conflicts with another BC Act or Regulation, the section in PIPA must be followed unless the other Act states that PIPA does not apply (section 3(5)).

EXAMPLES

WHEN DOES PIPEDA APPLY?

» Brenda is an airline passenger waiting in line to go through security at an airport. She notices that she is required to pass through a full-body imaging scanner to pass the security checkpoint and catch her flight. She objects to the collection of her personal information by the body scanner and is told that she will have to complain to the airport authority. Since airports are regulated by the federal government, PIPEDA applies.

1 Be accountable for your information practices

EXAMPLES

IDENTIFYING PERSONAL INFORMATION UNDER YOUR CONTROL

» ABC Corp sends electronic information to XYZ Corp to process or store it for ABC Corp. The information is still under ABC Corp's control even though it has sent it to XYZ Corp. ABC Corp is obligated under PIPA to make sure that XYZ Corp protects that *personal information*, so includes a privacy protection clause in its contract with XYZ.

Highlights: Accountability

Your organization is legally responsible for all *personal information* under your control even if it isn't in your custody.

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

You must have procedures in place to receive and respond to complaints or questions about your policies and practices relating to the collection, use and disclosure of *personal information*.

PIPA requires you to choose an individual who is responsible for compliance with PIPA. You must make the individual's name and contact information publicly available.

Identifying *personal information* under your control

Organizations are accountable for the *personal information* under their *control*, including information that is not in their custody (section 4(2)).

Control includes an organization's authority or ability to decide how to use, disclose and store *personal information*, how long to keep *personal information* and how to dispose of it.

Control can take a number of forms, even if *personal information* isn't in your custody. 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.

You can use the following questions to help identify *personal information* that is in your organization's *control*, even if it isn't in your custody:

- Was the *document* containing *personal information* created by an employee, officer, director or owner of your organization in the course of your organization's operations?
- Was the *document* containing *personal information* created by an outside consultant for your organization?
- Was the *personal information* disclosed to you through your own collection?
- Was the *personal information* disclosed to you by another individual or organization?
- Do you or your employees use or disclose the *personal information*?
- Have you relied on the *personal information* for your organization's operations?
- Is the *personal information* integrated with other *documents* held by your organization?

- Does your contract permit your organization to inspect, review, possess or copy *personal information* or documents containing *personal information*? (Order F06-01)

Protect *personal information* that is under your *control*, by including privacy protection clauses in contracts or using other means to ensure a comparable level of protection while the personal information is being held by a third party.

Identifying the reasonable purpose for collection, use or disclosure of *personal information*

To be accountable under PIPA, your organization must do what a reasonable person would consider appropriate in the circumstances (section 4(1)). To develop policies and procedures that protect *personal information*, you must first identify the reasonable purposes for which your organization collects, uses and discloses *personal information*. This will allow your organization to determine what information it needs to fulfill its business purposes and ensure that *personal information* is collected, used and disclosed only for the reasonable purposes that you have identified.

Consider the following principles when developing secure information practices:

- You must limit the collection of *personal information* to that which is 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 the collection, use or disclosure of *personal information* beyond what is necessary to provide him or her with a product or service.
- *Personal information* should be collected by fair and lawful means.

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

EXAMPLES

IDENTIFYING YOUR REASONABLE PURPOSE FOR COLLECTION

» 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.

» 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, if the dealer wanted to use or disclose Susan's personal information for a different purpose, the dealer would have to satisfy two conditions: (1) the new purpose must be reasonable and, (2) Susan must consent to the new purpose, unless PIPA authorizes the dealer to use or disclose Susan's personal information without consent.

Designing compliant privacy policies and procedures

Your organization will need to develop and put into practice policies and procedures to protect the personal information that you collect, use and disclose (section 5). You can use the following questions to help assess whether your current practices comply with PIPA: [6]

1. What *personal information* do we collect?
2. For what purposes do we collect *personal information*?
3. Do we only collect *personal information* that we really need for our purposes?
4. How do we collect *personal information* and what do we tell individuals the purpose for collection is?
5. What do we use *personal information* for and are those uses reasonable and appropriate? Do these uses match what we tell individuals?
6. How do we obtain consent for collecting, using and disclosing *personal information*?
7. How do we ensure that the *personal information* is correct, complete and current?
8. Where do we keep *personal information* and how is it secured?
9. Who, within our organization, has access to or uses the *personal information*, and for what purposes? Are we limiting access on a need-to-know basis?
10. Who is *personal information* disclosed to outside our organization and why? Should we be disclosing personal information to others for the purposes we disclose it?
11. How long do we retain the *personal information*? When is it disposed of and how? Is it disposed of securely?
12. How do we respond to complaints or questions from individuals about our information practices?
13. In light of PIPA, should we change any of our practices?

Designating a privacy officer

Your organization must designate one or more individuals to make sure that your organization follows PIPA's rules. You must make the identity and contact information of your privacy officer(s) available to the public (section 4(3)). This individual may also be the contact person for answering questions about PIPA and for handling your access requests and complaints

6 See the OIPC website for more resources on developing privacy policies.

Creating procedures to handle privacy complaints

PIPA requires you to have procedures in place to receive and respond to complaints or inquiries about your organization's handling of *personal information* (section 5).

Your complaint procedures should be easily accessible and simple to use. If you receive a complaint, you should inform individuals about your complaint procedures. You may find it easier to provide a copy of a privacy policy or complaint process than to answer questions or otherwise make information available. Your organization should investigate all complaints and take appropriate measures in response if a complaint is justified, including amending your organization's policies and practices if necessary.[7]

Tips For Best Practice:

- **Analyze your own practices** – Identify the purposes for which your organization is collecting *personal information* and analyze your business' *personal information* handling practices.
- **Develop and implement privacy policies** – Implement policies and procedures to protect *personal information*, including complaint-handling procedures.
- **Insert privacy clauses in agreements** – Include privacy protection clauses in your contracts to make sure that your contractor protects *personal information* the same way your organization does.
- **Review your policies** – Review your *personal information* handling practices and policies on an ongoing and regular basis.
- **Support the privacy officer** – Have senior management support the designated privacy officer and give the privacy officer authority to deal with privacy issues related to your operations.
- **Advertise the identity of the privacy officer** – Make sure that all staff know who the designated privacy officer is and include the privacy officer's contact information on materials you provide to the public, such as on your website.
- **Inform staff** – Inform and train staff on privacy policies and procedures.
- **Communicate your privacy policies** – Make information available explaining your policies and procedures, such as in brochures and on websites.

7 See the OIPC website for resources on how to develop fair and effective complaint handing procedures. Although written for the public sector, see the Office of the Ombudsperson's Public Report No. 40, "Developing an Internal Complaint Mechanism" under Resources and Publications at http://www.ombudsman.bc.ca/.

2 Obtain consent

EXAMPLES

OBTAINING VALID CONSENT

» 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. The company then sells the information to marketers. Because the company did not notify Kyle of the intended sale of his information, the company did not have valid consent to sell his name and address for marketing purposes.

Highlights: Consent

You must have consent from an individual before you can:

- collect his or her *personal information*,
- collect his or her *personal information* from a source other than that individual,
- use his or her *personal information*, or
- disclose his or her *personal information*.

Even if you have consent, you must be able to demonstrate that the collection, use or disclosure of *personal information* is for a purpose that a reasonable person would find appropriate in the circumstances.

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

You cannot require an individual to consent to the collection, use or disclosure of *personal information* beyond what is necessary to provide a product or service.

You should decide what type of consent to obtain based on what is reasonable for the individual, the circumstances of collection, your proposed use or disclosure, 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 that would interfere with a legal obligation.

You may collect, use or disclose *personal information* without consent in only limited and specific circumstances.[8]

Obtaining valid consent under PIPA

Under PIPA, an individual cannot consent to the collection, use and disclosure of his or her *personal information* until your organization has created certain conditions for that consent. First, you must establish that there is a reasonable purpose for the collection, use or disclosure of and individual's *personal information*. Reasonable means that a reasonable person would consider the purpose for collection, use or disclosure of the *personal information* appropriate in the circumstances. Second, once you have established that reasonable purpose, you must notify the individual of that purpose. This means you must give the individual enough information about the collection of his

8 See Guidelines 3, 4, and 5 for information on collecting, using and disclosing personal information without consent.

or her *personal information* so the individual can make an informed decision whether to give consent (section 10(1)).[9] It is only at this point that an individual can provide consent in one of the ways described under PIPA (section 7(1)).

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)).

Requiring consent as a condition of supplying a product or service

Your organization can only require an individual to consent to the collection, use or disclosure of *personal information* if that information is "necessary" to provide the product or service (section 7(2)). This means that the *personal information* must be more than convenient to have or be of some possible future use. The personal information you require should be integral to the provision of your product of service (Order P09-01).

When determining whether you should require consent, consider the following questions:

- What is the purpose for requiring consent to the collection, use or disclosure of the *personal information*?
- Does the *personal information* fulfill a significant role in enabling your organization to achieve that purpose?
- Are there less privacy-intrusive means of achieving that purpose? (Order P09-01)

Types of Consent

Once you have established that you need to obtain consent from an individual to collect, use or disclose his or her *personal information*, you must choose an appropriate form of consent. PIPA recognizes the following types of consent:

1. express consent,
2. deemed consent, and
3. consent by not declining to give consent, also known as 'opt-out consent' (sections 7 and 8).

EXAMPLES

REQUIRING CONSENT

» 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.

» 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.

» Sharmeen, a senior citizen, orders an alcoholic drink in a restaurant. Her server tells Sharmeen that she must provide identification before serving her alcohol because the restaurant has a policy of requiring identification from all customers to determine whether they are of legal drinking age. The collection of Sharmeen's *personal information* is not necessary for the purposes of serving her. The restaurant cannot require this information according to PIPA (Order P10-01).

9 The obligation to provide notice is discussed further in Guideline 3.

EXAMPLES

EXPRESS CONSENT

» Naomi 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 Naomi signs the form agreeing to those things.

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

DEEMED CONSENT

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

» Using the same scenario, if the owner of the dry cleaner were part of a larger store and wanted to use Lee's name and phone number for the purpose of marketing, the owner could not do so without first, notifying Lee that the owner wanted to use Lee's information for this purpose and, second, getting Lee's consent. This is because at the time Lee brought in his dry cleaning it would not have been obvious to a reasonable person that the *personal information* being collected would be used for marketing purposes..

Express consent

Express consent signifies that an individual, knowing what *personal information* is being collected and for what purposes, willingly agrees to his or her *personal 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.

Deemed consent

Deemed consent happens when an individual doesn't expressly give consent but volunteers information for an obvious purpose and a reasonable person would think that it was appropriate for the individual to volunteer that information in those circumstances. In this case, PIPA says that an individual is deemed to consent to collection, use or disclosure of his or her *personal information* (section 8(1)).

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 this situation. This is because deemed consent only works in cases where those purposes for collection are considered so obvious that notification is unnecessary.

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

In some cases, an organization may give notice to an individual that it intends to collect, use and disclose the individual's *personal information* for a specific purpose, and gives the individual a reasonable amount of time to decline (opt out) to have his or her *personal information* collected, used or disclosed. If the individual does not opt out, he or she has provided consent for the organization to collect, use or disclose *personal information* for the specified purposes (section 8(3)).

For example, some organizations provide forms that notify individuals of their intended uses for *personal information* collection with a "check-off" box. Individuals can check the box if they do not want the organization to use their information for this purpose. By opting out, the individual has declined to give consent. However, if an individual leaves the check-off box blank, he or she has consented to the collection of his or her *personal information* for this use.

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

- Your purpose for collection must be reasonable in the circumstances.
- 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 communicate your purposes through an easy-to-understand notice, which you must give before or at the time you collect, use or disclose the information.

- The individual must have had a reasonable chance to say no to the collection, use or disclosure.
- The *personal information* must not be so sensitive that it would be unreasonable for your organization to use an opt-out form of consent to collect, use or disclose it.

Withdrawing or changing consent

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

If an individual wants to withdraw or change consent, you must let him or her 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 allow your organization to use his or her *personal information* to supply a specific product, but not to use *personal information* to market new products.

Tips For Best Practice:

- Consider the purpose behind your request for consent and whether the collection is necessary for the purposes of delivering your service or providing your product.
- Obtain express consent whenever possible, especially when the *personal information* is sensitive.
- 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.
- Obtain consent in writing or orally, or in person, by phone, by mail or the Internet.
- Make consent clauses easy to find. Use clear and simple language and be as specific as possible about your intended uses and disclosures.
- 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.

EXAMPLES

CONSENT BY NOT DECLINING

» Tran 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 Tran does not want to receive this advertising information.

» 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.

» 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.

3 Follow the rules for collecting *personal information*

EXAMPLES

REASONABLE COLLECTING OF PERSONAL INFORMATION

» A nightclub uses a scanning device to collect the driver's license information of its customers. The *personal information* collected by these devises is stored in a database for two years. The nightclub says it collects the information for court actions and to assist with police investigations. It is not reasonable for the nightclub to collect such a broad scope of *personal information* from customers and hold it for such a long time in the event that a crime occurs (Order P09-01).

Highlights: Collection

You may only collect *personal information* for a purpose that a reasonable person would consider appropriate in the circumstances. You must limit your collection to the amount and type of *personal information* that is necessary to fulfill your purposes for collecting it.

You must notify individuals of the reasonable purposes for collecting *personal information* before or at the time you collect that information.

You must obtain consent from an individual before or at the time you collect *personal information*.

You should collect *personal information* directly from the individual unless he or she agrees that someone else is allowed to provide his or her *personal information* to you.

You may collect *personal information* without consent in limited and specific circumstances.

Collecting *personal information* for a reasonable purpose

An organization may collect *personal information* only for purposes that are reasonable and may only collect *personal information* that is reasonable for fulfilling those purposes (section 11).

In order to limit the amount and type of *personal information* you collect and ensure it is for reasonable purposes, it is important to clearly identify your purposes for collection. Doing so lessens the risk that you are improperly collecting, using or disclosing *personal information* and the cost incurred from collecting, storing and retaining unnecessary information.

Reasonable means that a reasonable person, knowing the purposes for collection and the surrounding circumstances, would consider the purposes for collection to be appropriate. What is reasonable depends on the kind of *personal information* being collected, the purposes and circumstances around the collection, how the organization handles the information, and how an organization plans to use and disclose the information (Order P09-02).

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 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 collection.

Notification required for the purpose of collection

Before or at the time your organization collects *personal information* from an individual, you must let the individual know the purposes for your collection and the name of a person who can answer questions about it (section 10(1)). The information you provide must be clear and detailed enough to identify the particular purpose for collecting the information, as distinct from all other purposes, in a way that is understandable to members of the public. 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, sign or website) 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.

Tips for best practice: What to include in a notification of collection

- A description of the *personal information* you are collecting.
- All the purposes for your collection, use or disclosure of an individual's *personal information*.
- When and to whom you will disclose the individual's *personal information*.
- When an individual may "opt out" of collection, use or disclosure.
- The contact information for your privacy officer in case the individual has questions about your privacy policy or your collection, use and disclosure of his or her *personal information*.

EXAMPLES

NOTIFICATION REQUIRED

» A strata council installs video cameras in its complex for prevent break-ins, but does not place any signs notifying complex owners or guests about the use of video surveillance or the purpose for the video surveillance. The strata council has not disclosed that it is collecting *personal information* (images) or the purposes behind this collection (security), thus, has contravened section 10 of PIPA (Order P09-02).

Collecting personal information without consent or from another source

PIPA allows you to collect *personal information* about an individual without consent or from a source other than an individual in certain situations (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). For example, a skydiving company collecting a client's emergency contact information from the client's friend after an accident.
- When collecting the *personal information* is necessary for the medical treatment of the individual and the individual is unable to give consent (section 12(1)(b)).
- When the collection with consent would compromise the availability or accuracy of the *personal information* and the collection is for an *investigation* or *proceeding* (section 12(1)(c)). For example, an insurer can collect information about an insurance claimant's financial history to investigate suspected fraudulent activity.
- 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 (section 12(1)(d)).
- When the *personal information* is available to the public (section 12(1)(e)). Section 6 of the PIPA Regulations defines the type of information that is "available to the public".[10]
- When the information is used to decide whether an individual is suitable for an honour, award or other similar benefit, such as an honorary degree, scholarship or bursary (but not a job or a promotion) (section 12(1)(f)).
- When a credit reporting agency collects *personal information* to create a credit report, but only if the individual had consented to that disclosure by the original collector of the information (section 12(1)(g)). For example, when a customer who applies for a bank loan consents to the bank disclosing *personal information* to a credit reporting agency.
- When another Act or regulation requires or allows for the collection of information without consent (section 12(1)(h)). For example, an organization collecting an employee's social insurance number as required by the *Income Tax Act* to issue a T-4 slip.
- When the collection is necessary to collect or pay a debt owed to or by the organization (section 12(1)(j)).
- When the organization collects the information to provide legal services to a third party and the collection is necessary for that purpose (section 12(1)(k)).

10 The Personal Information and Protection Act Regulations are available at: http://www.bclaws.ca/

PIPA also allows your organization to collect information that was disclosed to you by another individual or an organization under certain conditions in the following circumstances:

- Where consent is not required for the disclosure (section 18).
- For employment purposes, as discussed in Guideline 6 (section 19).
- To facilitate the sale of a business or its assets, as discussed in Guideline 7 (section 20).
- For research or statistical purposes (section 21).
- For archival or historical purposes (section 22).

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. You must also be sure that the *personal information* you are collecting from another source was also collected from the individual in accordance with PIPA's rules.

Collecting personal information from or on behalf of another organization

PIPA allows you to collect *personal information* from or on behalf of another organization without consent in order to carry out work for that organization if the individual has already consented to the collection and provided that the collection is consistent with the purpose for which the *personal information* was originally collected (section 12(2)).

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. Your organization may continue to use and disclose this information for reasonable purposes and to fulfill the purposes for which it was originally collected. If your organization wants to use this information for a new purpose, you must obtain consent from the affected individuals. All other rights and obligations under PIPA for *personal information*, including the rules for its protection, use, disclosure and an individual's access, apply to *personal information* collection before January 1, 2004 (Order P06-01).

EXAMPLES

COLLECTING PERSONAL INFORMATION

» Jim wants to move to a new apartment. He gives the prospective landlord permission to contact his current landlord to obtain a reference. However, before giving the reference, the current landlord needs to be satisfied that Jim actually did consent to the reference before disclosing any personal information about Jim. Jim may have already asked his current landlord to act as a reference and, if so, this would be sufficient. If the current landlord is unaware of Jim's plans, when she receives a call from a prospective landlord she should call Jim to confirm the permission before giving the reference.

4 Follow the rules for using personal information

EXAMPLES

REASONABLE PURPOSES TO USE PERSONAL INFORMATION

» A strata council installs a video surveillance system to counter ongoing vandalism and notifies its residence of this collection. A month later, the council suspects that a number of its residents are not cleaning up after their dogs in the shared courtyard, which is against strata bylaws. The council decides to review the surveillance footage on a regular basis to detect violations and enforce the bylaw. Without evidence that this bylaw violation has become a problem that warrants the monitoring of residents by video surveillance (a use that fulfills the reasonable purpose), the strata council is not using the *personal information* captured by the video surveillance system for the original or a reasonable purpose (Order P09-02).

Highlights: Use

You must only use *personal information* for purposes that that a reasonable person would consider appropriate in the circumstances. You must limit the amount and type of personal information you use to what you need to fulfill the purposes that you identified to the individual from whom you collected the *personal information*.

You must notify individuals of the reasonable purposes for your use of their *personal information* at the time you collect it.

If you want to use *personal information* in a new way, that use must also have a reasonable purpose. You must also notify the individual whose personal information you collected about that new use and obtain his or her consent.

You may use *personal information* without consent in only limited and specific circumstances.

What is use?

Sometimes it is hard to see the difference between using *personal information* and disclosing *personal information*.

Using *personal information* usually means using it internally to carry out your organization's purpose for collecting the information. For example, your organization may use *personal information* to provide an 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 a customer's name and address, which was collected by the billing department, would be a valid use of that *personal information*.

Disclosing *personal information* means showing, sending, or giving some other organization, government or individual the *personal information* in question. To continue the example above, providing the customer's name and address when lawfully requested by the Canada Revenue Agency would be a valid disclosure of *personal information*.

Using *personal information* without consent

PIPA allows your organization to use *personal information* about an individual without consent in certain situations (section 15). These circumstances are the same as those listed in Guideline 3 (collection of information without consent). PIPA 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). For example, if you use the information to prevent an individual from being injured after hearing another person make a threat against that individual.

Using information from or on behalf of another organization

PIPA allows you to use *personal information* from or on behalf of another organization without consent to carry out work for that other organization if the individual has already consented to the use of the *personal information* and provided that the use is consistent with the purpose for which the *personal information* was originally collected (section 15(2)).

Using *personal information* collected before January 1, 2004

PIPA allows your organization to use, without consent, *personal information* collected before January 1, 2004 for reasonable purposes and to fulfill the purposes for which it was originally collected. If 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 must obtain consent for that new use unless PIPA allows otherwise. 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*.

EXAMPLES

REASONABLE PURPOSES TO USE PERSONAL INFORMATION

» Anja owns a bookstore and maintains an email list of customers who want information on new releases. When her friend, Rose, decides to run for city council, she uses this list to send out a mass email urging her customers to vote for Rose as a pro-book candidate. Rose has contravened PIPA because she is using the collected information for a new purpose (to campaign for Rose) without first determining whether the new use is reasonable and before notifying her customers that she wishes to use their email addresses for this new purpose and obtaining their consent to do so.

5 Follow the rules for disclosing personal information

Highlights: Disclosure

You must only disclose information for purposes that a reasonable person would consider appropriate in the circumstances. You must limit the amount and type of *personal information* you disclose to what you need to fulfill that purpose.

You must notify an individual of the reasonable purposes your organization identified for your disclosure of his or her *personal information* at the time you collect it.

If you want to disclose *personal information* in a new way, that disclosure must also have a reasonable purpose. You must also notify the individual whose *personal information* you collected about that new disclosure and obtain his or her consent.

You may disclose *personal information* without consent in only limited and specific circumstances.

What is disclosure?

Your organization can only disclose *personal information* for purposes that a reasonable person would consider appropriate in the circumstances and, unless PIPA allows otherwise, only to fulfill the purposes for which it was collected (section 17).

Sometimes it is hard to see the difference between using personal information and disclosing *personal information*.

Using *personal information* usually means using it internally to carry out your organization's purpose for collecting the information. For example, your organization may use *personal information* to provide an 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 a customer's name and address that was collected by the billing department would be a valid use of that *personal information*.

Disclosing *personal information* means showing, sending or giving some other organization, government or individual the personal information in question. To continue the example above, providing the customer's name and address when lawfully requested by the Canada Revenue Agency would be a valid disclosure of *personal information*.

Disclosing *personal information* without consent

PIPA allows your organization to disclose *personal information* about an individual without consent in certain situations (section 18). With one exception, the situations listed in section 18 are the same as those in Guideline 3 (collecting *personal information* without consent). The exception is that section 18 does not allow disclosure of *personal information* for credit reporting purposes.

PIPA allows the following additional 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 (section 18(1)(h)).
- 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* (section 18(1)(i)). For example, an organization may disclose *personal information* without consent when a court order is served on the 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 (section 18(1)(j)). For example, disclosing *personal information* to the WorkSafe BC to carry out an investigation of a workplace accident.
- When 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 (section 18(1)(k)). For 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 (section 18(1)(l)).
- When the disclosure is to a lawyer representing your organization (section 18(1)(m)).
- When the disclosure is to an archival institution if the collection of the *personal information* is reasonable for research or archival purposes (section 18(1)(n)).

Disclosing information from or on behalf of another organization

PIPA allows you to disclose *personal information* from or on behalf of another organization without consent in order to carry out work for that organization if the individual has already consented to the disclosure of the personal information and provided that the disclosure is consistent with the purpose for which the *personal information* was originally collected (section 18(2)).

An organization may also disclose *personal information* to another organization, individual or *public body* if the information was collected for the purpose of providing legal services or other services to a third party and the disclosure is necessary (section 18(4)).

Disclosing *personal information* collected before January 1, 2004

PIPA allows your organization to disclose, without consent, *personal information* collected before January 1, 2004 for purposes that are reasonable and to fulfill the purposes for which the *personal information* was originally collected. If 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 must obtain consent for that new disclosure unless PIPA authorizes otherwise. 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*.

6 Follow special rules for employee *personal information*

Highlights: *Employee personal information*

PIPA has special rules for *employee personal information*.

Volunteers are defined as your *employees* under PIPA.

Whether or not your organization needs consent, your collection, use and disclosure of *employee personal information* must be reasonable for the purpose of starting, managing or ending an employment relationship.

If you are authorized to collect, use or disclose *employee personal information* without consent, you must notify the *employee* that you are doing so.

If you make a decision using *employee personal information* that directly affects an *employee*, you must keep the information you used for that decision for one year.

What is *employee* personal information?

PIPA defines the terms *employee*, *employee personal information*, *contact information* and *work product information* (section 1). 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 volunteers.

To qualify as *employee personal information*, the information must be collected, used or disclosed for the purposes reasonably required to establish, manage or terminate an employment relationship, and must be collected solely for those purposes (Order P06-04).

PIPA does not define managing, however, managing personnel means human resource management activities relating to the duties and responsibilities of *employees*, not contractors or consultants. The type of records collected, used or disclosed for the purposes of establishing, managing and terminating an employment relationship would normally include personnel records such as letters of application, results of interviews, personal references, performance evaluations and letters of resignation or termination. That is, the type of information collected and retained by human resources officers and an individual's supervisor (Order P10-03).

Employee personal information does not include business *contact information* or *work product information*. These mean the following:

- *Contact information* refers to information used to contact an individual at a place for business, including the individual's name, position or title, and the individual's business telephone number, address, e-mail and fax number.

EXAMPLES

EMPLOYEE PERSONAL INFORMATION

» 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 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 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 how long his absence for medical reasons will be. 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.

EXAMPLES

DISCLOSING EMPLOYEE PERSONAL INFORMATION

» Celia makes a complaint to WorkSafe BC about the unsanitary conditions at her work. When WorkSafe BC investigates, Celia's manager, Victor, tells her co-workers that Celia made a complaint. This is not an authorized disclosure for the purposes of managing Victor's employment relationship with Celia (Order P06-03).

- *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 or employees. For example, a work report prepared and signed by an *employee* would be that employee's *work product information*. However, if the report contained information about other employees, that would be the *personal information* of the other employees.

Collecting, using and disclosing *employee personal information* without consent

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.

Your organization can collect, use and disclose *employee personal information* without consent in the following circumstances:

- Where PIPA allows the collection, use and disclosure of *personal information* without consent (sections 12, 15 and 18),[11] or
- Where the collection, use or disclosure is for reasonable purposes related to managing or recruiting personnel, provided that you have given the *employee* prior notification that your organization is collecting, using or disclosing his or her *employee personal information* and your purpose for doing so (sections 13, 16 and 19).

Using *employee personal information* to make a decision about an employee

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 (section 35(1)). Otherwise, your organization must destroy *documents* containing *employee personal information* once the purpose for which the *employee personal information* was collected is no longer served by keeping it and retention is not necessary for legal or business purposes (section 35(2)).

11 See Guideline 3 for collection of personal information without consent.

7 Follow the special rules for business transactions

Highlights: Business transactions

When buying or selling a business, your organization may collect, use and disclose *personal information* without consent under very limited circumstances relating only to the business transaction.

You may not disclose *personal information* without consent in *business transactions* where the primary objective of the transaction is the sale or purchase of *personal information*.

Once the transaction has been completed, the organization that received the *personal information* may continue to use and disclose that information for business purposes provided that the organization properly notifies individuals whose *personal information* was disclosed as part of the transaction.

If the transaction does not proceed, the organization that has received the *personal information* must destroy it or return it to the other party to the transaction.

What is a business transaction?

A *business transaction* means 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 (section 20(1)). 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).

Collecting, using and disclosing *personal information* without consent

The following rules do not apply where *personal information* is the only asset being purchased, sold, leased or otherwise acquired. If *personal information* is the central asset that is subject to the business transaction you must obtain consent (section 20(7)).

You may collect, use and disclose *personal information* of employees, customers, directors, officers and shareholders of the organization without consent to a prospective party, for the purpose of deciding whether to proceed with a *business transaction*, on the following conditions:

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 (section 20(2)).

EXAMPLES

RULES FOR BUSINESS TRANSACTIONS

» 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 long 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 the customers and employees are notified that the transaction has taken place and that their personal information has been disclosed. If the deal does not proceed, ABC must return the personal information to XZY or destroy it.

EXAMPLES

RULES FOR BUSINESS TRANSACTIONS

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

The company decides to sell the now lucrative dating service data-base. Since client personal information is the only asset involved in the business transaction, the owners must first obtain the consent of their dating service customers before the data-base can be disclosed to a potential or actual purchaser.

If the transaction goes 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 following conditions:

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

2. The organization may only disclose *personal information* relating directly to the part of the organization or its business assets covered by the business transaction (carrying on the business), and

3. All employees, customers, directors, officers and shareholders whose *personal information* is disclosed must be notified that the business transaction has taken place and that the *personal information* about them has been disclosed (section 20(3)).

If the transaction does not go ahead, the organization that received the information for the transaction must return or destroy it (section 20(6)).

Tip For Best Practice:

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

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

Highlights: Access

Individuals have the right to access their own *personal information* held by your organization, to know how you use their *personal information*, and to know to whom and when you disclosed their *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*.

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

PIPA regulations list who may act for another individual in some cases, for example, a parent on behalf of a young child.

Your organization may charge individuals a minimal fee for access to their *personal information*, but must not charge employees for access to their *employee personal information*.

An individual's right of access to his or her *personal information*

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

An individual who makes a request is called an *applicant* (section 25). A request for access by an *applicant* must be in writing and must give enough information so the organization can find the information with reasonable effort (section 27). 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.

Unless your organization does not have *personal information* about the applicant or PIPA allows or requires you to refuse access, you must provide the applicant with the following upon request:

- access to his or her *personal information*,
- information on how your organization has used or is using his or her *personal information*, and
- the names of the individuals and organizations your organization has disclosed his or her information to and in which situations you disclose his or her *personal information* (section 23).

If an applicant's *personal information* is in electronic form, the *applicant* has the option to receive a copy of the information in electronic or paper form.

Who can request *personal information*

The PIPA Regulations set out who has the right to access *personal information* for minors or deceased individuals. In addition, an *applicant's* legal representative, as defined in the Regulations, may act for that individual under PIPA.

Duty to assist *applicants*

An organization has a duty to assist *applicants*. This means that your organization must do the following:

- make a reasonable effort to help an *applicant* seeking access to her or his own *personal information*,
- respond to an *applicant* as accurately and completely as is reasonably possible, and
- unless PIPA says otherwise, provide the *applicant* with the *personal information* requested or, if the *personal information* cannot be reasonably provided, an opportunity to view it (section 28).

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

You must respond to an access request within 30 business days after your organization received the request (section 29). You can take up to an extra 30 business days to respond in the following circumstances:

- The *applicant* does not give enough information to allow you to find the requested *personal information* or document.
- 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.
- You have to consult with another organization or *public body* to decide if access should be given (section 31(1)).

You may also ask the *Commissioner* to authorize a period longer than 30 business days to respond to the *applicant* (section 31(1)).

If you take extra time to respond, you must tell the *applicant* the following information 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(2)).

The *applicant* can complain to the *Commissioner* if you do not respond to the applicant in the required time.

What must your response to an access request say?

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

- whether you have a document that contains the individual's *personal information*,
- whether you will give access to all or part of the *personal information*, and
- if access will be given, where, when and how it will be given (sections 23 and 28)

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

- the reasons for refusing access and the sections of PIPA that allow or require you to refuse 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 may refuse access in a number of situations:

- 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) (section 23(3)(a)).
- 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 (section 23(3)(b)).
- When the *personal information* was collected for an *investigation* or *proceeding* that has not concluded (including any appeals) (section 23(3)(c)).

EXAMPLES

ACCESS REQUESTS

» Joe is an employee of ABC Corporation. Joe and ABC Corporation are involved in a dispute regarding allegations against Joe that he has been bullying his co-workers. Joe asks ABC Corporation to provide him with his personnel file. ABC Corporation reviewed Joe's file and refused to give him access to the following personal information in his file:

- information prepared by company lawyers about the bullying dispute and the grievance Joe filed (information protected by solicitor-client privilege), and
- information about ABC Corporation's ongoing investigation into the bullying allegations against Joe (information collected for the investigation).

EXAMPLES

ACCESS REQUESTS

» 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 the notes made by the human resources consultant.

The company reviews the consultant's notes and asks the three employees if they will consent to the release of their opinions about Mary, including their identities. One employee gives her consent but the other two employees who have had an ongoing feud with Mary do not give their consent. Mary receives the notes containing the opinions of the employee who consented to disclosure, including information that may reveal the identity of that employee. The company severs the names and any information that would reveal the identities of the two other employees who did not give consent from the notes. Any information in the notes about Mary that has not been severed is disclosed to her, with an explanation why the information was severed and the provision of PIPA that required the severing.

- 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 before the request was made (section 23(3.1)).
- When the information was collected by a mediator or arbitrator in conducting a mediation or arbitration if the mediator or arbitrator was appointed under a collective agreement, a law or by a court (section 23(3)(e)).
- When the information is in a document that is subject to a solicitor's lien (section 23(3)(f)).

When must your organization refuse to give someone their *personal information*?

Your organization must refuse access to an individual's *personal information* in the following circumstances:

- The disclosure could reasonably be expected to threaten the safety or physical or mental health of another individual (section 23(4)(a)).
- The disclosure could reasonably be expected to cause immediate or serious harm to the safety or to the physical or mental health of the individual who made the request (section 23(4)(b)).
- The disclosure would reveal *personal information* about another individual (section 23(4)(c)).
- The disclosure would reveal the identity of the person who provided you with the *applicant's personal information*, and that person does not consent to the disclosure of his or her identity (section 23(4)(d)). For example, an *applicant* might be able to determine a person's identity based on his or her handwriting, special knowledge or presence at an incident involving the *applicant*.

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 *applicant* (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.

Charging 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)).

Minimal means that what you charge must cover only the actual costs you incurred in producing the record. Typically, a minimal charge would include costs associated with locating, retrieving and producing a *document*, preparing it for disclosure, shipping it, and providing a copy of the *document*. Charging for services not required to create documents, such as the creation of an index for the *documents*, is not a minimal charge (Order P10-03).

If the *applicant's* request only involves a few pages of documents that are easy to locate, this fee should be small. If the request involves a large number of *documents* and it takes a long time to locate and produce them, the fee could be larger, but you are still limited to charging a minimal fee for access to *personal information*. Your fee must never generate any profit (Orders P08-02, P08-03 and P10-03).

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

When charging fees, 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)).

Tip 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.
- Keep your access fees to actual, out-of-pocket costs, such as copying or postage.

EXAMPLES

CHARGING FEES FOR ACCESS

» Raj asks his doctor for clinical records, including any medical reports. The doctor charges him a professional fee for the copies plus photocopying costs of $1.00 per page. The professional rate the doctor charged is not minimal because it exceeds the cost of access and includes a profit component (Order P08-03).

9 Follow the special rules for correcting personal information

EXAMPLES

CORRECTION REQUESTS

» 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 notify the organizations that it disclosed this information to within the preceding year of this change.

» 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 him 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.

Highlights: Corrections

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

If you decide there is no error or omission, you must annotate the *personal information* with the *applicant's* 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.

If you decide to correct any errors or omissions, you must provide your corrections to any other organizations you disclosed the incorrect information to in the past year.

Requests to correct *personal information*

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.

An individual who believes that 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(1)).

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 (section 27). Your organization cannot charge a fee for handling requests for correction (section 32(2)).

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 you must correct that *personal information* as soon as possible. In addition, your organization must send the corrected *personal information* to every organization that your organization disclosed the wrong information to during the year before the correction date (section 24(2)).

If your organization decides to not make the requested correction, you must annotate the *personal information* so that others reading the information will see what the applicant believed to be the correct or missing information (section 24(3)). Annotations are often made by attaching a copy of the correction request to the personal information.

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* (section 24(4)).

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

Highlights: Accuracy, protection and retention

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

If your organization is likely to use *personal information* to make a decision that will affect 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 is reasonable to carry out business or legal purposes. Use care in disposing of or destroying *personal information*.

If you use an individual's *personal information* to make a decision that directly affects that individual, you must retain that information for at least one year so the individual has a reasonable opportunity to access it.

Accuracy and completeness of *personal information*

Your organization must make a reasonable effort to ensure that *personal information* collected by or on behalf of your organization is accurate and complete. This is essential 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 if your organization is likely to disclose the *personal information* to another organization (section 33).

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.

One way to decide if you need to update *personal information* is to consider whether your use or disclosure of an individual's *personal information* 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.

Protecting *personal information*

Your organization must use reasonable physical, administrative and technical safeguards to protect *personal information* from unauthorized access, collection, use, disclosure, copying, modification or disposal, or similar risks (section 34). For example, your safeguards should protect *personal information* from the following:

- someone being able to read, 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*.

Factors to consider when implementing appropriate safeguards should include the sensitivity of the *personal information*, the likelihood of a privacy breach, the harm caused if there were a privacy breach, the practices commonly used by other organizations, the type of record containing the *personal information*, the likelihood of criminal activity or intentional wrongdoing, and the cost of the security measures (Order P06-04). 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.

The following are some examples of safeguards you can employ to protect *personal information* in your custody:

Physical safeguards

- Locking file cabinets and areas where files are stored when no one is there.
- Restricting employee access to storage areas or filing cabinets.
- Clearing files and documents containing *personal information* off your desk at the end of the day.
- Shredding papers containing *personal information* rather than just placing them in a garbage can or recycling bin.
- Destroying computer hard drives that contain *personal information* before you discard them.

Administrative safeguards

- Regularly training and reminding employees so that they know your privacy policies and PIPA's requirements for protecting *personal information*, and the disciplinary consequences of not following them.
- Having employees enter into confidentiality agreements regarding *personal information*.
- Ensuring that *personal information*, especially sensitive information, is accessible only to those employees who need to know the information.
- Using cover sheets when faxing *personal information* and establishing procedures for ensuring only the authorized recipient has received the fax.
- Conducting regular privacy audits to ensure employee compliance with your privacy policies.
- Implementing role-based access to systems so that employees are only able to access *personal information* they need to perform their duties.

Technical safeguards

- Positioning computer monitors so that *personal information* displayed on them cannot be seen by unauthorized personnel or by visitors.
- Using password-protected computer screensavers so unauthorized personnel or visitors cannot see *personal information*.
- Ensuring your computers and network are secure from intrusion by using firewalls, intrusion detection software, antivirus software, and by encrypting *personal information* .
- Using strong and secure passwords to make sure that only authorized employees have access to computer storage devices or to the network. Changing those passwords on a regular basis.
- Encrypting *personal information* stored on mobile electronic devices such as laptops and USB flash drives.
- Securely wiping all *personal information* from hard drives before you discard them, sell them or donate them. Deleted files can be recovered while wiped files cannot. Wiping may require specialized software. If you are unsure, the most secure method is to physically destroy hard drives.
- Modifying equipment and software so credit card or debit numbers are removed or truncated from receipts.

Retaining *personal information*

Your organization must destroy documents containing *personal information* or make the information anonymous as soon as it is reasonable to assume the following:

- the purpose for which the *personal information* was collected is no longer being served by keeping the *personal information*, and
- it is no longer necessary to keep the *personal information* for legal or business purposes (section 35(2)).

However, 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(1)).

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 PIPA.

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?

Highlights: Enforcement

Individuals may complain to the Office of the Information and Privacy Commissioner if they believe that an organization has not met its obligations under PIPA with respect to their *personal information*.

The OIPC can also initiate investigations if the *Commissioner* is satisfied that there are reasonable grounds to believe an organization is not complying with PIPA.

When an individual initiates a complaint, the OIPC will generally require the individual to first try to find a solution directly with the organization without OIPC involvement. If the OIPC accepts an individual's complaint, an OIPC investigator will attempt to mediate a settlement.

Under limited circumstances, the OIPC may hold a formal inquiry if a complaint does not settle. The OIPC has a number of powers, including the ability to compel testimony, order production of evidence and enter premises.

The OIPC can also 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* within that 30-day period.

There are various offences under PIPA and fines of up to $10,000 for individuals and up to $100,000 for organizations.

The *Commissioner's* powers under PIPA

The *Commissioner* has the power to review the actions and decisions of organizations under PIPA. For example, the *Commissioner* can review or investigate any of the following:

- An organization's decision, action or failure to act respecting a request for access to or correction of *personal information.*
- A complaint that *personal information* has been improperly collected, used or disclosed.
- A complaint that an organization has not properly assisted an *applicant* with a request, has taken longer than authorized under PIPA, or has charged an unreasonable fee (section 36(2)).

The *Commissioner* also has the power to initiate audits and investigations where there are reasonable grounds to believe an organization is not compliant with PIPA (section 36(1)(a)).

In responding to a complaint, the *Commissioner* can do any of the following:

- Send the individual to another 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).

EXAMPLES

HANDLING COMPLAINTS

» Trevor 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 realized that Company Y had a copy of his personnel file during a meeting about the incident.

Trevor complains to the OIPC that Company X disclosed his *personal information* to Company Y improperly. Before the OIPC opens a file, it will ask Trevor if he has tried to resolve his complaint with Company X's privacy officer. If he has not, he may be asked to do that. If he has, the OIPC may open a file on the complaint. If a file is opened, an investigator from the OIPC will contact Trevor and Company X to investigate the complaint and, if possible, find a solution that satisfies both parties. If this is not possible, the investigator may issue formal findings and/or recommendations as necessary. In limited circumstances, the complaint may go to an inquiry.

- Hold an inquiry (a hearing) (section 50). An inquiry can be held in writing or in person, but is almost always held in writing.

Typically, the OIPC will address a complaint through an investigation and mediation (section 49). Complaints rarely go to an inquiry (a hearing). The OIPC has a number of powers for the purposes of investigation or inquiry, including the ability to compel testimony, order production of evidence and enter premises (section 38(1)).

If a person reports a contravention or a possible contravention of PIPA to the OIPC, the OIPC may keep the name of the "whistleblower" confidential (section 55).

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 may involve the OIPC referring would-be *complainants* back to the organization's privacy officer if they have not already gone there. There may be situations where the OIPC will not refer *complainants* back to the organization, for example, where an employee or customer may feel threatened by someone at the organization.

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 about complaint procedures. Finally, your organization should investigate all complaints and, if a complaint is found to be justified, take appropriate measures (including, if necessary, amending your policies and practices).

Duty to comply with Commissioner's orders

The *Commissioner* can issue binding orders (section 52). Your organization must comply with an *order* no later than 30 business days from the day the *order* is given unless you apply to the BC Supreme Court for judicial review of the *order* (section 53). You have 30 business days after the day on which you received a copy of the *order* to seek judicial review. The *order* is then stayed (stopped) until the BC Supreme Court makes its decision.

Employee "whistleblowers"

PIPA provides protection for an employee who, in good faith, reports contraventions of PIPA to the OIPC, acts in a way to avoid or prevent a contravention of PIPA, or refuses to do anything he or she believes contravenes PIPA. If any of these situations arise, the employee, or "whistleblower," is protected from any punitive action taken by an organization against him or her, such as suspension or dismissal (section 54).

If an employee or any other person reports a contravention or a possible contravention to the OIPC, the OIPC may keep the name of the "whistleblower" confidential (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 the intent to evade a request for access to the *personal information.*
- Obstruct or mislead the *Commissioner* or one of his or her 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)).

If an offence is committed, PIPA provides for fines of up to $10,000 for individuals and up to $100,000 for organizations for offences committed (section 56(2)).

An individual or organization cannot be prosecuted for an offence against PIPA or any other Act for complying with a requirement *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 appealed 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

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

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 with authority under PIPA (section 1).

Contact information means information to enable an individual at a place of business to be contacted and includes the name, position, 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. Control can take a number of forms even if *personal information* isn't in an organization's custody.

Disclosure includes the showing, sending or giving of *personal information* to some other organization, public body, 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 (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)

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

Investigation means an investigation related to any of the following

- 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, if the investigation is based on the reasonable 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, and can also refer to activities such as payroll and succession planning. It does not apply to the management of contractors or consultants.

Order means a decision of the Information and Privacy Commissioner.

Organization includes the following:

- a person
- a corporation, including a strata corporation,
- a society,
- a cooperative association, including a housing co-op,
- a partnership,
- a doctor's office,
- a church or other religious organization,
- a charity,
- a sports club,
- a political party,
- 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 set up by an individual for the benefit of friends or family) (section 1).

Personal information means information about an identifiable individual and includes employee personal information. *Personal information* excludes contact information or *work product information* (section 1).

PIPA means the BC *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 any of the following:

- 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 provincial police force, an administrative tribunal, a regional health authority, a local government, a public school board, public post-secondary institution or a professional regulatory body (section 1).

Work product information means personal information prepared or collected 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 was not involved with preparing or collecting the *personal information* (section 1).

Office of the
Information & Privacy
Commissioner
for British Columbia

Protecting privacy. Promoting transparency.

Office of the Information and Privacy Commissioner for British Columbia

PO Box 9038, Stn. Prov. Govt. Victoria, BC V8W 9A4 | Telephone: 250.387.5629 | Toll free in B.C. 1.800.663.7867
E-mail: info@oipc.bc.ca | www.oipc.bc.ca