OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

PIPA and workplace drug and alcohol searches: a guide for organizations

January 2022

Introduction

This document aims to help organizations subject to BC's *Personal Information Protection Act (PIPA)* understand what conditions must be present before they can consider conducting random searches for drugs and alcohol. This guide applies to employers who search their own employees as well as employers that use contractors. It also applies to unionized and non-unionized workplaces.

This document does not deal with workplace drug or alcohol testing through breath or other samples, nor does it deal with searches or testing after a workplace accident, where an employer or organization might have reasonable cause to suspect an individual is impaired.

This is a guidance document and should not be taken as legal or other advice and cannot be relied on as such. For complete information, see our longstanding *Policy on Consultations with the OIPC*.

Searches are a collection of personal information, so PIPA applies

PIPA applies to information about an identifiable individual, whether the information is written or not. If someone searches an employee's bag for alcohol or drugs, for instance, and they do not find any, they have still collected information about that individual. If the search turns up drugs or alcohol, that is also personal information about the employee. PIPA therefore applies.

Similarly, when a canine trained to detect the scent of illicit drugs indicates at the door to someone's room that there is a suspicious smell, that indication may trigger the process for searching the room. The canine's initial indication is information disclosing that the room's occupant may be in possession of contraband. That is personal information of the occupant. An actual search will involve collection of personal information. This can, for example, be information about the occupant's possessions or interests. Information collected during a search is personal information and PIPA therefore applies.

Employee personal information and PIPA

PIPA contains special rules for collection, use or disclosure of "employee personal information". PIPA defines that term as "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.[1]

[1] The definition of "employee personal information" expressly excludes "personal information that is not about an individual's employment".

An employer can collect, use or disclose employee personal information without consent as long as the employer notifies the individual and two further conditions are met.

First, as the definition of "employee personal information" shows, the collection, use or disclosure must be "reasonable" for the purposes of establishing, managing, or terminating the employment relationship.

Second, the collection, use or disclosure itself must be reasonable. Factors guiding this assessment include: the purpose of the collection, use or disclosure; the amount of information involved; the sensitivity of the information; whether the collection, use or disclosure is reasonably likely to be effective in achieving the organization's goals; and, whether alternatives exist (and, if they do, whether they have been given reasonable consideration).[2]

The reasonable person standard when collecting personal information

Even if an organization has an individual's consent to search for drugs or alcohol, PIPA requires that the collection of such information be only for purposes that a "reasonable person would consider appropriate in the circumstances." Drug and alcohol searches are invasive of personal privacy as they can reveal information about an individual's personal habits, health, and possible criminality. Therefore, there must be good reasons before an organization takes this step.

Previous OIPC decisions[3] have established the following factors as relevant in deciding whether an organization is authorized to collect personal information under the reasonable person standard:

- Has the organization tried or considered other reasonable, less intrusive alternatives to address the issue?
- Is there a reasonable likelihood that the collection of the employee personal information will be effective in addressing the issue?
- Is the collection of employee personal information carried out in a reasonable manner?
- What is the type, nature and sensitivity of the information?
- What are the organization's intentions, at the time of collection, regarding the use and disclosure of the employee personal information?
- How long will the employee personal information be retained?
- Is the organization collecting or using the minimum amount of employee personal information reasonably required to address the issue?

[2] For a discussion of these factors see, for example, *Schindler Elevator Corporation (Re)*, 2012 BCIPC 25 (CanLII) <https://canlii.ca/t/fvfdl>, starting at paragraph 141. A more recent example is *Teck Coal Limited (Re)*, 2020 BCIPC 24 (CanLII), <https://canlii.ca/t/j7xs3>.

[3] See *Owners, Strata Plan BCS1964 (Icon 1 and 2) (Re)* 2021 BCIPC 35 (CanLII) <https://canlii.ca/t/jh228>.

For workplace drug and alcohol searches the OIPC has, consistent with Supreme Court of Canada and labour arbitration decisions, noted that other factors are relevant.

The fact that a workplace is shown to be dangerous does not alone justify searches. It is also necessary to have evidence of a workplace problem with drugs and alcohol that creates safety risks.[4]

A problem at one workplace is not a basis to search at another

An organization that wants to search employees, their belongings or accommodation must have evidence of a specific problem at the worksite in question. It is not enough to say that similar worksites have a problem and that employee searches are justified at the organization's own worksite. One worksite's challenges are not, in other words, evidence of a problem at another worksite that justifies employee searches.

Policies and enforcement may be enough without searches

The preferred practice for organizations with concerns about drugs and alcohol in the workplace is to first establish, communicate, and consistently enforce a drug and alcohol policy short of searching employees.

If the organization can later show that, despite communicating and enforcing the policy, drugs and alcohol are making the workplace dangerous, this may be enough to allow the organization to collect employee personal information through a search policy (which the organization would also need to create).

Governing personal information collected through searches

Any organization that searches employees should establish policies and procedures governing the flows of personal information the searches yield. Access to search results should be limited to those with a real need to know the information, such as health and safety officials and human resources personnel. Measures to protect the information from unauthorized access or disclosure are also needed. Procedures enabling individuals to request access to their own information, and to seek its correction, must also be in place.

For these general requirements, refer to our general guidance on PIPA.

Conclusion

Any employer thinking about searching employees for drugs and alcohol must be ready to justify this with clear evidence that it is appropriate in the circumstances. Before acting, consider whether you have evidence of a real safety problem that endangers the workplace; that existing policy, communication and enforcement are ineffective; and that searches are reasonably the least intrusive method to address the problem.

---

[4] See *Communications, Energy and Paperworkers Union of Canada, Local 30 v Irving Pulp & Paper, Ltd*. 2013 SCC 34 (CanLII) at paragraphs 4-6 <https://canlii.ca/t/fz5d5>.

For more information, or to consult with the OIPC, please contact us at (250) 387-5629 or info@oipc.bc.ca.

These guidelines are for information purposes only and do not constitute a decision or finding by the Office of the Information and Privacy Commissioner for British Columbia. These guidelines do not affect the powers, duties, or functions of the Information and Privacy Commissioner regarding any complaint, investigation, or other matter under FIPPA or PIPA.