

COVID-19 PRIVACY + FOI BULLETIN – MARCH 30, 2020

By Keri L. Bennett and Jordan Michaux

The recent COVID-19 pandemic has imposed significant strain on individuals and organizations. At the same time as employers must consider critical operational and health and safety issues, employers must continue to protect company confidential information, as well as customer and employee personal information, all while navigating the new uncertain landscape.

Work From Home

Wherever possible, business have been requiring employees to work from home, in accordance with guidelines or mandatory requirements of public health authorities. WorkSafeBC has issued guidance [here](#) on occupational health and safety requirements for employees working from home.

The sudden move of a workforce from an office to a home environment creates increased security risks. Hackers have been taking the opportunity to test networks that have become vulnerable due to strains on the network. In addition, standard protocols for protection of company, customer and employee information must be re-considered for the “work from home” environment.

Employers can consider the following recommendations:

- Establish a short, straightforward work-from-home policy that defines employee responsibilities and their role in protecting company and customer data away from the office, as well as how to secure their remote workspace
- Include breach reporting requirements in the policy
- Establish or update security protocols to ensure protection of company information including updating firewalls and implementing or updating password protection requirements
- Require employees to use the company laptop, VPN or other secure network whenever able
- Require employees to save company documents on that secure network
- Prohibit employees from downloading and storing company documents on personal devices
- Prohibit employees from sharing company/client information through personal email addresses



- Require employees to only use company-approved cloud-based networks to store documents
- Require employees to protect all devices, flash drives, paper files and ensure other individuals in the home do not have access to company information
- Remind employees of increased risks from malicious emails, phishing scams, and more
- Require employees to conduct telephone, conference or video calls in a private room in the home wherever possible

B.C. Data Localization Requirements

Public sector employers and service providers of public sector employers are required to comply with strict and detailed requirements regarding access, processing and storage of personal information in Canada under the British Columbia *Freedom of Information and Protection of Privacy Act*.

However, in order to support health care bodies and other public bodies in their management of the COVID-19 pandemic, the Ministry of Citizen Services issued Ministerial Order No. M085 permitting disclosure of personal information inside and outside of Canada in accordance with Section 33.2(a) and (c) of the Freedom of Information and Protection of Privacy Act on conditions specified in the order, which is [here](#).

Specifically, health care bodies may disclose information outside of Canada if the disclosure is necessary:

- a. for the purposes of communicating with individuals respecting COVID-19,
- b. for the purposes of supporting a public health response to the COVID-19 pandemic, or
- c. for the purposes of coordinating care during the COVID-19 pandemic.

Public bodies may do so where:

- a. the third-party tools or applications are being used to support and maintain the operation of programs or activities of the public body or public bodies,
- b. the third-party tools or applications support public health recommendations or requirements related to minimizing transmission of COVID-19 (e.g. social distancing, working from home, etc.), and
- c. any disclosure of personal information is limited to the minimum amount reasonably necessary for the performance of duties by an employee, officer or minister of the public body.



Employee Privacy and COVID-19

Employers must also address the challenge of balancing employee privacy rights with occupational health and safety obligations in the context of COVID-19.

The British Columbia Office of Information and Privacy Commissioner issued a brief [statement](#) confirming that B.C.'s privacy laws are designed to ensure that public bodies and private organizations can share information to protect health and safety. The Office of the Privacy Commissioner of Canada also issued guidance [here](#). In short, applicable legislation permits sharing and disclosure of personal information about employees in order to protect health and safety. However, employers must still carefully assess the facts of each situation to ensure the potential use or disclosure is authorized by law. If you have questions, please contact us (see information below).

[Keri L. Bennett](#) is a partner at the employment and labour law boutique of Roper Greyell LLP where she provides strategic advice and representation to public and private sector clients in all areas of workplace law and leads the firm's Freedom of Information and Privacy Law practice. Keri can be reached at (604) 806-3848 or kbennett@ropergreyell.com.

[Jordan Michaux](#) is an associate at the employment and labour law boutique of Roper Greyell LLP where he practises in all areas of labour and employment law with an emphasis on workplace privacy issues, litigation, labour advocacy, and regulatory advice. Jordan can be reached at (604) 806-3878 or jmichaux@ropergreyell.com.

To obtain contact information of any other lawyer at our firm, please visit: <https://ropergreyell.com/our-people/>

While every effort has been made to ensure accuracy in this article, you are urged to seek specific advice on matters of concern and not to rely solely on what is contained herein. The article is for general information purposes only and does not constitute legal advice.