



Office of the Information  
and Privacy Commissioner

Suite 2460, 801 – 6<sup>th</sup> Ave. SW  
Calgary, Alberta  
T2P 3W2  
Phone: (403) 297-2728  
Fax: (403) 297-2711  
Toll Free: 1-888-878-4044  
Web: [www.oipc.ab.ca](http://www.oipc.ab.ca)  
Email: [generalinfo@oipc.ab.ca](mailto:generalinfo@oipc.ab.ca)

***Personal Information Protection Act (PIPA)***  
**PIPA ADVISORY #7**  
**ACCESS REQUESTS UNDER PIPA: EXCEPTIONS TO ACCESS**

This document was prepared to help organizations implement the *Personal Information Protection Act* (“PIPA” or “the Act”). This document is an administrative tool intended to assist in understanding the Act. It is not intended as, nor is it a substitute for, legal advice. For the exact wording and interpretation of PIPA, please read the Act in its entirety. This Advisory is not binding on the Information and Privacy Commissioner of Alberta (OIPC).

**Contents**

**[Introduction](#)**

**[Exceptions to access](#)**

**[Discretionary exceptions](#)**

**[Legal privilege](#)**

**[Confidential commercial information](#)**

**[Investigation or legal proceeding](#)**

**[Information may no longer be provided](#)**

**[Mediation and/or arbitration](#)**

**[Prosecutorial discretion](#)**

**[Mandatory exceptions](#)**

**[Threat to life or security](#)**

**[Reveals personal information](#)**

**[Confidential opinions](#)**

**[Severing records](#)**

**[Other resources](#)**

**Introduction**

The *Personal Information Protection Act* (“PIPA” or “the Act”) provides individuals with a right to access their own personal information contained in a record in an organization’s custody or control. However, this right of access is not absolute. In responding to a request for access to personal information, PIPA may authorize or require an organization to refuse access to personal information.

This Advisory is part of a series developed by the OIPC to assist organizations in handling and responding to

requests for access. It provides an overview of how to apply discretionary and mandatory exceptions to access.

**Exceptions to access**

Sections 24(2) and (3) of the PIPA describe the circumstances under which an organization **must** or **may** refuse to provide access to personal information.

The organization may have to review the records containing requested personal information on a document by document, or line-by-line basis in order to determine whether exceptions to access may be applied.

An organization must state which exceptions do apply to the personal information.

**NOTE:** An organization may only refuse to provide an individual with access to his or her own personal information if one or more of the exceptions to access outlined in sections 24(2) and (3) of the Act apply. Otherwise, the organization **must** provide access to the personal information.

An organization may not refuse access on the basis the applicant already has the record, or it would be embarrassing to the organization to release the information.

Should there be an inquiry into an organization's decision to partially or completely refuse access to personal information, section 51 of the PIPA states that it is the organization's responsibility to establish (to the Commissioner's satisfaction) that the individual has no right of access.

**TIP:** Organizations should be guided by the principle that the purpose of the Act is to provide an individual with access to his or her own personal information whenever possible. Organizations should adopt a policy of openness that "defaults" to openness, minimizing refusal to access requests.

**Discretionary exceptions**

Section 24(2) of the PIPA identifies the circumstances under which an organization **may** refuse to provide

access to personal information. These exceptions are “discretionary” – the organization has the **option** to refuse access to the information.

Discretionary exceptions to access are intended to be applied document by document. An organization must not replace the exercise of discretion with a blanket policy that information will not be released simply because it can be withheld under one or more discretionary exceptions.

Exercising discretion involves looking at all relevant factors in order to make a decision about providing access to the personal information. For example, the organization might need to consider:

- the general purpose of the legislation, which is to ensure individuals have a right of access to their own personal information
- whether the individual originally provided the information to the organization
- whether some personal information must be severed from the record and the applicant provided with access to the remainder
- the organization’s practices regarding release of similar types of records
- the age of the record

If the applicant requests that the OIPC review an organization’s decision to refuse access on the basis of a discretionary exception, the organization should be prepared to demonstrate how it exercised its discretion.

**TIP:** If an organization decides to exercise discretion in favor of releasing a record protected by legal privilege, for example, the organization may wish to first consult with its legal counsel.

**Legal  
privilege  
s. 24(2)(a)**

Section 24(2)(a) of the PIPA allows an organization to refuse to provide access to personal information if the information is protected by legal privilege.

Legal privilege has been addressed in a number of Orders issued by the Commissioner under the

*Freedom of Information and Protection of Privacy Act* (FOIP), and in the common law. In the event the OIPC is asked to review an organization's decision to refuse access based on this exception, the organization may be required to specify the privilege that applies (for example, solicitor-client privilege, litigation privilege, etc.) and may be asked to provide evidence regarding the particular type of privilege claimed.

For example, if the organization is claiming that **solicitor-client privilege** applies to personal information contained in a record, the organization must be able to demonstrate that the record meets a criterion that is similar to that set out in FOIP Order [96-017](#). For example, the organization may be required to show that each document is:

- a communication between solicitor and client
- entailing the seeking or giving of legal advice, and
- which is intended to be confidential by the parties.

If the organization is claiming **litigation** privilege applies, it may be required to demonstrate that each record meets criteria similar to that set out in paragraphs 101-104 of FOIP order [97-009](#) as follows:

- the record is a third party communication, such as that between a solicitor and a third party to assist in giving legal advice
- the maker of the document or person under whose authority the document was made must have intended the document to be confidential, and
- the "dominant purpose" for which the document was prepared must be to submit it to a legal advisor for advice and use in existing or contemplated litigation.

If legal privilege is accepted as applying to a document, or a portion of it, the organization is not required to sever the record, but instead may refuse access to the entire document.

**Example:** An employee requests access to all records about him held by his employer. The requested records included a memo from the organization's

legal counsel to a Human Resources (HR) Manager advising as to the legal implications of terminating the employee.

The organization refuses to provide the individual with access to the memo, claiming solicitor-client privilege applies as the record involves a confidential communication of legal advice between the organization (HR Manager) and its legal counsel.

**Confidential commercial information s. 24(2)(b)**

Organizations have the discretion to refuse to provide access to personal information if disclosure would reveal confidential information of a commercial nature, and it is not unreasonable to withhold that information.

**Example:** Mr. Smith submits a request for access to his personal information held by a financial investment company. The organization responds that they will provide access to only a portion of one of the documents, saying that the excepted information includes a confidential formula used to target investment opportunities in the market.

Upon review of the organization's decision to refuse access, the OIPC determined that the formula was confidential commercial information. As a result, the organization was able to sever this information from the record, and provide access to the remainder.

**Investigation or legal proceeding s. 24(2)(c)**

Organizations may refuse to provide access to personal information collected for an investigation or legal proceeding.

An "investigation" is defined in section 1(f) of the PIPA to mean an investigation related to:

- a breach of an agreement
- a contravention of an enactment of Alberta or Canada or of
- another province of Canada, or
- circumstances or conduct that may result in a remedy or relief being available at law.

The breach, contravention, circumstances or conduct must have occurred, or must be likely to occur, and it must be reasonable to conduct an investigation.

**Example:** An employee requests that an organization provide him with records related to an internal investigation into his conduct. The organization refuses to provide access to the information, saying the records were collected for an investigation of suspected theft of computer equipment.

**TIP:** For more information on determining whether information has been collected for an investigation, see [Information Sheet 2: Investigations](#) produced by Alberta Government Services, Access and Privacy Branch, available at [www.pipa.gov.ab.ca](http://www.pipa.gov.ab.ca).

A “legal proceeding” is defined in section 1(g) of the PIPA to be a civil, criminal or administrative proceeding related to

- a breach of an agreement
- a contravention of an enactment of Alberta or Canada or of
- another province of Canada , or
- a remedy available at law.

**Example:** Printing Ltd. sued Joe Johnson for breach of a confidentiality agreement. In preparing for trial, the organization’s legal counsel collected information about Mr. Johnson from various sources, including his neighbours.

Mr. Johnson requested access to all personal information about himself. In its response to Mr. Johnson, the organization refused to provide access, saying the information was collected for a legal proceeding.

Organizations should be prepared to demonstrate that the circumstances that required the collection of the personal information meet the definition of an investigation or legal proceeding under the Act.

**Information  
may no longer  
be provided  
s. 24(2)(d)**

There are situations where an organization may refuse to provide access to personal information if disclosure might result in that type of information no longer being provided to the organization, when it is reasonable that that type of information would be provided.

**Example:** Iva Job requested access to her personnel file held by Gotta Work Inc.

The records included three references from her former employers. The references were provided with the understanding that the evaluations of Ms. Job would remain confidential. The organization stated that referees may refuse to provide this kind of information if it was turned over to the individual.

In its response to Ms. Job's request for access, the organization refused to provide the notes of specific references. Even if the names of the referees were removed, the content of the evaluations would identify them.

Organizations should be prepared to show why providing access to the information might result in it no longer being provided, and why it is reasonable that it be provided.

**Mediation  
and/or  
arbitration  
s. 24(2)(e)**

Under section 24(2)(e) of the PIPA, an organization may refuse to provide access to personal information collected by a mediator or arbitrator, or created in the process of a mediation or arbitration where the mediator or arbitrator has been appointed under an agreement, enactment, or by a court.

**Example:** During a court appointed mediation with his employer, Dennis Menace was offered a settlement.

When mediation ended unsuccessfully, Mr. Menace requested a copy of the settlement details under PIPA. The organization refused to provide access to the information claiming that it was created during the conduct of the mediation proceeding.

**Prosecutorial discretion**  
**s. 24(2)(f)**

An organization may refuse to provide access to personal information if it relates to, or may be used in, the exercise of prosecutorial discretion.

Prosecutorial discretion refers to any discretionary decision made by a prosecutor in matters within his authority related to the prosecution of offences. The core elements are discretion to:

- bring the prosecution of a charge
- enter a stay of proceedings
- accept a guilty plea to a lesser charge
- withdraw from criminal proceedings altogether
- take control of a private prosecution<sup>1</sup>

**Mandatory exceptions**

Section 24(3) of the PIPA states the circumstances under which an organization **shall not** provide access to personal information. These exceptions are “mandatory” – the organization shall not provide access where the exception applies.

A line-by-line review of each record should be conducted to ensure that information that must be excepted from disclosure is not released. This can be a lengthy procedure, but it must be done carefully and thoroughly to avoid contravening the Act. Providing reasons related to a specific section of the Act will provide clarity and perhaps avoid the possibility of unnecessary misunderstanding.

**TIP:** Even where an organization is able to reasonably sever an individual’s name from a record, organizations should carefully review the records to ensure that the context or circumstances do not reveal additional information that must not be released.

---

<sup>1</sup> *Krieger v. Law Society of Alberta* (2002), 217 D.L.R. (4<sup>th</sup>) 513 (S.C.C.).

**Threat to life  
or security  
s. 24(3)(a)**

Section 24(3)(a) of the Act requires that an organization shall refuse to provide access to personal information if the disclosure could reasonably be expected to threaten the life or security of someone else.

In applying this exception, an organization must be able to demonstrate that a threat exists. FOIP Orders [96-003](#) and [96-004](#) present criteria that may assist in determining the criteria for harm.

The guiding criteria set out in these Orders allow that an organization be required to show:

- there is a reasonable expectation of probable harm
- the harm must constitute damage or detriment and not mere inconvenience; and
- there must be a causal connection between disclosure and the anticipated harm.

All three elements are likely to be required in order for an organization to successfully show that release of the information could threaten the life or security of another person.

**Reveals personal  
information  
s. 24(3)(b)**

Section 24(3)(b) of the PIPA requires an organization to refuse to provide access to personal information if doing so would reveal personal information about another individual.

The Act gives an individual a right to access his or her own personal information. It does not allow an individual to access someone else's personal information.

**Example:** Dick Tracy submitted a request to his local video store, You Rent It, for access to his personal information.

In its response to Mr. Tracy, the organization provided access to details of his rental history, phone number and home address, but removed his spouse's rental history.

**Note:**

“Personal information of another individual” does not include “business contact information,” defined in section 1(a) of the Act to mean *“an individual’s name, position name or title, business telephone number, business address, business e-mail, business fax number and other similar business information.”*

The Act does not apply to “business contact information,” when it is collected, used or disclosed for the purposes of contacting an individual in his or her capacity as an employee or official of an organization.

Section 24(3)(b) of the Act does NOT require an organization to refuse to disclose this information.

**Example:** Donald Duck submitted a request to his grocery store for access to his personal information. Some of the responsive records were emails between Mr. Duck and various store employees. In providing copies of the emails, the organization removed the names of the employees, citing section 24(3)(b).

Asked to review the organization’s decision, the OIPC found that the name of an employees acting in the course of his or her employment is not personal information. The organization provided the records to Mr. Duck without removing employee names, saving a substantial amount of time that would have been spent reviewing and severing the records.

**Confidential opinions  
s. 24(3)(c)**

An organization **shall not** provide access to personal information if to do so would reveal the identity of someone who has, in confidence, provided an opinion about someone else, and that person does not consent to the disclosure of his or her identity.

In order for this exception to apply, the opinion must have been provided in confidence (either implicitly or explicitly), and the person providing it should have the opportunity to consent to the disclosure. Where the organization can reasonably sever the individual’s identity, it must do so.

**Example:** Jane Doe requests access to all records containing her personal information. On reviewing the records, the organization's privacy officer notes there is a letter from a customer who filed a complaint against Jane. The writer had an expectation of confidentiality and stated her opinion of Jane.

The privacy officer contacts the customer, who indicates she does not consent to the release of the complaint letter. As a result, the officer severs the customer's name, as well as additional information in the letter that would identify the customer. Jane is given access to the remainder of the record.

**TIP:** When responding to an applicant, organizations should take the time to explain the differences between discretionary and mandatory exceptions to access, and how the organization has applied them. In so doing, organizations may find fewer individuals requesting the OIPC review decisions about access.

## **Severing records**

After reviewing all records responsive to a request for access, an organization may decide that one or more exceptions to access apply to some or all of the personal information requested.

Depending on which exceptions these are, section 24(4) of the Act **requires** the organization to sever personal information from the record, in order to provide access to the remainder. The exceptions that require the record be severed are where disclosure of the personal information:

- would reveal confidential information of a commercial nature [section 24(2)(b)]
- could reasonably be expected to threaten the life or security of another individual [section 24(3)(a)]
- would reveal personal information about another individual [section 24(3)(b)]
- would reveal the identity of an individual provided a confidential opinion, and the individual providing the opinion does not consent to the disclosure of his or her identity [section 24(3)(c)]

Organizations are not required to sever personal information from records where any of the other exceptions to access may have been applied.

For more information on how to sever records, see PIPA Advisory #3 *Access Requests Under PIPA: Responding to a Request*.

**Other  
resources**

For an overview of the Act with examples and tips for incorporating good privacy practices, see [\*A Guide for Businesses and Organizations on the Personal Information Protection Act\*](#).

[\*The Personal Information Protection Act, A Summary for Organizations\*](#) summarizes the key obligations of organizations.

[\*Ten Steps to Implement PIPA\*](#) is a quick reference for organizations preparing for the Act.

Publications are available at the website of the Office of the Information and Privacy Commissioner ([www.oipc.ab.ca](http://www.oipc.ab.ca)).

Publications are also available online at the Alberta Government Services, Access and Privacy Branch website ([www.pipa.gov.ab.ca](http://www.pipa.gov.ab.ca)).

Visit the Queen's Printer website to view an online version of the Act ([www.qp.gov.ab.ca](http://www.qp.gov.ab.ca)).