Privacy Considerations During COVID-19

Consider the Risks

The spread of COVID-19 increases in situations involving close interactions with others, in closed spaces, and crowded places. The chances of COVID-19 spreading during these activities depends on the number and characteristics of people who attend (e.g., age, maturity, physical ability, comprehension), proximity, length of the interactions between people, as well as the prevention measures put in place by employers.

Introduction

This tip sheet will help employers and workers understand the privacy considerations when personal information is collected during the COVID-19 pandemic.

For general COVID-19 prevention practices for both employers and workers, refer to the CCOHS resource "Protect Yourself and Others".

Control Measures

Each workplace is unique. It is important for employers to assess the risks of COVID-19 for their specific workplace and implement appropriate hazard controls using the hierarchy of controls: elimination, substitution, engineering controls, administrative policies, and personal protective equipment (PPE). Use a layered approach by including multiple personal preventive practices to protect yourself and others from COVID-19.

Personal and Health Information to Consider During the COVID-19 Pandemic

Privacy is considered a fundamental right for Canadians. Any information that can identify an individual is considered to be personal information. The age of an employee, their marital status, medical history, education, and even the opinions you have about them are all examples of personal information.

Personal health information includes an employee's COVID-19 test results, COVID-19 vaccinations, and accommodation needs. How will you ensure personal and health information will be kept private?

What Privacy Laws Apply to My Workplace?

There are several privacy laws which govern the collection, use, and disclosure of personal information of Canadians:

Federal Privacy Laws

- The **Privacy Act** explains how personal information is handled by federal government institutions and Crown corporations. It protects information concerning old age security, employment insurance, tax collection, border security and federal policing and public safety.
- The **Personal Information Protection and Electronics Document Act (PIPEDA)** applies to private sector organizations who are not federally regulated and collect or disclose information while engaging in commercial activity. Banks, education and daycares, real estate agents and even dog breeding businesses might apply; however, charity and not-for-profit organizations might not. Refer to the Office of the Privacy Commissioner of Canada to determine if PIPEDA applies to your organization.

Provincial and Territorial Privacy Laws

- Organizations in the Northwest Territories, Yukon and Nunavut are covered under PIPEDA. Others may be covered by their own jurisdictional privacy laws.

Considerations for Employers

Privacy Considerations During COVID-19

Organizations should consider the implications of collecting personal information when implementing measures to prevent COVID-19 transmission. What information will be collected, by whom, and for what reasons? Visit the Privacy Guide for Canadian Businesses for additional details on how organizations can comply with privacy laws. General guidance is provided as follows:

Assign responsibility

Identify who in the organization will be responsible for privacy issues. Will this responsibility be shared? Who will collect employee, customer, or client screening information? Who will be the contact person to address inquiries or concerns about the use of personal information? Clearly outline the roles and responsibilities and provide training to all employees who will be responsible for private data.

Develop and communicate polices and practices

Ensure your employees and others (e.g., clients and customers) understand your privacy policies and practices. Outline the roles and responsibilities of all stakeholders and include information on how individuals can access their personal information from the organization. Make your policies readily available (e.g., postings, website, etc.).

Establish complaint procedures

Employee customers and clients should understand what steps they can take if they have concerns about how their private information is collected, used, stored, and destroyed. Establish easy-to-follow procedures for responding to inquiries and complaints about a privacy concern.

Identify the reasons for collecting personal information and obtain consent

Make sure you identify the reasons why the personal information is collected before and during the time of collection. Your employees (and others) should know what information is being collected (e.g. name, phone number and mailing address), for what purpose (e.g., for contract tracing purposes) and what the employer will do with the information (e.g., share it if required by public health authorities for contact tracing purposes).

Confirm information is accurate and only gather what is needed

Ensure employee information is accurate, complete, and current. Only gather what is needed for its intended purpose (e.g., screening, contact tracing, point-of care rapid antigen detection test results, accommodation requests, etc.).

Limit use of collected information

Only use the information for its intended purpose. For example, personal information used for contact tracing should not be used for an employer's mailing list. Always obtain consent, even from your employees, to use personal information for reasons other than why it was originally collected.

Protect information

Keep all personal information private and secure from loss or theft. Keep in mind that employees have the right to access their own personal information.

Keep records

Determine whether documentation will be on paper, electronic or combination of both. Follow your privacy laws and establish a procedure for recording, storing, access, and destruction of personal information.

Considerations for Workers

Your employer and other businesses may collect your personal information when implementing measures to prevent

Privacy Considerations During COVID-19

COVID-19 transmission. Your personal information may be obtained through screening, collecting information for contact tracing, point of care testing results, accommodation requests, and when traveling. To learn more about your privacy rights, visit the privacy laws for individuals for additional details. General guidance is provided as follows:

Understand the reasons for collecting your personal information

Make sure you understand what information is being collected from you and how it will be used. Ask questions so you know what the employer will do with the information (e.g., share it if required by public health authorities for contact tracing purposes).

Review company policies

Review your company policies and those of any websites and apps you use. Ensure you understand how your personal information will be used, stored, and destroyed. Remember you have the right to access your personal information including the information your employer has of you.

Understand how privacy laws apply

Read up on the basics of Canada's federal privacy laws. Learn about how the Federal Government handles your personal information. Find out about a business' obligations with respect to your personal information. Learn how to raise a privacy concern with an organization that possesses your information. Remember, you have the right to access and correct your personal information.

Keep your personal information safe

There are many ways to keep your personal information safe while still complying with safety measures to protect you and others from COVID-19:

- Subscribe to the National Do Not Call List to avoid telemarketers.
- Remove your name from mailing lists by subscribing to the Canadian Marketing Association's Do Not Mail Service.
- Take steps to protect your privacy online. Ensure your computer, smartphone and other mobile devices are password protected.
- Safeguard your Social Insurance Number for income reporting purposes only.
- Take measures to prevent your personal information from putting you at risk for of fraud or identity theft. Make sure your passwords are hard to guess, using eight or more characters, and a combination of letters, numbers, and symbols. Keep your passwords in a secret, safe and locked place.
- Make sure data stored on devices you no longer use is properly deleted before selling, recycling or throwing them away.

If you or someone you know is in crisis, please contact your local hospital, call 911 immediately, or contact a Crisis Centre in your area.

It is important that mental health resources and support are provided to all workers, including access to an employee assistance program, if available.

For further information on COVID-19, refer to the Public Health Agency of Canada.

Note that this guidance is just some of the adjustments organizations can make during a pandemic. Adapt this list by adding your own good practices and policies to meet your organization's specific needs.

from any use or reliance upon the information.