Managing Privacy and Cyber Risks During a Pandemic

This is an article from 2020, reflective upon the COVID-19 pandemic, but the principles and strategies mentioned are still applicable for HR directors facing any cyber risks or crisis in the workplace due to external factors.

In a recent announcement, the Office of the Privacy Commissioner of Canada (OPC) reaffirmed its commitment to protecting Canadians' privacy during the COVID-19 outbreak, stating that, "[d]uring a public health crisis, privacy laws still apply, but they are not a barrier to appropriate information sharing." Other privacy commissioners throughout Canada have made similar statements.[1]

Given the extraordinary nature of the current situation, organizations are understandably concerned about protecting the safety of their clients and employees. At the same time, they are increasingly being asked to reveal personal information about known or suspected cases of the virus within their establishments and to provide information about their employees and customers to different public authorities. This has led some to implement various screening measures (*e.g.* temperature checks, questionnaires, etc.) to reduce the chances of the virus spreading. Before collecting or disclosing any information about an identifiable individual, organizations must accurately assess their obligations under the laws that govern the protection of personal information in Canada (Canadian Privacy Laws)[2] in order to determine the extent to which they may collect and share such information, and under what conditions.

Employers should also be aware of the increased security risks posed by malicious actors who want to take advantage of the disruption and confusion caused by the virus. In particular, many cyber security experts have warned about an increase in the number of phishing emails about COVID-19. Organizations must ensure that effective security measures are in place to protect both the health and physical safety of their employees and clients, as well as from a cyber risk perspective for employees working remotely.

Below, we provide answers to key questions related to managing privacy and cybersecurity-related issues during a pandemic.

Collecting employee personal information

Can businesses lawfully request their employees disclose whether they have tested positive for the COVID-19 virus or been exposed to certain risk factors? Can employers request that employees undergo certain types of testing or compulsory checks?

Under Canadian Privacy Laws, an organization that collects, uses or discloses personal information is generally required to obtain an individual's consent before disclosing their information to a third party, unless a consent exception applies (see section II of this article for more information on consent).

Necessity

Regardless of the type of information being collected or the practice pursued, an organization must respect the data minimization principle, and limit its collection of personal information to what is necessary to achieve its stated purpose (*e.g.* preserving the health and safety of its employees). Similarly, an organization should avoid screening individuals multiple times in a relatively short period without a legitimate reason.

Reasonable and Legitimate Purposes

Under Canadian Privacy Laws, an organization must collect, use and disclose personal information for purposes that are **reasonable and legitimate in the circumstances**. The notion of reasonableness must be evaluated on a case-by-case basis, taking into account the organization's activities and statutory obligations (*e.g.* health and safety of workers), guidance issued by public health authorities and other health professionals, and the sensitivity, quantity and nature of the personal information involved.

Given that the pandemic has been declared a public health emergency in a number of provinces, and that employers are generally required to preserve the health and safety of their employees, an organization may be justified in collecting some types of information related to an employee's exposure to COVID-19. This may include requiring the employee to disclose whether they recently travelled to an affected region, been in contact with a person that has contracted the virus, or been diagnosed with the virus themselves.

However, given that personal medical information is sensitive, employers should exercise caution and limit collecting of this type of information as much as possible. An employer is advised to collect personal medical information only where there is a reasonable risk that the employee may have been exposed to COVID-19.

An employer should not indiscriminately require employees to undergo periodic testing or screening (*e.g.* temperature checks), as privacy regulators generally consider this practice to be highly invasive, unless the role of the employee justifies this type of screening. In any event, an employer should always ensure that the testing method used is reliable, and weigh the benefits to be gained from a particular practice against the impact it may have on an employee's privacy rights. Employers should also consider whether alternative testing methods or practices may be available that would achieve the same goals in a less intrusive way.

While a practice may not be considered "reasonable or appropriate" today, it may become reasonable in the future depending on the evolution of the pandemic. In other words, the answers to the questions above are moving targets that must periodically be reassessed and adjusted.

The table below lists provisions establishing the reasonableness and necessity requirements for collecting personal information.

Necessity and Reasonableness			
Sections 4, 5, ARPPIPS	**Section 18(1)(k), BC PIPA**	**Section 20(g), Alberta PIPA**	**Section 7(3)(e), PIPEDA**
"Any person carrying on an enterprise who may, for a serious and legitimate reason, establish a file on another person must, when establishing the file, enter its object." "Any person collecting personal information to establish a file on another person or to record personal information in such a file may collect only the information necessary for the object of the file."	"Subject to this Act, an organization may collect personal information only for purposes that a reasonable person would consider appropriate in the circumstances and that fulfill the purposes that the organization discloses under section 10(1)." (*i.e.* the purposes for which they were collected)	"An organization may collect personal information only for purposes that are reasonable." (*i.e.* that a reasonable person would consider appropriate in the circumstances)" "Where an organization collects personal information, it may do so only to the extent that is reasonable for meeting the purposes for which the information is collected."	An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances." "The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization."

Sharing personal information

In the context of a public health emergency such as COVID-19, when can organizations share personal information – including health-related information – with other employees, clients or regulatory authorities, without the consent of the affected individual(s)?

Canadian Privacy Laws provide certain **consent exceptions**. These exceptions may allow organizations to share an individual's personal information with a third party without their consent, in the context of the COVID-19 pandemic. Depending on the consent exception relied on by an organization, and the province in which it operates, the organization may be required to provide notice to the concerned individual that their personal information was disclosed without their consent. In addition, an organization may wish to consider whether there are other factors in favour of notifying the individual whose information has been disclosed, even if there is no legal obligation to notify.

Threat to life, health or security

Generally, organizations in Canada, except in Québec, may disclose personal information without consent when necessary to respond to an emergency that threatens the life, health or security of **any individual**. This means they can disclose an affected employee's personal information within the organization or to its clients. Under PIPEDA and the BC PIPA, an organization must also notify the individual – in

writing and without delay – of this disclosure. There are no equivalent notice requirements under the Alberta PIPA.[3]

In contrast, Québec's ARPPIPS considerably narrows the scope of this exception to situations where the emergency threatens the life, health or security of **the person** whose personal information is disclosed. It is, therefore, less clear whether an organization in Québec would be allowed to disclose an affected employee's personal information within the organization or to its clients.

The table below lists the provisions related to disclosing personal information without consent based on a threat to life, health or security.

Threat to Life, Health or Security			
Section 18(7), ARPPIPS	**Section 18(1)(k), BC PIPA**	**Section 20(g), Alberta PIPA**	**Section 7(3)(e), PIPEDA**
"to a person to whom the information must be communicated by reason of the urgency of a situation that threatens the life, health or safety of the person concerned"	"if there are reasonable grounds to believe that compelling circumstances exist that affect the health or safety of any individual and if notice of disclosure is mailed to the last known address of the individual to whom the personal information relates"	"the disclosure of the information is necessary to respond to an emergency that threatens the life, health or security of an individual or the public"	"made to a person who needs the information because of an emergency that threatens the life, health or security of an individual and, if the individual whom the information is about is alive, the organization informs that individual in writing without delay of the disclosure"

Necessary or reasonable to manage an employment relationship

With the exception of Québec's ARPPIPS, Canadian Privacy Laws enable organizations to collect, use and disclose their employees' personal information without consent for the purposes of "establishing, managing or terminating an employment relationship" between the organization and the individual concerned. Under the BC PIPA and the Alberta PIPA, the collection, use or disclosure must be "reasonable" in order to establish, manage or terminate the employment relationship, whereas under PIPEDA, it must be "necessary," which indicates a higher standard for employers subject to the federal privacy legislation. In addition, an organization relying on this consent exception must notify the individual concerned (*i.e.* the employee) in advance that their personal information will be collected, used or disclosed for those purposes.

Under provincial occupational health and safety laws, employers are generally required to take reasonable measures to provide a safe work environment. Complying with occupational health and safety requirements has been found to fall under the definition of "managing an employment relationship" by the Alberta OIPC.[4] Under this interpretation an organization may be allowed to let its employees know that a co-worker has COVID-19 without obtaining the infected employee's consent, in order to provide a safe work environment.

Québec's ARPPIPS does not contain a similar consent exception. However, a Québec employer may nonetheless be justified in collecting, using or disclosing such information without its employee's consent in order to comply with its obligations to protect the health and safety of its employees, as enshrined in section 46 of the *Charter of Human Rights and Freedoms* and under the *Act Respecting Occupational Health*

and Safety.

In all circumstances and provinces that rely on such consent exceptions, an employer should always ensure that its proposed collection, use or disclosure of personal information is proportionate to the purpose of ensuring workplace health and safety.

The table below lists provisions that govern disclosing personal information without consent for the purpose of managing an employment relationship.

Managing an Employment Relationship			
ARPPIPS	**Section 13, 16, 19, BC PIPA**	**Sections 15, 18, 21, Alberta PIPA**	**Section 7.3, PIPEDA**
N/A	"The collection, use or disclosure is reasonable for the purposes of establishing, managing or terminating an employment relationship between the organization and the individual." "An organization must notify an individual that it will be collecting, using or disclosing employee personal information about the individual and the purposes for the collection, use or disclosure before the organization collects, uses or discloses employee personal information about the individual without the consent of the individual."	"The information is collected, use or disclosed solely for the purposes of establishing, managing or terminating an employment or volunteer-work relationship between the organization and the individual; it is reasonable to collect, use or disclose the information for the particular purpose for which it is being collected, used or disclosed; and in the case of an individual who is a current employee of the organization, the organization has, before collecting, using or disclosing the information, provided the individual with reasonable notification that personal employee information about the individual is going to be collected, used or disclosed and of the purposes for which the information is going to be collected, used or disclosed."	"The collection, use or disclosure is necessary to establish, manage or terminate an employment relationship between the federal work, undertaking or business and the individual; and the federal work, undertaking or business has informed the individual that the personal information will be or may be collected, used or disclosed for those purposes."

Request from government authorities (including public health authorities)

In the context of a public health emergency, Canadian Privacy Laws generally permit the disclosure of personal information to public authorities, as long as it relates to the public health issue. Although there may be certain differences, these statutes generally include consent exceptions when the disclosure is required by law or is for the purpose of enforcing or administering a law. These exceptions may apply to disclosures to public health authorities, which generally have broad permission to collect information from organizations.[5] Organizations may also be required to disclose information to other types of public authorities, such as public safety entities, under emergency legislation or decrees or orders issued under such legislation.

It is also worth noting that disclosures made to public health authorities pursuant to these consent exceptions do not generally require an organization to inform the concerned individual. However, an organization may determine that it wishes to inform said individual anyway, whether they are an employee or a client, even if it is not

legally required.

In this rapidly evolving environment, organizations must **stay up to date** in order to accurately evaluate their obligations, and assess whether they must comply with any additional disclosure requirements in their respective provinces.

The tables below lists the relevant provisions pertaining to disclosing personal information without consent pursuant to applicable law requirement and to public authorities.

Required by Law			
Section 18(4), ARPPIPS	**Section 18(1)(o), BC PIPA**	**Section 20(b), Alberta PIPA**	**Section 7(3)(i), PIPEDA**
"to a person to whom it is necessary to communicate the information under an Act applicable in Québec or under a collective agreement"	"the disclosure is required or authorized by law"	"the disclosure of the information is authorized or required by a statute of Alberta or of Canada, a regulation of Alberta or a regulation of Canada, a bylaw of a local government body, or a legislative instrument of a professional regulatory organization"	"required by law"

Public Authorities			
Section 18(5), ARPPIPS	**BC PIPA**	**Section 20(c), Alberta PIPA**	**Section 7(3)(c.1), PIPEDA**
"to a public body within the meaning of the Act respecting Access to documents held by public bodies and the Protection of personal information (chapter A-2.1) which, through a representative, collects such information in the exercise of its functions or the implementation of a program under its management"	N/A	"the disclosure of the information is to a public body and that public body is authorized or required by an enactment of Alberta or Canada to collect the information from the organization"	"made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that the disclosure is requested for the purpose of administering any law of Canada or a province"

Requirements applicable to all disclosures

Even if an organization is permitted by law to disclose certain personal information without consent in the context of a pandemic, it remains bound by its other obligations under Canadian Privacy Laws. The organization remains accountable to those individuals whose personal information it discloses, and must limit the type, quantity and content of personal information it is disclosing. For instance, in a particular situation, the specific identity of the person whose personal information is disclosed might not need to be divulged, or the reasons why an individual has been asked to self-quarantine may not be relevant. In other words, an organization must ensure that any disclosure of personal information it makes with respect to COVID-19 is:

- Justified by law (on the basis of consent or an exception to the consent requirement);

- Limited to what is necessary to achieve the purpose of the disclosure (otherwise known as the data minimization principle); and
- Documented in sufficient detail to enable individuals to understand the organization's reasoning and justification.[6]

To this end, it is advisable that whenever an organization discloses COVID-19-related personal information about an employee, the organization document the disclosure, including such things as the legal authority for the disclosure, what information was disclosed, who disclosed the information, to whom it was disclosed, the date of the disclosure and other material information (*e.g.* if notice was provided to the individual whose information was disclosed pursuant to any applicable statutory requirement).

Managing cybersecurity risks

What must organizations do to comply with Canadian Privacy Laws and address the cybersecurity risks triggered by remote working arrangements and COVID-19?

Under Canadian Privacy Laws, an organization is required to take adequate security measures to protect the personal information under its custody or control from unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction. More specifically, an organization is responsible for the actions of its employees and service providers who may handle personal information on its behalf. Everyone within an organization must play a proactive role in preserving the security and confidentiality of personal information, especially when working from home.

In practice, this often translates into an obligation to implement physical, organizational and technical measures related to when, where, what and how personal information may be accessed, and by whom. However, considering that many organizations have had to rapidly adapt to the present situation by allowing their employees to work from home, their IT infrastructure and systems may be particularly vulnerable to cyberattacks. In recent weeks, many have seen a large number of phishing emails related to COVID-19 that were designed to take advantage of the mass disruption and confusion caused by the virus.

It is crucial for organizations to take proactive steps to reduce the risk of a successful cyberattack. These steps may include:

- **Review and update the organization's policies and procedures**. Organizations should ensure that their information security and incident response plans are up to date and reflect potential issues related to remote working conditions and the heightened risk of cyberattacks. More specifically, given the rise of cyberattacks taking advantage of the current situation, organizations should ensure that they are **ready to respond** in case of a security incident;
- **Review, update and implement the security measures in place.** These security measures would typically include: monitoring and logging network-related activities to and from the organization's network; encrypting communications containing personal and confidential information through a virtual private network (VPN); and implementing multi-factor authentication measures and other access-based security features (*e.g.* periodic password resets) in order to protect access to employees' accounts;
- **Educate and train employees**. Employee training should focus on specific measures to take when working from home, such as only using organization-supported communication platforms and other IT tools, avoiding the use of free tools that may not afford an adequate level of confidentiality and security, and maintaining prudent practices to limit the extent to which personal information is exposed to other members of the household; and how to detect and report

threats such as phishing emails.

Footnotes

1 For example, in its guidance document, the Office of the Information and Privacy Commissioner of Alberta (AB OIPC) aptly stated that "[p]rivacy laws are not a barrier to appropriate information sharing in a pandemic or emergency situation," while also reminding that "[i]t is important that public bodies, health custodians and private sector organizations know how personal or health information may be shared during a pandemic or emergency situation." The Office of the Information and Privacy Commissioner of British Columbia and the Commission d'accès à l'information du Québec issued similar statements.

2 In Canada, there are four general privacy laws that govern the collection, use and disclosure of personal information in the private sector: the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA), Québec's *Act Respecting the Protection of Personal Information in the Private Sector* (ARPPIPS), British Columbia's *Personal Information Protection Act* (BC PIPA) and Alberta's *Personal Information Protection Act* (Alberta PIPA) (collectively, Canadian Privacy Laws). Private sector organizations in Québec, British Columbia and Alberta are subject to the ARPPIPS, BC PIPA and Alberta PIPA respectively, whereas private-sector organizations operating in other parts of the country are subject to PIPEDA. One major difference between PIPEDA and the aforementioned provincial privacy laws is that the former does not protect the personal information of non-federally regulated employees, whereas the provincial privacy laws do apply to the personal information of employees within those provinces.

3 That said, the AB OIPC recommends that organizations inform their employees of the "specific legislative authority that is engaged" to disclose their personal information without consent.

4 See decision of the AB OIPC P2019-04 at para. 31. See also Order P2010-002, in which the Alberta OIPC held that the organization's disclosure of its former employee's personal information (*i.e.* the fact that he was no longer working for the employer) to contractors and customers were made "solely to manage an employment relationship between the organization and the individual," and that "[t]o find otherwise would result in a situation where an organization could not inform its contractors and customers as to who is currently employed with, or representing, the organization."

5 See Québec's Public Health Act, section 123(3).

6 In its guidance document related to COVID-19, the OPC stated that organizations that rely on a consent exception to disclose personal information should be able "to communicate to the persons involved the specific legislative authority under which this is done."

The content of this article is intended to provide a general guide to the subject matter. Specialist advice should be sought about your specific circumstances.

by Éloïse Gratton , Elisa Henry , Ira Parghi , François Joli-Coeur and A. Max Jarvie, Borden Ladner Gervais LLP