



## PIPA and the Hiring Process

April 10, 2006

### **INTRODUCTION**

Any private sector employer who collects, uses or discloses personal information about employees or job applicants has to comply with British Columbia's *Personal Information Protection Act* ("PIPA"). PIPA applies to all provincially regulated private sector "organizations". It covers all businesses (such as corporations, partnerships, sole proprietorships and individuals acting as agents or contractors for an "organization"). PIPA also applies to non-profit organizations (including trade unions, charities, foundations, trusts, clubs, religious institutions, associations and amateur sports organizations).

PIPA requires every organization to have policies on how the organization will meet its obligations under PIPA to protect personal information, including employee personal information. It is good practice for employers to give their new employees a copy of the privacy policy or, at least, to tell new employees how to get a copy of the policy. It is also a good practice to train employees about their role in ensuring the policy is properly applied.

PIPA is still relatively new, since it came into force on January 1, 2004. The Office of the Information and Privacy Commissioner for British Columbia ("OIPC") continues to receive requests from employers for clarification of their responsibilities in relation to the hiring of new employees. This document answers questions we most frequently hear.

If you need more information or have questions about situations not covered by this document, you can call or write us and we will try to help. You can also find general guidance on PIPA and how it applies to businesses and organizations in our "Guide for Businesses and Organizations to British Columbia's *Personal Information Protection Act*" ([http://www.oipc.bc.ca/pdfs/private/a-GUIDE\\_TO\\_PIPA\(3rd\\_ed\).pdf](http://www.oipc.bc.ca/pdfs/private/a-GUIDE_TO_PIPA(3rd_ed).pdf)).

*Please read the important notice at the end of this document.*

## **DEFINITIONS**

PIPA gives these definitions for terms that are relevant to this document:

**“contact information”** means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual;

**"employee"** includes a volunteer;

**"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;

**"employment"** includes working under an unpaid volunteer work relationship;

**"personal information"** means information about an identifiable individual and includes employee personal information but does not include

- (a) contact information, or
- (b) work product information;

**"work product information"** means information prepared or collected by an individual or group of individuals as a part of the individual's or group's responsibilities or activities related to the individual's or group's employment or business but does not include personal information about an individual who did not prepare or collect the personal information.

## **FREQUENTLY ASKED QUESTIONS**

### **Q. I'm not hiring. What do I do about unsolicited résumés?**

*Dispose of them carefully.* First of all, you aren't collecting personal information you don't ask for, unless you keep unsolicited résumés with the idea that one day you might use them. If there's no job open, then you are not making a decision using the personal information in unsolicited résumés and the one-year retention requirement described below does not apply. Even if you don't keep unsolicited résumés when you receive them, you should take reasonable care when disposing of them, so that no one can misuse the personal information they contain. You should shred paper copies and delete electronic copies.

*Keep a résumé for a year if you use it to make a decision.* If you use information in a résumé (or simply hold onto it for possible future use), you're responsible for protecting the personal information in it and for responding to the individual's enquiries about how her or his personal information has been used or disclosed. If you use it to make a decision to hire or not to hire the individual, you have to keep the résumé for at least a year so the individual can obtain access to it.

Make sure your staff knows your policy about accepting résumés. If managerial or supervisory staff are in the habit of putting off prospective applicants by asking them to send in a résumé, that amounts to soliciting the résumé. You're collecting the personal information in it and therefore must protect it and retain it for at least a year.

**Q. What kinds of personal information can I ask for in the hiring process?**

*Consent implied for collection of relevant information.* When an employer has a job to fill, applicants provide personal information in exchange for being considered for the job. PIPA allows an employer to request any personal information that is reasonably relevant to the hiring decision. Typically, that might include relevant qualifications, experience, knowledge, skills and abilities as well as answers to interview questions and skills tests.

*Collection, use or disclosure without consent.* PIPA allows collection, use or disclosure of "employee personal information" (refer to definition above) without the consent of the job applicant if it is reasonable for the purposes of establishing, managing or terminating an employment relationship. The employer must first give the individual notice and explain the purpose for collecting, using or disclosing the information without consent. In limited and specified circumstances, PIPA allows collection, use or disclosure of "employee personal information" without consent or notice. These provisions generally have limited application in the typical hiring process.

*Consent needed for collection of other information.* It wouldn't be reasonable for an employer to require personal information for any purpose other than assessing suitability for the job and establishing an employment relationship. If you do require personal information for other purposes, you should tell the applicant that he or she is free to refuse to disclose the requested information and that doing so will have no effect on the hiring process.

*Collection of personal information must be reasonable.* Whether or not a job applicant has given consent to the collection of personal information, you have to be able to show your collection and use of the personal information are reasonably required to determine the job applicant's suitability for the position. For example, credit checks on a job applicant should only be conducted if you can establish that the information is both relevant and necessary to verify the

applicant's ability to perform the job functions and that the verification cannot be done through less intrusive means.

In some circumstances it may be reasonable to ask fairly open-ended questions that, in other contexts, would be unreasonably intrusive. For instance, in hiring a daycare worker it may be reasonable to seek information relating to the applicant's patience, anger management and attitudes toward children or even about family life or substance abuse issues.

The reasonableness of the collection of certain types of information may be assessed in the context of a statutory requirement or other legal obligation of the employer. For example, those in the business of processing raw food must comply with Canadian Food Inspection Agency Guidelines for pre-employment testing for health related reasons. Other employers may have a contractual obligation to have new employees undergo security checks.

*Notification needed for post-hiring collection, use or disclosure of employee information.* Once you've made a hiring decision, you can collect, use and disclose employee personal information without consent if doing so is reasonable for the purpose of establishing or managing an employment relationship. Canada Revenue Agency registrations for income tax purposes or enrollment in employee benefit plans are two examples of post-hiring collection and use of employee personal information. But even though you can collect, use and disclose employee personal information without consent, except for a few cases described in PIPA, you still have to tell the employee in advance about the collection, use or disclosure of personal information and the reason for it. In short, even though you don't need an employee's *consent*, you generally still need to *notify* the employee in advance of your purpose for collection, use and disclosure of their personal information.

**Q. How do I handle reference checks?**

*Assume the job applicant's consent for contact with listed references.* An applicant who has listed references in a job application or resume implicitly consents to your contacting listed references, but only so you can collect reference information that is reasonably related to the job requirements.

Likewise, by asking someone to act as a reference, a job applicant implicitly consents to the referee's disclosure of personal information to a prospective employer. Although not strictly required, when an employer does a reference check on a job applicant, it is a good practice to first confirm that the applicant has authorized the referee to talk to you. A job applicant should be sure to tell referees which employers might be contacting them. Otherwise, a referee who is called out of the blue for a reference may feel unable to share any information about the individual's abilities.

*At a minimum, notify applicants about other reference inquiries.* You may want to conduct background checks or make informal inquiries about a job applicant with previous employers who are not listed as referees. Although you do not need the job applicant's consent, PIPA requires you to give notice to her or him in advance that you intend to do this. You also have to be able to show that the personal information you want to collect and use in this way is "reasonably required" to establish the employment relationship.

The problem for the person from whom you request information is that, without the job applicant's consent, that person might be breaching PIPA by disclosing personal information without consent. For this reason, you should consider doing more than giving notice to job applicants that you may go beyond their listed references and instead get their consent up front (perhaps on the job application form) for you to contact persons other than those the job applicant lists as references. If the applicant objects, PIPA would not stop you from inviting him or her to withdraw from the hiring process or from weighing the refusal to consent in determining the applicant's suitability for the position.

**Q. How can I ensure that information I get from a referee will stay confidential?**

*Familiarize yourself with PIPA exceptions to access.* Any factual information obtained about a job applicant and referees' opinions about an applicant are the applicant's personal information. PIPA gives individuals the right of access to their personal information under your control, but there are exceptions to this. For example, you cannot disclose personal information if doing so would reveal the identity of someone who has provided personal information and hasn't consented to disclosure of his or her own identity.

*Confirm confidentiality with referees.* If you prefer not to reveal a referee's comments to the job applicant, it may be best to make it clear to the referee in advance that his or her opinions will be received in confidence, document this agreement, and tell the applicant that all references will be received in confidence. However, there is no guarantee that job applicants will not be able to access comments by referees to prospective employers, as PIPA gives individuals a right of access to their own personal information, including employee personal information.

PIPA is still new legislation and this issue has not yet been decided in a formal inquiry by the Information and Privacy Commissioner. OIPC decisions under BC's *Freedom of Information and Protection of Privacy Act* ("FIPPA") suggest that public sector employers cannot withhold referees' opinions from job applicants, although referees' identities can be withheld if given in confidence. These decisions are based on the principle that a referee's opinions about an applicant are the personal information of the job applicant, since they are about that individual. The referee's identity remains the referee's personal information.

The wording of FIPPA and PIPA is different, so it is possible, but far from certain, that this issue could be decided in a different way under PIPA. However, both the federal and Alberta privacy commissioners have issued decisions confirming that a third party's opinion about an individual is the individual's personal information. Those decisions were made under Alberta's *Personal Information Protection Act*, which is very similar to BC's PIPA on this issue, and under federal private sector privacy law, which is substantially similar.

The OIPC believes that, despite the fact that this matter has not been formally decided under PIPA, the best approach is to assume that referees' opinions about a job applicant are the applicant's personal information and that employers cannot guarantee that referees' comments will remain confidential. As for a referee's identity, it is best to assume that the referee's name is the personal information of the referee and may be withheld.

**Q. Can I use personal information collected during the hiring process for other purposes?**

*Yes, for obvious purposes.* You can use personal information you collect during the hiring process for another purpose only if that other purpose would be obvious to a reasonable person at the time the information was collected *and* the job applicant voluntarily provided the information for that purpose. Orientation and training can be considered part of the hiring process, so it's reasonable to assume that personal information collected from job applicants might be used for that purpose.

If the other purpose isn't reasonably obvious, then you have to tell the job applicant what the other purpose is and get the applicant's consent. For example, it would not necessarily be obvious to a job applicant that an employer might send written material to employees' residences or home email addresses inviting to support a particular political candidate. Nor would it seem obvious that you would send someone's résumé to another employer who might be hiring, even though that might appear to benefit the applicant. When in doubt, give notice and get consent.

**Q. What do I need to do to protect and retain personal information collected during the hiring process?**

*Make it secure.* Section 34 of PIPA requires an organization to make "reasonable security arrangements" to protect personal information from "unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks". In other words, even though perfect protection is impossible, you should at the very least take the same precautions you might use for any document you want to protect from improper use by staff or anyone else. The greater the sensitivity of the employee personal information, the greater the

need for protection—for example, it is reasonable to expect a higher level of security for an employee’s medical information than for a résumé. Some factors for assessing what are “reasonable” security measures are discussed in OIPC Investigation Report F06-01.<sup>1</sup> This report was issued under FIPPA, but they will be useful considerations for s. 34 of PIPA.

*Retain it for at least a year if you use it.* If you use an individual’s personal information to make a decision that directly affects him or her (like hiring or not hiring), you have to keep it for at least a year after you make the decision, so that the individual has a reasonable opportunity to obtain access to it. This would include interview notes, hiring grids and other information about or related to the assessment of candidates. If an individual requests her or his own information of this kind, personal information of other candidates found in records containing the applicant’s information would have to be withheld from the applicant.

If you don’t use personal information for a decision, you either have to take reasonable steps to destroy it securely or else make it anonymous by removing any information that would identify a particular individual. You need to do this as soon as the purpose for which it was collected is no longer being served and you no longer need it for legal or business purposes.

**Q. What other PIPA obligations apply to personal information collected during the hiring process?**

*Know when information can’t be given out.* The bottom line is that anyone—including an employee and an unsuccessful job applicant—has a right to be given access to his or her own personal information, to know how it’s being used or has been used, and to know to whom and in what situations it’s been disclosed. However, PIPA permits or requires you in certain circumstances to deny someone access to their own personal information—for example, where disclosure would harm someone else, harm an investigation or legal proceeding, result in the disclosure of someone else’s personal information, or disclose confidential business information. If such information can be removed from a document, you have to give access to the rest of the document after the information is removed.

*Make sure information is accurate and complete.* You also have to make a reasonable effort to ensure that personal information collected by or on behalf of your organization is accurate and complete if you are “likely to” either use that information to make a decision that affects the individual to whom the information relates or disclose the information to another organization.

*Respond to requests for correction.* Anyone who believes there’s an error or omission in his or her personal information can ask the organization to correct it.

---

<sup>1</sup> [http://www.oipc.bc.ca/orders/investigation\\_reports/InvestigationReportF06-01.pdf](http://www.oipc.bc.ca/orders/investigation_reports/InvestigationReportF06-01.pdf).

If that happens, your organization must decide whether to correct the information. If the answer is yes, you must make the correction as soon as possible. If, on the other hand, you decide the information needs no correction, you must annotate the personal information to record the correction that was requested but not made. Like all of PIPA's requirements, this applies to paper and electronic records.

If you do make a requested correction, you must send the corrected information to every organization to which you have disclosed the information during the year before the correction date. And if you're notified by another organization that it has corrected an individual's personal information that was disclosed to it, you must also correct that personal information if it is under your organization's control.

\* \* \*

This document is for general information only. It is not intended to be, and cannot be relied upon as, legal advice or other advice. Its contents do not fetter, bind, or constitute a decision or finding by, the Office of the Information and Privacy Commissioner (OIPC) with respect to any matter, including any complaint, investigation or other matter, respecting which the OIPC will keep an open mind. Responsibility for compliance with the law (and any applicable professional or trade standards or requirements) remains with each organization and public body.