



Personal Information Protection Act **An Overview for BC Association's Member Programs**

This document outlines the basic elements of BC's Personal Information Protection Act. It is for general information only and is not intended as legal advice. More detailed information and resources can be found by accessing the Ministry of Management Services website or contacting their hotline. (See Section H below for contact information.)

A. Background--why we wrote this bulletin

The need to protect the privacy of survivors of violence is a fundamental concern for community-based advocates and service providers. As we know, another serious concern is the need to guard against further violence.

Over the past 20 years in Canada, *Criminal Code* amendments and provincial and federal privacy laws, as well as high profile court cases, have raised the profile of privacy issues. In 1998, the BC Association of Specialized Victim Assistance and Counselling Programs produced the *Records Management Guidelines*. They are used extensively by programs across BC and beyond. They act as a framework to assist service providers to collect, manage and, in certain cases, release personal information about their clients.

On January 1st of this year, the *Personal Information Protection Act* (PIPA) came into force in BC. PIPA contains safeguards designed to protect the privacy of personal information which is collected by private businesses and non-profit organizations.

To assess the impact PIPA would have on Association members, we met with staff from the Ministry of Management Services and the Ministry of Public Safety and Solicitor General. We asked them to review the *Records Management Guidelines*. We were encouraged to learn that most of the PIPA principles are already addressed in the *Records Management Guidelines*.

This Bulletin provides a brief overview of PIPA and highlights a few areas where information management practices will need to be slightly adapted to reflect the new law.

Based on input from the Ministry of Management Services, the Association proposes that the *Records Management Guidelines*, combined with this Bulletin, serve as a blueprint for programs to help ensure their compliance with the current PIPA requirements.

Copies of the *Records Management Guidelines* can be downloaded from the BC Association of Specialized Victim Assistance and Counselling Program's website at: www.endingviolence.org

B. What is the *Personal Information Protection Act*?

It is a provincial law that establishes rules about the collection, use or disclosure of personal information.

C. What is meant by personal information?

Personal information means information that would identify a particular person. For example it includes information such as their name, home address and phone number, medical information, marital status, and education. Personal information does *not* include contact information which is meant to enable someone to be contacted at a place of business for business purposes. This would include information such as their position name, job title, business address, and telephone number.

PIPA does not apply to documents related to a prosecution if all proceedings related to the prosecution have not been completed.

D. Which agencies or programs must follow PIPA rules?

PIPA applies to all private sector organizations in BC including non-profit organizations. PIPA does not apply to an agency or program already covered by BC's *Freedom of Information and Protection of Privacy Act* (FOIPPA).

Whether or not your program is covered by FOIPPA, rather than PIPA, will depend on the wording of your contract with the funding ministry. If the wording of the contract suggests that your records are under your agency or program's "custody or control", then PIPA rules apply. If you are uncertain about this, you can refer to the *Records Management Guidelines* for further information including an overview of the factors affecting who has "custody or

control". You may also wish to contact the contract manager at your funding ministry.

To date, wording of the community-based victim assistance program and stopping the violence contracts has been interpreted in the field as the programs having "custody or control". This means these programs would be governed by PIPA. Contract wording can change from year to year so we recommend that you review the contract terms again, during the upcoming fiscal year.

If your agency runs more than one program, then some records may be governed by PIPA and some by FOIPPA. Each individual contract should be reviewed to determine who has "custody or control" of the records.

E. Will existing privacy policies at my agency need to be changed?

Most BC anti-violence programs already use the *Records Management Guidelines* or have locally developed in-house information management policies which are based on the *Records Management Guidelines*. If your agency or program is following the *Records Management Guidelines*, then most of the PIPA privacy requirements will be met. For example, like PIPA, the *Records Management Guidelines* provide that only as much personal information as is needed for a specific purpose should be collected and that it should be used only for the purpose for which it was collected. The *Records Management Guidelines* also suggest that consent be given before client information is released and that the agency take measures to protect the physical security of personal information.

The *Records Management Guidelines*, along with the recommendations in Section F of this Bulletin, can be used as your organization's privacy policy under PIPA.

F. What additions should my agency make to the *Records Management Guidelines* to satisfy PIPA?

1. Consent requirements

The *Records Management Guidelines* already provide that agencies get consent before *using or disclosing* personal information. Under PIPA you must also obtain consent before *collecting* this information. Agency/program intake

forms should be changed to include this requirement. (See Appendix B for sample consent/confidentiality clause wording.)

2. Personal information which was collected before PIPA was in effect
PIPA regards information collected before January 1/04 to have been collected with consent but only for the purpose for which it was collected. You do not need to go back and get consent for clients that went through the intake process before the effective date, provided you are only using their information for its original purpose.

Only the "collection" process is grandparented. This means that PIPA *will* apply to how you *use, secure and disclose* the personal information that was collected before January 1/04. To satisfy PIPA, organizations should ensure that personal information collected before the effective date is only used and disclosed for purposes that a reasonable person would consider appropriate in the circumstances and that fulfill the purposes for which it was originally collected. In terms of client information, if your agency has been following the *Records Management Guidelines*, you will already be in compliance.

3. Release of personal information to third parties

Defendants or offenders sometimes request records or personal information about the victim from a victim-serving agency. They base their claim on the grounds that the record also includes information about them or their child and that therefore they are entitled to see it. In other cases the offender simply wants to harass or intimidate the victim to discourage her from legal proceedings.

The *Records Management Guidelines* provide that subject to certain limited exceptions, personal information should not be released to a third party without the client's consent. PIPA also requires consent for information to be so released. In addition PIPA sets out specific situations in which personal information must not be disclosed to *anyone*. These include situations where:

- disclosure would reveal information about another individual (*For example, if personal information in the victim's file includes information she provided about the offender, then releasing this to the offender would have the prohibited effect of also revealing to him information about her.*)
- disclosure could reasonably be expected to threaten the health or safety of someone other than the person who made the request (*For example, releasing information about what the victim said to service providers might incite the defendant/offender to further acts of violence against her. This situation would involve some assessment of the degree of risk involved.*)

- disclosure would reveal the identity of someone who has provided personal information about another individual and the individual providing the personal information does not consent to disclosure of their identity. (*For example, the victim's sister provides information about the offender which is included in the victim's file and the sister does not wish her identity revealed.*)

In addition to the restrictions on disclosure already set out in the *Records Management Guidelines*, agencies/programs should not release personal information in the above situations.

4. Obtaining personal information about employees

To satisfy PIPA rules, agencies may collect, use and disclose employee information without consent if it is reasonable for starting, managing or ending the employment relationship. Agencies may wish to develop specific in-house policy regarding employee-related information. Employees include volunteers, students and board members. The *Records Management Guidelines* deal only with information obtained from clients as opposed to employees.

5. Contractors

PIPA rules also apply to personal information that your organization has transferred to a contractor for processing or information the contractor may have collected on your organization's behalf. To ensure this personal information is properly protected, your contracts should clearly state what requirements must be met to comply with applicable privacy legislation and any policies your organization has developed to manage the personal information. Sample contract language can be downloaded from the Ministry of Management Services website at:

http://www.msers.gov.bc.ca/foi_pop/Privacy/Tools/PIPA_Tool_9.pdf

6. Personal information collected for fundraising purposes

In terms of fundraising information, adjustments may be necessary. For example, your agency may have a pre-existing donor list and want to contact these donors for an upcoming event. In this situation, agencies can use an opt-out clause: this informs donors of the intended use and gives them the option of being taken off the list.

Possible wording for donor opt-out clause

Our agency/program has your contact information on a list of individuals and businesses who might be interested in information about our programs or in attending future fundraising events. Please advise us if you would like to be taken off this list.

7. Retention Periods

PIPA requires that personal information be kept for *at least* one year. After that, the retention period should be based on legal or business requirements. The *Records Management Guidelines* recommend that in general, adult client records be kept for a minimum of seven years while the records of a child client be kept seven years after they reach age 19. The seven year minimum is based on the need to protect agencies from potential legal liability and the client's possible need to access such records in the context of a civil suit for sexual assault. The *Records Management Guidelines* go on to suggest that some agencies consider whether client records might be kept indefinitely subject to financial and space restrictions.

The seven year minimum retention period in the *Records Management Guidelines* can be justified as consistent with current practice in related fields (social workers and psychologists) and with the legal or business needs of most community based victim assistance programs.

8. Privacy Officer

New under PIPA is the requirement for organizations to designate someone responsible for privacy compliance. This person is responsible for managing and implementing your agency's privacy policy. You may wish to designate one person within your agency as the Privacy Officer and must list their title and contact information on your intake form.

9. Complaints

PIPA provides that if someone feels that the act was not followed, they can contact the Privacy Officer. Information about the Privacy Officer should be made available either at intake or on request.

If there is a complaint, the Privacy Officer should make every effort to deal with the matter quickly and fairly. While different personnel may be called upon to help investigate, it makes sense to have one person responsible for receiving all complaints and making sure they are dealt with in a timely way. If the Privacy Officer is uncertain how to address a complaint they can contact the PIPA Hotline. (See Section H below).

If the concern cannot be resolved directly with the organization, the complainant may ask the Office of the Information and Privacy Commission for British Columbia to review the matter.

G. How does PIPA affect other laws that apply to information management?

The *Records Management Guidelines* deal with a number of situations in which legal proceedings are underway and third parties are seeking access to information contained in records as part of the proceedings.

PIPA does not limit information available by law to a party to a proceeding. Nor does PIPA override the *Criminal Code* or other federal legislation. This means that agencies can continue to follow the *Records Management Guidelines* in situations where records are being sought in a legal case.

Programs that provide services to minors under SAIP or other fee-for-service contracts with the Ministry of Children and Family Development may also be governed by Part 5 the *Child, Family and Community Service Act. (CFCSA)* As opposed to Part 3 of the Act which deals with child protection, Part 5 deals with confidentiality and disclosure of information. If there is a conflict between PIPA requirements and CFCSA rules, PIPA will override CFCSA Part 5. Programs should consult with their funding ministry's Director/Manager of Information and Privacy for clarification.

This Bulletin updates programs regarding PIPA, which is new legislation. It is important to note, that since the *Records Management Guidelines* were written in 1998, there have been amendments to other legislation referred to in the *Guidelines*. The BC Association hopes to provide programs with an updated version of the complete *Records Management Guidelines* in the near future.

H. Where do I get more information?

The Ministry of Management Services' Corporate Privacy and Information Access Branch is the central government agency responsible for PIPA. If you have more questions about PIPA contact them at:

Corporate Privacy and Information Access Branch
Ministry of Management Services
Email: CPIAADMIN@gems5.gov.bc.ca
Web Site: <http://www.msers.gov.bc.ca/FOI> POP/

Or call the PIPA hotline at:

PIPA Hotline: 250-356-1851

For toll free access call Enquiry BC at one of the numbers listed below and request a transfer to 250 356-1851.

From Vancouver: 604-660-2421
From elsewhere in BC: 1-800-663-1376.

Copies of the *Records Management Guidelines* can be downloaded from the BC Association of Specialized Victim Assistance and Counselling Programs website at:

BCASVACP@endingviolence.org

Consider cc'ing the BC Association of Specialized Victim Assistance and Counselling Programs regarding any issues and concerns. This helps us track and possibly address systemic issues related to PIPA's implementation.

Appendix A

Overview of PIPA Requirements¹

Get Consent

Get consent for collecting, using and disclosing an individual's personal information. There are exceptions to this requirement including employee personal information, and information needed in an emergency. PIPA considers consent to be given when a person, knowing the purpose of collection of their information, gives the information to you. Tell the person from whom the information is collected, either verbally or in writing, before or at the time of collection, why the personal information is needed and how it will be used. Programs using the *Records Management Guidelines* will already be in compliance. They only need to adapt their consent forms slightly to include consent to *collecting* personal information. (See Appendix B for a sample consent/confidentiality clause.)

Decide whether consent will be oral or written

Consent should be in a form appropriate to the type of personal information involved. Getting express written consent is often desirable. Consider here what is reasonable for the individual, the circumstances of collection, your proposed uses or disclosures of the information, the sensitivity of the information and whether you may need to prove that the person consented. The *Records Management Guidelines* recommend that written consent be included as part of the intake form. (See Appendix B of this Bulletin for a sample consent/confidentiality clause.)

Determine the scope of information you need

Collect personal information only for reasonable purposes and collect only as much as is reasonable for those purposes. Collect information directly from the individual unless PIPA permits otherwise or the person agrees to someone else giving the information to you. Programs using the *Records Management Guidelines* will already meet this requirement.

Obtaining personal information about employees

Employees include volunteers, students and board members. You can collect, use and disclose employee information without consent if it is reasonable for starting, managing or ending the employment relationship.

Set limits on the use of the information you have collected

¹ This information is adapted from: *Personal Information Protection Act—A thumbnail sketch for organizations* prepared by the Office of the Information and Privacy Commissioner for British Columbia

Use and disclose the information only for the purpose for which it was collected unless the person consents or PIPA permits release without consent. This is consistent with the *Records Management Guidelines*.

Provide access to the person the information is about

On request, provide an individual with information about the existence, use and disclosure of the personal information you have collected about them. If you receive such a request, respond within 30 days. Provide the individual with access to the requested information unless PIPA excuses you from giving access. For example, you can refuse access where release of the information would harm an investigation or where disclosure would harm someone else or would disclose someone else's personal information. On request, correct information that is inaccurate or incomplete. Access to personal information by the person who provided it, is also addressed in the *Records Management Guidelines*.

Keep records secure

Ensure that the personal information you have is secure. Recommendations contained in the *Records Management Guidelines* can be followed here.

Be able to justify how long you keep the information

PIPA requires that records be kept for a *minimum* of one year. After that, keep the information for only as long as is reasonable for business or legal reasons. If you have been using the retention period recommended in the *Records Management Guidelines*, you won't need to change your policy. Use care in disposing of or destroying information.

Develop a personal information or confidentiality policy and designate someone as a Privacy Officer

Designate someone in your organization who is responsible for ensuring your organization complies with PIPA. That person is responsible for developing and implementing a privacy policy and making sure it is working effectively. You can use Section F of this Bulletin, along with the *Records Management Guidelines*, as your agency privacy policy. Make information on your management of personal information available on request.

Respond to concerns

If someone complains about how your organization handles personal information, try to resolve the complaint quickly and fairly.

Appendix B

Sample Consent and Confidentiality Clause for Intake Purposes

I consent to receive the service(s) I have indicated above [*list them above*] which are provided by [*insert agency name*]. I understand that this application does not guarantee I will receive all the services I have indicated.

I also consent to having staff from the [*insert agency name*] collect personal information about me necessary for the purpose of delivering those services.

I understand that the personal information I provide is confidential. The release of any information regarding my involvement with the [*insert agency name*] may occur only with my written and signed consent subject to certain limited exceptions. These are:

- If agency staff have reason to believe that a child needs protection under section 13 of the *Child, Family and Community Service Act* they are obligated (as are the general public) to inform the Ministry of Children and Family Development;
- If agency staff have reason to believe that I am likely to cause serious physical harm to my self or another, they are obligated to inform the appropriate authorities (family doctor etc.);
- If agency staff are required by court order to disclose specific records or to attend court and give evidence.

Date_____

This agreement is in effect from [*insert start date*] until [*insert end date*].

Client name

Client's Signature

Agency staff signature

Information about [*insert agency name*] privacy policy can be obtained by contacting [*insert position title of privacy officer*] at: [*insert phone number.*]