

# Do Your Flu & Infectious Illness Prevention Measures Violate Employee Privacy?



There are a lot of infectious illnesses floating around Canada right now, including influenza, measles, COVID, and pertussis (whooping cough). OHS and public health laws require employers to take measures to safeguard workers against risk of infection. But carrying out this responsibility may require you to collect, use, and disclose personal health information about your employees. For example, you might have to ask if they have a medical condition that increases their vulnerability to flu or find out which employees have kids at home that they might have to stay home and care for. Gathering this kind of information raises risk of liability under privacy laws. Here's how to manage this risk based on guidelines issued by the Privacy Commissioners of Canada, Alberta and BC during the H1N1 outbreak (the "Guidelines"). To the extent they were issued at a time when a public health emergency was expected but not yet declared, the Guidelines offer general guidance on workplace infection control involving any other contagious illness in non-public health emergency conditions.

## **The 4 Things Employers Must Do to Respect Employees' Privacy Rights**

All employees have some right to privacy vis-à-vis their employers. There are 4 things employers must do to avoid invading employees' privacy rights when collecting, using and disclosing their health information for purposes of general workplace infection control. **Caveat:** Be aware that the rules change when and if a public health emergency is declared, as it was with COVID-19.

### **Rule 1: Get Employees' Consent, If Necessary**

Privacy laws make it illegal to collect, use, or disclose an individual's protected health information without their consent. However, exceptions apply. In the HR context, the most important of these exceptions is the employer's right to collect, use, and disclose employees' protected information without consent when necessary to carry out certain core business or employment-related operations. As explained by an official Alberta information sheet, "an employer has a legitimate need to collect, use, and disclose certain types of personal information about employees in order to operate the business and fulfill its obligations to employees." Examples of

legitimate functions that privacy tribunals have allowed employers to use private employee information to perform without consent:

- Verifying an employee's eligibility for sick leave or disability benefits.
- Determining what accommodations to make for disabled employees.
- Filing workers' compensation claims.

However, it's unclear whether this exemption from consent extends to normal workplace infection prevention and response in times when a public health emergency is not in effect. The H1N1 Guidelines suggest that it's not and that employers need consent to perform these functions.

## **Rule 2: Collect Only the Minimum Protected Information Necessary**

Employers must collect, use, and disclose only the amount and type of protected information they need to carry out the infection prevention and response function that they need the information for. Thus, for example, it would be inappropriate to ask employees to undergo a physical exam or submit a complete medical record to assess their vulnerability to seasonal flu.

## **Rule 3: Notify Employees of Uses of Their Protected Information**

Privacy laws generally require employers to notify employees of:

- The purpose of collecting the employee's protected health information.
- How they'll use the information.
- To whom they'll disclose it.
- When and how they'll destroy it.

## **Rule 4: Keep Employees' Protected Information Secure & Properly Destroy It**

Employers must maintain the security of any protected health information they collect from employees. Security measures typically include:

- Physical barriers such as keeping files locked.
- Electronic measures such as password protection and encryption.
- Administrative controls, such as keeping the number of staffers with access to the information limited to the minimum necessary.