

CARTERS

BARRISTERS
SOLICITORS
TRADEMARK AGENTS

SPECIAL CARTERS COVID-19 WEBINAR: LEGAL ISSUES FOR CHARITIES AND NFPS

April 9, 2020

PRIVACY AND DATA SECURITY ISSUES IN RESPONSE TO COVID-19

By Esther Shainblum, B.A., LL.B., LL.M., CRM


eshainblum@carters.ca
1-866-388-9596


© 2020 Carters Professional Corporation

CARTERS PROFESSIONAL CORPORATION
BARRISTERS . SOLICITORS . TRADEMARK AGENTS
TOLL FREE: 1-877-942-0001

Toronto Ottawa Orangeville

www.carters.ca www.charitylaw.ca www.antiterrorismlaw.ca

 <p>BARRISTERS SOLICITORS TRADEMARK AGENTS</p>	<p>Special Carters COVID-19 Webinar: Legal Issues for Charities and NFPs April 9, 2020</p>
<p>Privacy and Data Security Issues in Response to COVID-19</p> <p>Esther Shainblum, B.A., LL.B., LL.M., CRM eshainblum@carters.ca 1-866-388-9596</p> <p>© 2020 Carters Professional Corporation</p>	
<p>CARTERS PROFESSIONAL CORPORATION TOLL FREE: 1-877-942-0001</p>	<p>Toronto Ottawa Orangeville www.carters.ca www.charitylaw.ca www.antiterrorismlaw.ca</p>

2	
	<p>Esther Shainblum, B.A., LL.B., LL.M., CRM – Ms. Shainblum practices at Carters Professional Corporation in the areas of charity and not for profit law, privacy law and health law. From 2005 to 2017 Ms. Shainblum was General Counsel and Chief Privacy Officer for Victorian Order of Nurses for Canada, a national, not-for-profit, charitable home and community care organization. Before joining VON Canada, Ms. Shainblum was the Senior Policy Advisor to the Ontario Minister of Health. Earlier in her career, Ms Shainblum practiced health law and corporate/commercial law at McMillan Binch and spent a number of years working in policy development at Queen’s Park.</p> <p>eshainblum@carters.ca 1-866-388-9596</p>
<p>www.charitylaw.ca</p>	<p>www.carters.ca</p>

INTRODUCTION

- Charities and Not-for-Profits (“NFPs”) must be aware of privacy and data security issues when dealing with this crisis
- Privacy laws continue to apply – must balance protecting individual privacy against protecting the health and safety of the larger community/workplace
- Brief presentation - two key areas of risk:
 - COVID-19 and personal information in the workplace
 - Cyber-safety

A. HANDLING PERSONAL INFORMATION – SCREENING AND MANAGING COVID-19 IN THE PHYSICAL WORKPLACE

- Charities and NFPs may have to collect, use and disclose personal information in order to:
 - Protect their employees, volunteers and clients
 - Maintain a safe workplace
 - Provide services to clients
- Charities and NFPs may adopt screening procedures including:
 - Taking temperatures of people coming into the workplace
 - Asking questions about travel history, family history, living arrangements, physical symptoms

- Management of COVID-19 in the workplace may include advising co-workers, clients and others that someone has been diagnosed, requiring certain individuals to self-isolate and making other notifications, if applicable, such as under OHSA
- All of these actions constitute the collection, use and disclosure of personal information
- Depending on where charities or NFPs operate, different privacy legislation, or no privacy legislation, may apply
- Charities and NFPs should continue to abide by the following basic, overarching privacy law principles when collecting, using and disclosing personal information in response to the COVID-19 emergency

1. Reasonable Purposes

- Charities and NFPs should only collect, use or disclose personal information for purposes that are reasonable and appropriate
 - Likely that collecting, using and disclosing personal information to prevent the spread of the disease would be seen as reasonable

2. Identify Purposes - A COVID-19 Response Policy

- Charities and NFPs should identify the purposes for which personal information is collected at or before the time of collection
 - Charities and NFPs should put in place and communicate to their employees, volunteers, clients and other stakeholders a COVID-19 response policy
 - The COVID-19 response policy should document how the charity or NFP will collect, use and disclose personal information to prevent and manage the spread of COVID-19
 - Will also assist in obtaining meaningful consent, to be discussed in a few minutes

3. Minimize Collection, Use And Disclosure

- Charities and NFPs should limit their collection, use and disclosure of personal information to the minimum necessary for the purposes identified
 - Should not collect more personal information than required to fulfil the identified purposes
 - What is necessary will likely depend on direction from public health authorities, medical professionals and other relevant sources
 - Use and disclosure of personal information should also be minimized to that which is necessary to achieve the purposes

4. Consent

- 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, the default position should be that consent is required
 - Legal advice should be obtained before making the determination that consent is not required
 - Must also consider the appropriate form of consent – e.g. express or implied - depends on the nature of the information and the reasonable expectations of the person

- Charities and NFPs should obtain express consent when the personal information is likely to be considered sensitive
 - such as health information
- Consent must also be meaningful
 - must understand the nature, purposes and consequences of what they are consenting to
 - COVID-19 response policy can be useful in this regard

5. Safeguarding

- Charities and NFPs should protect the personal information that they have collected by security safeguards appropriate to the sensitivity of the information
 - Should include physical, technological and administrative safeguards
 - Charities and NFPs with remote workforce should consider whether additional security measures are required to protect personal information

B. DATA SECURITY

- Many employees are working remotely due to social distancing and mandatory closure of all non-essential workplaces
- These arrangements – often hastily assembled – have put charities, NFPs and other workplaces at increased risk of cyber attacks and privacy breaches
- Cyber attacks have intensified as a result of the pandemic, with increases in the incidence of phishing, malware attacks and email scams
- One U.S. study found a 667% increase in cyber attacks in March 2020
(<https://thehill.com/policy/cybersecurity/490232-cyber-threats-spike-during-coronavirus-pandemic>)

- Cyber criminals are also taking advantage of the fact that many home devices are not securely protected
- Toronto Star - “most Canadians don’t realize how insecure their home internet connection is compared to the system in an office environment”
<https://www.thestar.com/news/gta/2020/03/18/working-from-home-youre-likely-now-at-greater-risk-of-being-hacked-experts-say.html>
- Other risks of remote work/access include using personal devices to access core IT systems, sharing computers and devices, not keeping devices, passwords and documents secure

- Difficult to keep systems secure, to keep track of sensitive information and who is accessing it and to find out about and respond to privacy breaches
- Challenging to protect personal information and confidential business information
- Directors and officers of charities and NFPs may be exposed to the risk of litigation, including potential claims of breach of their fiduciary duties and breach of duty of care
- Charities and NFPs need to take steps to ensure that personal information is adequately safeguarded, as discussed on the next few slides

1. What Charities And NFPs Should Do To Protect Personal Information

- Build a culture of privacy and training employees to be extra-vigilant against COVID-19 phishing scams
- Educate staff about the need to comply with privacy law and organizational privacy policies while working remotely
- Keep enterprise software up to date to reduce the risk of hacking and malware
- Set up a virtual private network to be used by employees for accessing work data
- Understand where personal information is stored and restricting access on a need-to-know basis
- Provide charity/NFP owned devices to employees as much as possible

- Vet employee owned devices to ensure that they meet security standards
- Encrypt data on portable enterprise devices and removable media
- Have robust contracts with third-party service providers
- Ensure that data is backed up regularly
- Ensure adequate and trustworthy IT support is available for remote workers
- Have clear privacy breach and security incident response protocols in place and ensuring that staff is informed of them
- Obtain adequate cyber insurance coverage to protect the organization against cyber-crime and fraud

2. What Remote Workforce Should Do To Protect Personal Information

- Charities and NFPs should also require their employees to take a number of steps, including:
 - Use only charity/NFP provided or approved devices and software that is regularly updated to protect against viruses and malware
 - Upgrade home routers to the latest version and ensure their Wi-Fi connection is secure
 - Fortify their passwords using multi-factor authentication where possible
 - Only access work data using the charity/NFP's virtual private network

- Avoid sending sensitive information via email and only using secure charity/NFP resources to share files
- Store work devices safely and securely, without access to anyone else
- Be suspicious of emails
 - that refer to the coronavirus,
 - that ask them to click on links or open files,
 - that create an image of urgency or severe consequences or
 - that ask for unusual things or information

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

CARTERS

BARRISTERS
SOLICITORS
TRADEMARK AGENTS

Disclaimer

This handout is provided as an information service by Carters Professional Corporation. It is current only as of the date of the handout and does not reflect subsequent changes in the law. This handout is distributed with the understanding that it does not constitute legal advice or establish a solicitor/client relationship by way of any information contained herein. The contents are intended for general information purposes only and under no circumstances can be relied upon for legal decision-making. Readers are advised to consult with a qualified lawyer and obtain a written opinion concerning the specifics of their particular situation.

© 2020 Carters Professional Corporation

