CARTERS

BARRISTERS
SOLICITORS
TRADEMARK AGENTS

SPRING 2017 - CARTERS CHARITY & NFP WEBINAR SERIES

May 25, 2017

DO'S AND DON'TS OF DONOR INFORMATION

By Terrance S. Carter, B.A., LL.B., TEP, Trade-mark Agent
tcarter@carters.ca

and

Ryan M. Prendergast, B.A., LL.B.
rmp@carters.ca

1-877-942-0001

© 2017 Carters Professional Corporation

CARTERS
BARRISTERS
SOLICITORS
TRADEMARK AGENTS

SPRING 2017
CARTERS CHARITY & NFP WEBINAR SERIES
May 25, 2017

Do's and Don'ts of Donor Information

By Terrance S. Carter, B.A., LL.B., TEP, Trade-mark Agent
tcarter@carters.ca
Ryan M. Prendergast, B.A., LL.B.
rmp@carters.ca

1-877-942-0001

© 2017 Carters Professional Corporation

Terrance S. Carter, B.A., LL.B, TEP, Trade-mark Agent
Managing Partner of Carters, Mr. Carter practices in the area of charity and not-for-profit law, and is counsel to Fasken Martineau on charitable matters. Mr. Carter is a co-author of *Corporate and Practice Manual for Charitable and Not-for-Profit Corporations* (Carswell), a co-editor of *Charities Legislation and Commentary* (LexisNexis Butterworths, 2017), and co-author of *Branding and Copyright for Charities and Non-Profit Organizations* (2014 LexisNexis Butterworths). He is recognized as a leading expert by *Lexpert* and *The Best Lawyers in Canada*, and is a Past Chair of the Canadian Bar Association and Ontario Bar Association Charities and Not-for-Profit Law Sections. He is editor of www.charitylaw.ca, www.churchlaw.ca and www.antiterrorismlaw.ca.

Ryan Prendergast, B.A., LL.B.
Called to the Ontario Bar in 2010, Mr. Prendergast joined Carters with a practice focus of providing corporate and tax advice to charities and non-profit organizations. Ryan is a regular speaker and author on the topic of directors' and officers' liability and on the topic of anti-spam compliance for registered charities and not-for-profit corporations, and has co-authored papers for the Law Society of Upper Canada. In addition, Ryan has contributed to The Lawyers Weekly, Hilborn:ECS, Ontario Bar Association Charity & Not-for-Profit Law Section Newsletter, Charity & NFP Law Bulletins and publications on www.charitylaw.ca.

3

INTRODUCTION: WHY YOU SHOULD CARE

- Donor information constitutes personal information that must be respected and protected by the charity
- Who are donors? In addition to those making donations, they can include members, employees, patients, and even customers where a gift is tied to a donation
- Donor information can include the donor name, mailing address, email address, phone numbers, birthdate, name of family members, photos, financial information, name of business, place of employment, preferred donation restrictions and even health information

www.carters.ca www.charitylaw.ca

4

- What can go wrong?
  - Good intention sharing of personal information with volunteers without appropriate restrictions
  - Intentional intrusion by employees
  - Cyber attacks
  - Information requests by CRA
  - Information requests by donor
  - Information requests by the press
- Canadian laws concerning the collection and use of donor personal information vary from province to province and are in an ongoing state of flux
- Failure to comply with applicable legal requirements for the use and protection of donor information can result in serious consequences for the charity and its directors
- This presentation provides an explanation of the legal context and some “Do’s” and “Don’ts” involving donor information

www.carters.ca www.charitylaw.ca

5

PART I - UNDERSTANDING THE LEGAL CONTEXT

A. Overview

- Respecting and protecting donor information requires an understanding of applicable privacy and related law
- There is no single source of law in Canada dealing with donor information
- Instead, there are complicated, integrated, and highly nuanced privacy and related laws in place
- The primary statutory sources of privacy laws are:
  - Federal private sector legislation, e.g., *Personal Information Protection and Electronic Documents Act*
  - Provincial private sector "substantially similar" legislation, e.g., Ontario *Personal Health Information Protection Act* and public sector privacy legislation, e.g., *Freedom of Information and Protection of Privacy Act*
  - *Canada's Anti-Spam Legislation*

www.carters.ca www.charitylaw.ca

6

- In addition to these specific statutory sources of privacy legislation, there are other related sources of law that may give rise to obligations for charities in dealing with donor information:
  - Common Law;
  - *Income Tax Act* disclosure and books and record keeping obligations;
  - National Do-Not-Call List;
  - Anti-terrorism and anti-money laundering legislation;
  - Sector Standards; and
  - Contractual Obligations

www.carters.ca www.charitylaw.ca

7

B. Legislative Sources of Privacy Law

1. General Statutes

a) Federal Private Sector Legislation

- The *Personal Information Protection and Electronic Documents Act* ("PIPEDA") is the main private-sector legislation for protecting privacy
- PIPEDA applies to the collection, use or disclosure of personal information in the course of a "commercial activity" – broadly defined as any transaction, act or conduct of a commercial character, and includes the sale, lease or exchange of donor, membership or other fundraising lists
- Given that it is hard to predict when a "commercial activity" by a charity may occur, it is generally best for a charity to take steps to comply with PIPEDA

8

- Organizations that are subject to PIPEDA must also follow the *Model Code for the Protection of Personal Information* which is incorporated in PIPEDA and includes the following ten principles:
  1. **Accountability**: an organization is responsible for personal information under its control and shall designate an individual to ensure compliance
  2. **Identifying Purposes**: purposes for collecting personal information shall be identified at or before collection
  3. **Consent**: consent (express or implied) is required for the collection, use or disclosure of personal information (some exceptions)

9

4. **Limiting Collection**: collection of personal information shall be limited to what is necessary for the purposes identified by the organization
5. **Limiting Use, Disclosure, and Retention**: personal information shall not be used or disclosed for purposes other than those for which it was collected (some exceptions), and shall be retained only for as long as necessary to fulfill those purposes or to comply with relevant laws
6. **Accuracy**: personal information shall be accurate, complete and up-to-date
7. **Safeguards**: personal information shall be protected by appropriate security safeguards

www.carters.ca www.charitylaw.ca

10

8. **Openness**: organizations shall make readily available to individuals specific information about its policies/practices relating to the management of personal information
9. **Individual Access**: upon request, an individual shall be informed of the existence, use, and disclosure of their personal information and shall be given access to it and be able to challenge the accuracy and completeness of the information
10. **Challenging Compliance**: individuals shall be able to address compliance concerns with the above-noted principles with a designated individual

- These ten principles should be reflected in a privacy policy for the charity

www.carters.ca www.charitylaw.ca

11

b) Provincial Privacy Legislation

- An organization may be exempt from PIPEDA if the province has enacted privacy legislation "substantially similar" to PIPEDA - in that case, the substantially similar provincial legislation would apply instead of PIPEDA
- Alberta, British Columbia, and Quebec have passed substantially similar legislation
- Some jurisdictions may have stricter application than PIPEDA
  - B.C.'s *Personal Information Protection Act* (PIPA) applies to all organizations and to all personal information held by organizations, unless stated otherwise
  - PIPA expressly states that an "organization" includes a not-for-profit organization

12

  - PIPA differs fundamentally from PIPEDA, such that it applies to the entire private sector (subject to limited exceptions), in both commercial and non-commercial transactions

- Determining the jurisdictional question of which legislation (provincial or federal) applies is complex, and is a question that the Office of the Privacy Commission of Canada ("OPC") investigates at the time a complaint is launched, taking into account:
  - the location in which the activity complained of takes place;
  - the location of preparatory activities;
  - the location and residency of the parties involved; and
  - the location of the contract

13

- The OPC has stated "organizations faced with this kind of scenario [where more than one law may be applicable] may look at the differences between the laws. [...] If you follow the more stringent requirement all the time, you will very likely comply with both laws."
- This means that from a practical context, if a charity is fundraising across Canada, either by mail or by the internet, it is important for the charity to establish appropriate protocols that will ensure compliance with all applicable provincial and federal privacy legislation

14

2. Sector Specific Privacy Legislation

- Ontario, New Brunswick and Newfoundland have passed substantially similar legislation with respect to personal health information (e.g., in Ontario, the *Personal Health Information Protection Act* ("PHIPA"))
- PHIPA generally applies to the collection, use and disclosure of personal *health* information in Ontario by health information custodians or the agents of them, and to anyone that receives information from a health information custodian
- The definition of "health information custodian" ("HIC") is central to the application of PHIPA and is deceptively complex - it extends to organizations that have "custody or control over personal health information as a result of or in connection with that person's or organization's powers, duties or work"

15

- Examples of HICs include practitioners, hospitals, psychiatric facilities, long term care homes, laboratories, and ambulance service providers
- *Freedom of Information and Protection of Privacy Act* ("FIPPA") applies to the provincial government and many "institutions" (e.g., hospitals, universities), and governs the use of *non-health* personal information held by hospitals
- Personal *health* information held by hospitals is governed by PHIPA (and not FIPPA)
- Although hospital foundations are not directly subject to FIPPA, FIPPA has an impact on hospitals' ability to disclose information to associated foundations for fundraising

www.carters.ca www.charitylaw.ca

16

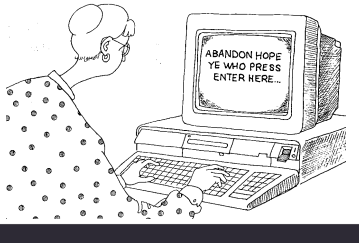
- Foundations may collect personal information independently from the hospital - such personal information will not be subject to FIPPA (though it may be subject to other privacy legislation)
- FIPPA has two main purposes. It establishes:
  - a privacy protection regime for personal information held by "institutions" - applies to the sharing of information by hospitals with foundations (e.g., for fundraising)
  - a freedom of information regime requiring institutions to respond to requests for access to records - may include any hospital records about a foundation, and any foundation records held by a hospital (subject to certain exclusions, e.g., records relating to the operations of a hospital foundation and to charitable donations made to a hospital)

www.carters.ca www.charitylaw.ca

17

3. Anti-Spam Legislation

- Canada's Anti-spam legislation ("CASL") prohibits organizations to send, or cause to be sent, "commercial electronic messages" ("CEM") unless:
  - The recipient of the CEM has consented (express or implied)
  - The CEM contains prescribed information
  - CASL regulations exclude CEMs sent by, or on behalf of, registered charities if the message has a "primary purpose" of raising funds for the charity



18

  - Came into force on July 1, 2014
    - Transition period until July 1, 2017 - existing implied consents where the relationship included communication of CEMs extended for a period of 3 years following the coming into force date of July 1, 2014
    - New implied consents that arise after July 1, 2014 are not covered by the transitional provisions in CASL
- Private right of action for CASL violations (this includes class actions) as of July 1, 2017
- Sections of the Canadian Bar Association, amongst others have recommended that the government delay bringing the private right of action provisions into force until the statutory review and a thorough analysis of the implications of the private right has been completed

19

4. National Do-Not-Call List

- On September 30, 2008, the Canadian Radio-television and Telecommunications Commission ("CRTC") launched Canada's National Do-Not-Call List ("National DNC List")
  - Registered charities are among a select list of organizations exempted from the National DNC Rules
  - But must still comply with the Telemarketing Rules, which include a requirement to maintain a do-not-call list
  - Entities that use telemarketing must still register with, and provide information to the National DNC List operator, pay applicable fees, and maintain records on registration and payment

20

5. Anti-Terrorism and Money Laundering Legislation

- *Anti-Terrorism Act*, 2015, Bill C-51
  - Received Royal Assent on June 18, 2015
  - Charities operating in conflict areas may be particularly affected by the proposed amendments, which include:
    - *Security of Canada Information Sharing Act, 2015* authorizes and facilitates the sharing of information among government agencies (e.g., CRA, RCMP and CSIS) in situations where there is "activity that undermines the security" of Canada
- The 2001 *Anti-Terrorism Act* already permits the government of Canada to share information with foreign institutions and agencies

21

6. Key Principles from Privacy Legislation

- Charities and gift planners are responsible for donor personal information under their control where privacy legislation applies
- Despite their differences, all privacy legislation in Canada generally imposes two main categories of obligations on organizations regarding the collection, use and disclosure of donor personal information:

  a) First - the required consent (expressed or implied) being obtained prior to any collection, use or disclosure of personal information, subject to certain specified exemptions

www.carters.ca www.charitylaw.ca

22

  b) Second - each organization is required to comply with various administrative obligations including:
     - Appointing a privacy officer to oversee compliance
     - Developing public privacy policies and internal practices
     - Maintaining the security of the information
     - Responding to complaints and access requests
     - Developing contracts with any third parties
     - Identifying purposes for using the information
     - Ensuring the purposes for use are reasonable
     - Limiting the collection to what is necessary
     - Limiting the use, disclosure, retention of information
     - Ensuring the accuracy of the information

www.carters.ca www.charitylaw.ca

23

C. Common Law Sources of Privacy Law

- There are also "judge-made" laws (i.e., common law) that have established privacy torts (e.g., a civil personal wrong)
- In *Jones v. Tsige*, 2012, the Ontario Court of Appeal recognized the tort of "intrusion upon seclusion," which is essentially a breach of privacy
- The Court stated that the tort occurs when:
  - "The conduct complained of is intentional or reckless, the person's private affairs or concerns were unlawfully invaded, and a reasonable person would regard the invasion as highly offensive, causing distress, humiliation or anguish"

www.carters.ca www.charitylaw.ca

24

- In *Doe 464533 v. N.D.,* 2016, the Ontario Superior Court of Justice recognized the tort "public disclosure of private facts"
- The Court stated that the tort occurs when:
  - "One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of the other's privacy, if the matter publicized, or the act of the publication (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public"

www.carters.ca www.charitylaw.ca

25

D. *Income Tax Act*

- The *Income Tax Act* governs how CRA officials must protect taxpayer information
  - Section 241 sets out when CRA officials may be permitted to disclose charity information of the registered charity to other government officials, individual taxpayers or the public, including the circumstances in subsection 241(4)
  - Under freedom of information legislation in Canada, (e.g., *Access to Information Act* or the *Privacy Act*), certain taxpayer information held by CRA may be disclosed
  - With respect to registered charities, subsection 241(3.2) identifies taxpayer information relating to registered charities that may be released to the public (e.g., governing documents of the charity)

26

  - CRA can request donor information in the course of a CRA audit
    - *Redeemer Foundation* case - concerning audit powers, SCC determined that donor lists are part of a charity's books and records, which the CRA can obtain without judicial authorization
  - For gifts of $10,000 or more that a charity receives from a donor who is not resident in Canada, the charity has to report on the T3010 the identity of the donor and the amount of the gift unless the donor is:
    - a Canadian citizen;
    - employed in Canada;
    - carrying on business in Canada; or
    - a person that has disposed of taxable Canadian property

27

E. Sector Standards

- Various umbrella organizations for charities in Canada set out standards for their members concerning the handling and protocols of donor information
- Some examples in this regard include:
  - Imagine Canada - Standards Program
  - CAGP - Code of Ethics
  - AFP - Code of Ethical Standards
  - CCCC - CCCC Seal of Organizational Integrity and Accountability

28

F. Contractual Obligations

- Charities may have obligations to deal with donor information under contract (e.g., gift agreements, grant agreements and government funding agreements)
- As well, contracts which provide for protection of personal information should be in place with any third party (e.g., partners) and should consider:
  - The “ownership” of personal information of donors, beneficiaries, etc.
  - The storage of personal information
  - A comparable level of protection of personal information while the information is being processed by the third party
  - Consequences of a data breach by the service provider (e.g., indemnification, insurance etc.)

29

PART II – DO'S AND DON'TS OF DONOR INFORMATION

A. The Do's of Donor Information

1. Do Update And Implement A Privacy Policy At The Operational Level

- A privacy policy is an organic document that needs to be updated frequently and should be specific to your organization
- It must also be implemented at the operational level
- Failure to properly implement a privacy policy can lead to exposure to liability for deceiving the public
- Be cautious not to include misleading claims in the privacy policy (e.g., "we will never ever share your personal information no matter what")

30

2. Do Coordinate Privacy Considerations With A Social Media Policy

- The evolution of information sharing online has called into question how social media impacts individuals' privacy
- Social media has spurred a change in how individuals and organizations view and protect personal information
- Content posted on social media sites often include personal information and may be subject to privacy laws
- To help manage risk, organizations should consider:
  - Implementing a social media policy
  - Requiring consent for the posting of photographs and videos
  - However, avoid pictures, videos or any personal information involving minors since consent by parents or guardians is not enforceable

31

3. Do Be Prepared To Address Data Breaches

- One of the fastest growing areas of class actions involves data breaches (e.g., insecure disposal of records, lost/stolen devices, unauthorized access, etc.)
- The consequences of a data breach can be very serious and result in enormous potential liability
- The appropriate responses to a data breach are of critical importance - if appropriate and timely, such responses can pre-empt, at times defend against and mitigate the organizations exposure to liability

32

- Some prudent steps to help mitigate the chances of a data breach include:
  - Implement written information security and privacy policies regarding personal information
  - Designate an individual to oversee compliance with applicable legislation (e.g., privacy officer)
  - Promote awareness by regularly training employees
  - Keep paper documents in locked cabinets
  - Shred paper documents and securely destroy/erase portable devices (once acceptable in accordance with CRA's record keeping policies)
  - Limit who has access to building keys or alarm codes

33

- Use anti-virus software and stay current with security patch updates
- Use strong passwords that are often changed

- Best practices for responding to a data breach to help mitigate liability include:
  - Don't have one!
  - Have a data breach response plan
  - Understand the scope of the breach
  - Make appropriate notifications
  - Conduct post-breach analysis
  - Contact legal counsel to determine which laws govern your next steps, such as any obligations to report the breach to the relevant privacy commissioner

www.carters.ca www.charitylaw.ca

34

4. Do Review Insurance To Determine If There Is Coverage For Privacy Breaches

- A number of insurers are now providing liability coverage for privacy breaches
- Important to ensure that directors and officers policy includes coverage for liabilities associated with privacy or network security
- However, as with any insurance policy, it is important to read the fine print because the "devil is in the details" when it comes to what is included and excluded in an insurance policy
- It may be prudent to seek legal advice to review the scope of insurance coverage
- Also consider obtaining cyber attack insurance

www.carters.ca www.charitylaw.ca

35

5. Do Have Appropriate Safeguards When Storing Donor Information Using Cloud Computing

- With the emergence of cloud technology, a huge amount of personal and business information has migrated from personally owned hard drives to remote servers managed by data companies
- In particular, since cloud computing may involve cross-border transfers of information, if the data involved includes personal information, organizations should be cognizant of privacy laws applicable to such transfers
- Before "moving to the cloud", charities should be aware of applicable laws and guidance from the privacy commissioners respecting cross-border transfer of personal information

www.carters.ca www.charitylaw.ca

36

- Some legislation contains specific requirements or restrictions related to such activities. For example, privacy legislation in:
  - Quebec provides that enterprises that communicate personal information outside Quebec must first take all reasonable steps to ensure that the information will not be used for unauthorized purposes
  - Alberta contains certain notice and policy requirements if an organization uses a service provider outside Canada
  - Public sector privacy legislation in British Columbia and Nova Scotia generally requires that personal information be stored and accessed only in Canada (subject to certain exceptions, including where consent is obtained)

www.carters.ca www.charitylaw.ca

37

  - Health information privacy legislation in Ontario, Nova Scotia and Newfoundland & Labrador also contains some limitations on cross-border transfers of personal information without consent
  - PIPEDA does not prohibit the storage of data outside Canada, but there are administrative hurdles that must be met, including a requirement to obtain knowledgeable consent to collection, use and disclosure of personal information, as well as general security, openness and accountability obligations
- Charities must consider applicable legal requirements and restrictions, as well as the sensitivity of the information and the reasonable expectations of affected individuals, and carefully review and consider contracts governing cloud computing and/or server arrangements

38

- As well, the *Income Tax Act* states that books and records must be kept "at an address in Canada recorded with the Minister"
- Utilizing servers outside of Canada can be problematic so important to seek legal advice
- For more information see:
  - Guidance CG-002, Canadian registered charities carrying out activities outside Canada
  - http://www.cra-arc.gc.ca/chrts-gvng/chrts/prtng/bks-eng.html
  - http://www.carters.ca/pub/seminar/chrchlaw/2015/8rainsbooksandrecords.pdf

39

6. Do Coordinate Donor Information with a Record Retention Policy

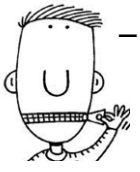
- Donor information forms part of the books and records that charities must keep, and therefore must be held subject to applicable statutory retention periods
- Retention periods for books and records for tax purposes under the ITA depends on the type of book or records (e.g., 6 years from the end of the tax year or two years from dissolution)
- There are also corporate law record requirements
- As a result, a charity should consider the protection of donor information in conjunction with the development of a record retention policy

www.carters.ca www.charitylaw.ca

40

7. Do Limit Access To Donor Personal Information On A "Need-To-Know" Basis

- Legal framework for donor information generally requires that personal information be kept secure while it is being held
- Access to personal information as defined by role, (e.g., "need-to-know") is one way to keep information secure
  - Limit access by employees and volunteers to donor information to the minimal amount needed for them to fulfill their duties
  - Consider the role of board members and others in senior management positions in determining their access



www.carters.ca www.charitylaw.ca

41

8. Do Implement A CASL Compliance Strategy

- Due diligence defence provided under section 54(1) of CASL may help mitigate against liability, or reduce the imposition of a penalty by the Canadian Radio-television and Telecommunications Commission ("CRTC")
- June 19, 2014, the CRTC released Compliance and Information Bulletin CRTC 2014-326 - describes important components of an effective corporate compliance program and provides guidance to develop such a program

42

- What should a CASL compliant policy include?
  - establish internal procedures for compliance with the CASL;
  - address related training that covers the policy and internal procedures;
  - establish auditing and monitoring mechanisms for the corporate compliance program(s);
  - establish procedures for dealing with third parties (e.g., partners and subcontractors) to ensure that they comply with CASL;
  - address record keeping, especially with respect to consent; and
  - contain a mechanism that enables employees to provide feedback to the chief compliance officer or point person

43

9. Do Have A Protocol To Address Access Requests For Personal Information

- Privacy legislation may provide individuals with a right to access their personal information held by organizations, subject to some exceptions
  - Generally, access is not provided to other third parties personal information, unless there is consent
- Requests are to made in writing and organizations are to respond promptly (generally 30 days) and provide the requested information at little to no cost to the requesting individual

44

- Organizations generally provide paper copies of personal information upon request, but under the law are only required to provide “access” to said information
- Under PIPEDA access to information may be prohibited (in limited circumstances) on the basis of: costs, references to other individuals, security, commercial proprietary, or other legal reasons (e.g., solicitor - client privilege)
- Upon request, organizations are to provide an account of the use that has been made of an individuals personal information and any third parties to which the information has been provided

45

- Similar to PIPEDA, under FIPPA and PHIPA individuals have a right to access their personal information held by institutions or health information custodian, as the case may be, unless an exception applies
- Likewise, in B.C. under PIPA, upon request private organizations are to provide individuals with access to their personal information, information on the ways in which their personal information is being used, and the names of any third parties to whom their information was disclosed, unless an exception applies

www.carters.ca www.charitylaw.ca

46

B. The Don'ts of Donor Information

1. Don't Sell, Barter, Or Trade Donor Information Without Consent

- PIPEDA specifically prohibits the "selling, bartering or leasing of donor, membership or other fundraising lists"
- Therefore, charities wishing to exchange donor or membership lists with other organizations must obtain consent from each listed donor or member prior to doing so

www.carters.ca www.charitylaw.ca

47

2. Don't Obtain A List Of Emails Through "Address Harvesting"

- Address harvesting is referred to in PIPEDA as collecting electronic addresses, such as email addresses, through scraping websites or generating a list of email addresses
- Section 7.1(2) of PIPEDA exceptions for the collection and use of personal information without consent do not apply to
  - the collection or use of an individual's electronic address, if the address is collected by the use of a program designed or marketed primarily for use in generating or searching for, and collecting, electronic addresses

www.carters.ca www.charitylaw.ca

48

3. Don't Share Personal Information With Affiliated Organizations Without Consent

- As explained above, the knowledge and consent of the individual are required for the collection, use, or disclosure of personal information
- Personal information collected from a donor should not be transferred to another charity without express consent - which includes separate corporations that form part of a "federation" or an "association" of charities
- As well, when personal information that has been collected is used for a new purpose, the express consent of the individual is required before information can be used for that new purpose

www.carters.ca www.charitylaw.ca

49

4. Don't Allow Employees To Snoop In Health Or Donor Records

- Legal Consequences: employee and/or professional regulatory discipline, offence prosecutions, fines (FIPPA, PHIPA), statutory or common law (tort) proceedings
- Information and Privacy Commissioner of Ontario ("IPC") makes it clear that hospitals are liable for actions of its "rogue" staff and has ordered hospitals to upgrade systems to permit auditing and detection of snooping
- In deciding whether to refer to the Attorney General, the IPC will consider the following :
  - Recent privacy training
  - Recently signed confidentiality agreement
  - Privacy warnings on the system
  - Number of occurrences
  - Disciplinary action taken

www.carters.ca www.charitylaw.ca

50

CONCLUSION

- With the advent of modern technologies as well as social media, the legislatures and courts in Canada are continually creating new avenues for privacy and related protection of individuals to keep up with the changing landscape
- In order to avoid potential pitfalls involving donor information, charities, directors and senior management should be aware of privacy related obligations with regards to donor information and implement a proactive approach to compliance

www.carters.ca www.charitylaw.ca

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.

© 2017 Carters Professional Corporation

CARTERS PROFESSIONAL CORPORATION
TOLL FREE: 1-877-942-0001

Toronto Ottawa Orangeville Mississauga
www.carters.ca www.charitylaw.ca www.antiterrorismlaw.ca