OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
for
British Columbia

Tips for Organizations Responding to a Privacy Complaint under the *Personal Information Protection Act*

June 2004

Purpose of This Document

This document offers suggestions for organizations to refer to when investigating a privacy complaint mate to them under the Personal Information Protection Act ("PIPA").

These suggestions are for information only and do not constitute a decision or finding by the OIPC with respect to any matter within the jurisdiction of the Information and Privacy Commissioner under PIPA. The suggestions do not affect the powers, duties or functions of the Information and Privacy Commissioner regarding any complaint, investigation or other matter under or connected with the Act, respecting which the Information and Privacy Commissioner will keep an open mind. Responsibility for compliance with PIPA remains with each organization. Those responsible for access and privacy matters within each organization must at all times apply their best judgment in discharging the powers, duties and functions of the organization under PIPA.

Step 1: Clarify the complaint and whether PIPA applies

Try to clarify the specifics with the complainant:

- What do you believe occurred?
- What personal information is involved and what happened to it?
- When and where did the events occur?
- Which staff do you believe were involved and why do you believe they were involved?
- Do you have written or other evidence that the alleged incident occurred?

Determine if, on the face of it, the complaint concerns a contravention of the privacy protections set out in PIPA:

- Does the complaint involve "personal information" as defined in PIPA—"information about an identifiable individual" but not including "employee personal information" or "contact information".
- Does it involve "employee personal information", a special category of personal information defined in PIPA, to which special rules apply?

- Does it involve "contact information" or "work product information", two other special categories of personal information under PIPA, to which special rules apply?

- Is the complaint about an alleged improper collection, use, disclosure, retention, storage or disposal of information in a record about an identifiable individual by your organization?

- Is the complaint about a failure or refusal to correct or annotate information? (To be sure, refer to the specific definitions and sections of PIPA.)

If the complaint does not involve a contravention of PIPA, the complaint may be resolvable at this point, so jump to Step 3, Part B.

If there might have been improper action of some kind, continue through Steps 2 and 3.

Step 2: Gathering information and making findings

If you are unfamiliar with the department in your organization where the complaint originates, you may need to learn more about the department to fully understand the circumstances of the complaint.

For example, if the complaint concerns an alleged inappropriate collection or disclosure of medical information as part of an application for medical leave, you may need to find out how the medical leave application process works; what the employer normally needs to assess the application; what the employee is expected to provide in way of personal medical information; and what happens to it during the application approval process in order to determine if there was inappropriate conduct or action.

Therefore, be sure to:

- Ask staff in the relevant department to comment on the complaint and explain what happened. You may need to interview people and ask for written reports.

- Consider and verify the authority in PIPA or other legislation, if any, under which staff believed they were acting.

- Clarify why staff did what they did--e.g. were they following established policies or guidelines or another enactment?--and gather the details of any policies, guidelines or enactments that may apply.

To determine whether the incident did actually contravene a specific section of PIPA ask the following questions:

Is the complaint about the way the information was collected?

- How was the information collected—directly from the individual or indirectly from another source?
- Did your organization have the authority under section 12 of PIPA to collect the information without consent from a source other than the individual?
- Or did you get consent, orally or in writing, from the individual before you collected the information or from another source?
- At the time the consent was given, would the purpose for the collection be considered to be obvious to a reasonable person?
- In other cases, did you provide the individual with notice of the specific purposes of the collection and the option to refuse consent?
- Did you tell the individual before you collected her or his information of the ways in which the information would be used and to whom it would be disclosed?

Is the complaint about the type and amount of personal information that is being collected?

- What are the purposes for which your organization is collecting this information?
- Would a reasonable person consider the collection of this personal information appropriate in the circumstances?
- Is the collection of this information necessary for your organization to supply a product or service to the individual?
- Can you provide the service or product without this personal information?
- If you can, has your organization refused to supply the product or service because the personal information was not provided?

Is the complaint about the way your organization used personal information?

- Was the personal information used for the same purpose for which it was collected?
- Did your organization have the individual's consent to use his or her personal information for the specified purposes?
- If your organization used the information for a new purpose, did you get the consent of the individual first?
- Did your organization have the legal authority under section 15 of PIPA to use the personal information without the individual's consent?

Is the complaint about how your organization disclosed personal information?

- Did your organization have the legal authority to disclose the personal information without the individual's consent?
- Did your organization have the individual's consent to disclose his or her personal information?
- Was the information disclosed to fulfill the purpose for which it was collected?
- If the information was disclosed for a purpose different from that for which you collected it, did your organization have legal authority under section 18 of PIPA to disclose it for another purpose?

Is the complaint about protecting personal information from unauthorized access, collection, use, disclosure, copying, modification or disposal?

- Is the complaint about your organization's alleged failure to take appropriate security measures to protect personal information from risks such as, but not limited to, unauthorized access, collection, use, disclosure, copying, modification or disposal?
- What measures does your organization have in place to ensure personal information is protected against such risks?
- What measures does your organization have in place to ensure that only staff who truly need the personal information in question to carry out their job duties have access to that personal information?
- Does the complaint arise from a failure by staff to apply these measures and if so, what are the apparent causes of their failure to apply these measures?

Is the complaint about the accuracy or completeness of personal information?

- Is the complaint about your organization's alleged failure to make a reasonable effort to ensure that personal information you collect, use and disclose is "accurate and complete"?
- If so, is the personal information in question information that, when you collected it, you were likely to use to make a decision that affects the individual or is it information that, when you collected it, you were likely to disclose to another organization?
- What steps did your organization take to meet its obligation of accuracy and completeness?

Is the complaint about a request that your organization correct an error or omission in the individual's personal information?

- If your organization did not correct the personal information as requested, did you annotate the affected personal information with the correction that was requested but not made?
- If your organization corrected the personal information, did you inform any other organization to which the personal information was disclosed in the previous year of the correction and ask those organizations to correct the information?

Is the complaint about an individual's request for access to his or her personal information?

- Has your organization responded to the individual's request for access to her or his own personal information?
- If so, did you respond in time--is the complaint about your failure to respond within the time PIPA requires?
- Did PIPA authorize your organization to refuse to disclose some or all of the individual's personal information?
- Did PIPA require your organization to refuse to disclose some or all of the individual's personal information?

- If your organization refused the request for access, did you tell the applicant the reason for the refusal and the legal authority under PIPA on which your refusal was based?
- In your organization's response, did you tell the individual the name, position title, business address and business telephone number of an officer or employee of your organization who could answer any questions the individual might have about the refusal?
- Did your organization tell the individual she or he has a right to complain about the refusal to the Office of the Information and Privacy Commissioner ("OIPC") within 30 business days?
- If the individual has requested it, has your organization disclosed the ways in which it has use or disclosed the individual's personal information?
- If the individual has requested it, has your organization disclosed the names of other individuals and organizations to which your organization has disclosed the individual's personal information?

Is the complaint about a fee that was charged for an individual's request for access to her or his personal information?

- Is the fee "minimal", as PIPA requires, and could you satisfy the OIPC on any appeal that it was "reasonable"?
- Did your organization provide the individual with a written fee estimate?
- Has your organization explained what the fee covers?
- Is the fee a barrier to the access and, if it is, can you reduce it?

Is the complaint about your organization's openness and accountability?

- As section 5 of PIPA requires, has your organization developed policies and practices necessary for it to meet its obligations under PIPA?
- Are your policies and practices easy to understand?
- Are they publicly available?
- As section 5 of PIPA requires, has your organization developed a process to respond to complaints under PIPA?

Detail what improper collection, use, disclosure, retention, storage or disposal of recorded personal information by a organization employee took place for which there is no authority under PIPA. If a PIPA contravention did occur, determine the specific cause (such as a poorly drafted policy, an accident, lack of knowledge or a deliberate action).

Step 3: Taking Action

Parts A or B should be followed dependent on the outcome of the above assessment whether the complaint is (A) substantiated or (B) not substantiated.

A. The complaint is substantiated:

If you determine there was a contravention of PIPA, consider whether any immediate actions are required to rectify the situation, such as:

- Recovering information that was inappropriately disclosed;
- Destroying or returning information that was inappropriately collected; or
- Immediately halting a practice that is found to be privacy-invasive, like video surveillance.

Provide the complainant with an explanation, preferably in writing, detailing:

- What happened, including the specific personal information of the complainant that was involved;
- Your findings;
- A description of any action you have taken to prevent a recurrence; and
- Your recommendations to your organization for improvements to its policies or procedures to better protect the privacy of personal information and comply with PIPA.
- If applicable, that your organization will develop and implement and monitor a method of preventing recurrence of the privacy invasion over the long term by techniques such as:
    - training;
    - changing policies or practices;
    - limiting who can access personal information; and
    - implementing better security measures, like audit trails, encryption, and passwords.
- Wherever possible, ask the complainant to comments on your complaint investigation report. Ask for these comments by a certain date so that you will know whether or not the complainant wants to make his or her comments known to you and the organization.
- Tell the complainant he or she has the right to appeal your investigation findings to the Office of the Information and Privacy Commissioner ("OIPC") and give the complainant the OIPC's contact information.

B. The complaint cannot be substantiated

If there was no contravention, you still need to explain your findings to the complainant. Tell the complainant:

- If there was legislative authority for what your organization did, tell the complainant that PIPA or other legislation in conjunction with PIPA authorizes your organization to do what it did

- If no personal information was involved, tell the complainant that the incident did not involve "personal information" as defined by PIPA.

- Tell the complainant she or he may comment on your complaint investigation findings. Ask for these comments by a certain date, so you will know whether or not the complainant wants to make his or her comments known to you and the organization.

- Tell the complainant she or he has the right to appeal your investigation findings to the OIPC and give the complainant the OIPC's contact information.