CARTERS
BARRISTERS
SOLICITORS
TRADEMARK AGENTS

CHARITY & NFP LAW BULLETIN NO. 468

MARCH 24, 2020

EDITOR: TERRANCE S. CARTER
ASSISTANT EDITORS: NANCY E. CLARIDGE,
RYAN M. PRENDERGAST AND ADRIEL N. CLAYTON

PRIVACY AND DATA SECURITY IN RESPONSE TO COVID-19

By Esther Shainblum[*]

A. INTRODUCTION

Responses to the COVID-19 pandemic could intersect with privacy and data security concerns in a number of ways. The following is a brief review of some of the privacy and data security issues that are arising in the context of the COVID-19 pandemic. Charities and not-for-profits ("NFPs") should take privacy and data security matters into account when determining the steps that they are taking to manage the situation.

B. THE OPC GUIDANCE

On March 20, 2020, the Office of the Privacy Commissioner of Canada ("OPC") released a guidance, titled *Privacy and the COVID-19 Outbreak* ("Guidance").[1] The Guidance points out that there is privacy legislation at the federal, provincial and territorial levels that govern the collection, use and disclosure of personal information and that, during a public health crisis, privacy laws still apply, but they are not a barrier to appropriate information sharing. It goes on to advise that normal privacy laws authorize the collection, use and disclosure of personal information in the context of a public health crisis, but that under both federal and provincial laws, governments are authorized to declare formal public emergencies. Where that is done, the powers to collect, use and disclose personal information may be further extended and can be very broad.

[*] Esther Shainblum, B.A., LL.B., LL.M., CRM, practices in the areas of charity and not-for-profit law, privacy law and health law with the Carters Ottawa office.
[1] Office of the Privacy Commissioner of Canada, "Privacy and the COVID-19 outbreak" (20 March 2020), online: <https://www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/health-emergencies/gd_covid_202003/>.

The Guidance also discusses certain provisions of the *Personal Information Protection and Electronic Documents Act* ("PIPEDA")[2] that may be relevant to the pandemic. The Guidance points out that organizations that are subject to PIPEDA are normally permitted to collect, use or disclose information only for purposes that a "reasonable person would consider appropriate in the circumstances," and the organizations must obtain the knowledge and meaningful consent of the individual for the collection, use, or disclosure of their personal information. However, there are a number of circumstances when organizations that are subject to PIPEDA may collect, use or disclose personal information without consent. These include situations such as:

- if an individual is critically ill and consent cannot be obtained in a timely way;[3]
- where disclosure is required by law or required to enforce a law, such as where a public health authority has the legislative authority to require the disclosure;[4]
- if an organization has reasonable grounds to believe that an individual has been, is being or is about to be in contravention of a quarantine order;[5] or
- if an individual requires urgent medical attention, and is unable to communicate directly with medical professionals.[6]

PIPEDA applies to all private sector organizations, including charities and NFPs, in respect of the personal information that they collect, use or disclose in the course of commercial activities. Charities and NFPs that operate in provinces that do not have substantially similar provincial privacy legislation may be caught by PIPEDA to the extent that they are engaged in commercial activity and should be aware of these provisions.

[2] *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 ["PIPEDA"].
[3] *Ibid*, para 7(1)(a).
[4] *Ibid*, paras 7(1)(e), 7(2)(d), 7(3)(c.1)(ii)-(iii), 7(3)(i).
[5] *Ibid*, para 7(3)(d)(i).
[6] *Ibid* paras 7(2)(b), 7(3)(e).

C. HANDLING PERSONAL INFORMATION

Charities and NFPs are expected to take steps to protect their employees and volunteers, as well as maintain a safe workplace. They may also have to collect, use or disclose personal information for other purposes, such as in the context of providing services to clients. These responsibilities may involve the collection, use and disclosure of personal information in order to identify individuals who are or may be infected with COVID-19, or who may have been exposed to the infection. Charities and NFPs must balance the competing interests of the privacy interests of the affected individuals against the need to protect the health and safety of the larger community/workplace.

Charities and NFPs should be guided by the fair information principles, which underlie all Canadian privacy statutes, when collecting, using and disclosing personal information. These include the following:

- Charities and NFPs should identify the purposes for which personal information is collected, when or before it is collected. These purposes should be reasonable and appropriate and should be documented, as in the COVID-19 response policy described below. What constitutes "reasonable" purposes in the midst of a pandemic would have to be determined with reference to communications made by public health authorities, medical professionals and other relevant sources.

- Charities and NFPs are accountable for the personal information under their control. Charities and NFPs should put in place and communicate to their staff, volunteers and other stakeholders a COVID-19 response policy, which should document how personal information will be collected, used and disclosed in their organization to prevent and manage the spread of COVID-19.

- Charities and NFPs should obtain consent for the collection, use, or disclosure of personal information. Although a number of privacy statutes may provide exceptions to the requirement to obtain consent in emergency situations, as discussed above, the default position should be that consent is required and legal advice should be obtained before making the determination that it is not required. In determining the form of consent to be obtained, charities and NFPs should generally obtain express consent when the information is likely to be considered sensitive, and may wish to seek legal advice in order to make this determination.

- Charities and NFPs should limit their collection, use and disclosure of personal information to what is necessary for the purposes identified. What is necessary in the circumstances will likely depend on direction from public health authorities, medical professionals and other relevant sources. While the identity of an individual who tested positive for COVID-19 may have to be disclosed to certain individuals in certain situations, such as to an employee's supervisor, it may not be necessary to disclose the person's identity to others and care should be taken to ensure that individuals are not inadvertently identified. Conversely, charities and NFPs should also take into consideration any occupational health and safety legislation that may require the collection, use and disclosure of personal information, such as if COVID-19 is contracted in the workplace.[7]

- Charities and NFPs should protect the personal information that they have collected by security safeguards appropriate to the sensitivity of the information. As many organizations now have employees working remotely in order to respond to the risks of exposure and contagion, they should consider whether additional security measures are required to protect personal information in the organization's custody.

Charities and NFPs must carefully balance the competing objectives of public health and individual privacy, in addition to taking a measured approach when managing personal information in the context of the COVID-19 pandemic. Even if a charity or NFP is not subject to PIPEDA or other specific privacy legislation, violations of privacy can give rise to damage awards, tort claims and class action litigation in the courts.

D. DATA SECURITY

As noted above, many employees are working remotely in order to minimize exposure to the disease. This has also become a critical requirement to continue working since the Ontario government's order on March 23, 2020 for the mandatory closure of all non-essential workplaces to fight the spread of COVID-

[7] For further discussion on the obligations of charities and NFPs, as employers, during the COVID-19 pandemic, see Barry W. Kwasniewski, *Charity & NFP Law Bulletin* No. 465, "Employer Obligations and Considerations in Response to the Covid-19 Pandemic" (24 March 2020), , online: Carters Professional Corporation <http://www.carters.ca/pub/bulletin/charity/2020/chylb465.pdf>.

19, effective March 24 at 11:59pm.[8] Charities and NFPs should increase their cyber-security measures to guard against cyber criminals who are taking advantage of the fact that many home devices are not securely protected. According to the *Toronto Star*, "most Canadians don't realize how insecure their home internet connection is compared to the system in an office environment."[9]

Under the *Canada Not-for-Profit Corporations Act* ("CNCA"), the Ontario *Not-for-Profit Corporations Act* ("ONCA") (expected to be proclaimed in 2020), and the Ontario *Corporations Act* ("OCA"), directors and officers of charities and NFPs are required to act honestly and in good faith with a view to the best interests of the company, and to exercise the care, diligence, and skill that a reasonably prudent person would exercise in comparable circumstances. Directors and officers of charities and NFPs impacted by privacy breaches may be exposed to the risk of litigation and claims that they are liable for the breach of their duties.[10]

The "Business Judgment Rule" protects directors and senior officers against hindsight and second guessing by third parties and the courts, provided that the directors have made an informed and reasonable decision. Directors can demonstrate that they met the duty of care and made an informed, reasonable decision by, among other things, confirming that the organization has appropriate safeguards in place to protect personal information.

Charities and NFPs whose employees are now working remotely should therefore take steps to protect the organization from cyber criminals, including:

- Building a culture of privacy and training employees to be extra-vigilant against phishing and scams related to COVID-19;

[8] Government of Ontario, "Ontario Orders the Mandatory Closure of All Non-Essential Workplaces to Fight Spread of COVID-19" (News Release by the Office of the Premier, 23 March 2020), online: Newsroom <https://news.ontario.ca/opo/en/2020/03/ontario-orders-the-mandatory-closure-of-all-non-essential-workplaces-to-fight-spread-of-covid-19.html?utm_source=ondemand&utm_medium=email&utm_campaign=p>.
[9] Toronto Star, "Working from home? You're likely now at greater risk of being hacked, experts say" (18 March 2020), online: <https://www.thestar.com/news/gta/2020/03/18/working-from-home-youre-likely-now-at-greater-risk-of-being-hacked-experts-say.html>.
[10] For further discussion on directors' and officers' liability, see Terrance S Carter & Ryan M Prendergast, *Charity & NFP Law Bulletin* No. 464, "Due Diligence by Directors and Officers of Charities and NFPs in Response to COVID-19" online: Carters Professional Corporation <http://www.carters.ca/pub/bulletin/charity/2020/chylb464.pdf>.

- Keeping enterprise software up to date to reduce the risk of hacking and malware;
- Setting up a virtual private network to be used by employees for accessing work data;
- Encrypting data on portable enterprise devices and removable media;
- Ensure that data is backed up regularly
- Ensuring adequate and trustworthy IT support is available for remote workers;
- Restricting access to sensitive data on a need-to-know basis;
- Having a clear privacy breach response protocol in place; and
- Obtaining adequate cyber insurance coverage to protect the organization against cyber-crime and fraud.

Charities and NFPs should also require their employees to take a number of steps, including:

- Upgrading home routers to the latest version and ensuring their Wi-Fi connection is secure;
- Fortifying their passwords using multi-factor authentication where possible;
- Using the organization's virtual private network to access work data;
- Ensuring that data is encrypted and regularly backed up;
- Using only organization-provided or approved devices, and software that is regularly updated to protect against viruses and malware; and
- Storing work devices safely and securely, without access to anyone else.

E. CONCLUSION

Charities and NFPs will encounter a number of privacy and data security issues during the COVID-19 pandemic. They should ensure that adequate strategies and measures are put in place to mitigate the risks of privacy and data breaches.