

**CARTERS**

BARRISTERS  
SOLICITORS  
TRADEMARK AGENTS

# The Ottawa Region 2017 *Charity & Not-for-Profit Law Seminar*


Ottawa – February 16, 2017

## PRIVACY PITFALLS FOR CHARITIES AND NFPs (AND HOW TO AVOID THEM)

By Sepal Bonni, B.Sc., M.Sc., J.D., Trade-mark Agent

[sbonni@carters.ca](mailto:sbonni@carters.ca)  
1-877-942-0001

© 2017 Carters Professional Corporation



BARRISTERS  
SOLICITORS  
TRADE-MARK AGENTS

**The Ottawa Region  
2017 Charity & Not-for-Profit Law  
Seminar**

Ottawa – February 16, 2017

**Privacy Pitfalls for Charities and NFPs  
(And How to Avoid Them)**

By **Sepal Bonni, B.Sc., M.Sc., J.D., Trade-mark Agent**  
sbonni@carters.ca  
1-866-388-9596

© 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

2

**OVERVIEW**

- Privacy law is a highly nuanced area and the law is continually changing - this presentation only can cover the “tip of the iceberg “
- This presentation will not discuss the intricacies of each type of privacy law or the numerous obligations the various pieces of legislation impose on organizations, or the interrelationship between privacy, and other related laws such as Canada’s anti-spam legislation or social media law
- Instead the presentation will focus on:
  - An overview of the key relevant privacy laws
  - Some common pitfalls that charities and NFPs may encounter and strategies on how to avoid those pitfalls

www.carters.ca

www.charitylaw.ca

3

**A. WHY PRIVACY MATTERS**

- As Canadians, we value our privacy
- Privacy is a basic human right
- The right to control who sees our personal information is recognized by our legal system
- Canadian laws recognize that individuals have a right to privacy in many different contexts

“Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual ... the right ‘to be let alone’ ... Numerous mechanical devices threaten to make good the prediction that ‘what is whispered in the closet shall be proclaimed from the house-tops.’”  
Warren and Brandeis, “The Right to Privacy”, 1890 (4:5) Harv. L. Rev. 193

www.carters.ca

www.charitylaw.ca

4

**1. Why Charities and NFPs Should Care About Privacy**

- Charities and NFPs may collect or have access to personal information about many different individuals, including clients, volunteers, employees, patients, and donors
- This personal information may be necessary for the charity or NFP to do its work, but the personal information is protected by privacy laws
- Privacy laws aim to strike a balance between an individual’s right to privacy and organizations need to collect, use, and disclose personal information in order to operate
- With the collection and use of personal information comes risks and obligations that charities and NFPs must consider


www.carters.ca

www.charitylaw.ca

5

**2. Privacy As A Risk**

- Breach of privacy is one of the key risks facing organizations today
- Personal information can contain highly sensitive information and the implications of a breach can be serious
- Rapidly evolving technology is one of the main drivers of privacy breaches - faxes, email, computers, smart cards, internet



www.carters.ca

www.charitylaw.ca

6

**3. Privacy Risks and Obligations For Charities and NFPs**

- These risks may include:
  - Privacy law suits and class actions
  - Privacy complaints to the relevant Privacy Commissioner
  - Financial costs
  - Operational loss
  - Reputation damage
- In order to manage these risks, charities and NFPs must consider:
  - Legal obligations
  - Regulatory obligations
  - Fiduciary duty

www.carters.ca

www.charitylaw.ca

7

**B. PERSONAL INFORMATION**

- All privacy laws hinge on the definition of "personal information"

**1. What is Personal Information?**

- "Personal information" is defined in privacy legislation as "any information about an identifiable individual"
- It does not include anonymous or non-personal information (i.e., information that cannot be associated with a specific individual)
- Examples of personal information include an individual's name, address, social insurance number, and photos or videos of individuals
- Personal health information is a subset of personal information

www.carters.ca www.charitylaw.ca

8

**2. Examples of Personal Information**


- Person's name
- Address
- Phone number
- Gender
- Race
- Credit card number
- Photograph of an identifiable individual
- Video of an identifiable individual
- Photograph of an individual's home that displays the house number
- OHIP number
- Family health history

www.carters.ca www.charitylaw.ca

9

**C. KEY CANADIAN PRIVACY LAWS THAT CHARITIES AND NFPS SHOULD BE AWARE OF**

- There is not a single national omnibus privacy law in Canada
- Instead, there are complicated, integrated, and highly nuanced privacy laws in place depending on the nature and use of the personal information
- The main privacy laws of interest for charities or NFPs are:
  - Federal private-sector legislation (PIPEDA) and "substantially similar" provincial legislation, e.g., PHIPA
  - Ontario public-sector privacy legislation
  - Privacy torts and privacy class actions



www.carters.ca www.charitylaw.ca

10


**1. PIPEDA and "Substantially Similar" Provincial Legislation**

- The *Personal Information Protection and Electronic Documents Act* (PIPEDA) is the main private-sector legislation for protecting privacy in all provinces that have *not* enacted "substantially similar" 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 then apply instead of PIPEDA
- Alberta, British Columbia, and Quebec have passed substantially similar legislation
- Ontario, New Brunswick, and Newfoundland have passed substantially similar legislation with respect to personal *health* information (e.g. in Ontario, the legislation is the *Personal Health Information Protection Act* (PHIPA))

www.carters.ca www.charitylaw.ca

11

- Organizations dealing with personal health information need to consider this legislation
  - Note: In Ontario, the public-sector FIPPA governs "institutions" (e.g. universities) use of *non*-health personal information (discussed later)
- 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



www.carters.ca www.charitylaw.ca

12

**2. Application of PHIPA**

- Generally applies to collection, use and disclosure of personal *health* information in Ontario by health information custodian or agents of the them, and to anyone that receives information from a health information custodian
- The definition of "health information custodian" 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 or organization's powers, duties or work"
- Examples include practitioners, hospitals, CCACs, psychiatric facilities, long term care homes, pharmacies, laboratories, ambulance services, and a centre, program or service for community health or mental health whose primary purpose is the provision of health care, and others

www.carters.ca www.charitylaw.ca

13

### 3. Application of FIPPA

- 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
- As discussed above, personal *health* information held by hospitals is governed by PHIPA (and not FIPPA)
- Although hospital foundations are not directly subject to FIPPA, it has an impact on hospitals' ability to disclose information to associated foundations for fundraising
- 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)

www.carters.ca www.charitylaw.ca

14

- 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

15

### 4. Key Principles From Privacy Legislation

- Despite their differences, all privacy legislation in Canada generally imposes two main categories of obligations on organizations regarding the collection, use and disclosure of personal information:
  - First - the requirement for consent of an individual be obtained prior to any collection, use or disclosure of their personal information, subject to certain specified exemptions

www.carters.ca www.charitylaw.ca

16

- Second - each organization is required to comply with various administrative obligations including with respect to:
  - 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

17

### 5. Privacy Torts

- There are also "judge-made" privacy torts (i.e., a civil personal wrong) in Ontario
- In *Jones v. Tsige*, 2012, the Ontario Court of Appeal recognized the tort of "intrusion upon seclusion" which is essentially, 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

18

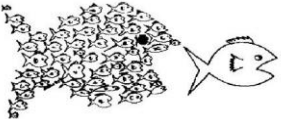
- In *Doe 464533 v. N.D.*, 2016, the Ontario Superior Court of Justice recognized the tort "public disclosure of private facts"
- The Court stated that the tort occurs when:
  - "One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion 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

19

### 6. Privacy Breach Class Actions

- A class action is a lawsuit that allows a large number of people with a common interest in a matter to sue or be sued as a group
- Public notice of the privacy breach is what triggers the class action, the privacy breach itself, or actual harm



www.carters.ca www.charitylaw.ca

20

- Rouge Valley Health System
  - Larger class action launched on behalf of 14,450 new mothers
  - Significant media attention, reputational damage
  - \$412 million class action lawsuit
- Chasles v. Bell Canada Inc.
  - Bell used its Relevant Ads Program to track, collect and sell customers' sensitive personal information to "affiliate" advertisers - Bell was using "opt-out" consent
  - Explicit "opt-in" consent required for targeted advertising
  - Lawsuit seeks damages for breach of privacy amongst other claims
  - Plaintiff's claiming \$750 million

www.carters.ca www.charitylaw.ca

21


- Evans v. The Bank of Nova Scotia
  - Bank employee allegedly provided 643 Bank customers' information to girlfriend who disseminated it to third parties for fraudulent purposes
- Condon v. Canada, 2014 FC 250
  - First Federal Court intrusion upon seclusion class action certified
  - Federal Government lost a hard drive containing personal information of approximately 583,000 individuals in connection with the student loan program administered by the Human Resources and Skills Development Canada

www.carters.ca www.charitylaw.ca

22

### 7. Overlapping Privacy Laws

- Several privacy acts may apply to one organization
- E.g., in Ontario, hospitals are governed by:
  - PHIPA with respect to personal health information
  - FIPPA with respect to non-health personal information
  - PIPEDA with respect to activities that are not core to its operations, e.g., personal information collected by a hospital while operating a parking garage




www.carters.ca www.charitylaw.ca

23

### D. COMMON PRIVACY PITFALLS AND HOW TO AVOID THEM

- Given the various complexities of privacy law, the second half of the presentation will focus on some common privacy issues that charities and NFPs may encounter, and strategies on how to manage the risk



www.carters.ca www.charitylaw.ca

24

### 1. Failure to Ensure Adequate Contracts with Third-party Service Providers

- Contracts which provide for protection of personal information should be in place with any third party, e.g., data processors, partners, affiliates
- These contracts 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

www.carters.ca www.charitylaw.ca

25

## 2. Failure to Update and Implement a Privacy Policy at the Operational Level

- Simply drafting and posting a privacy policy is not enough
- The privacy policy is an organic document that needs to be updated frequently
- The privacy policy should be very specific to your organization and implemented at the operational level
- Failure to implement the 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”

www.carters.ca www.charitylaw.ca

26

## 3. Sharing Personal Information With Separate Corporations That Form Part Of A “Federation”

- Subject to limited exemptions, the knowledge and consent (implied or express depending on circumstances) of the individual are required for the collection, use, or disclosure of personal information
- Personal information collected from a donor cannot be transferred to another charity without express consent - this includes separate corporations that form part of a “federation” or an “association”
- 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

27

## 4. Sharing Of Personal Information With A Hospital Foundation For Fundraising

- The two main pieces of privacy legislation that govern the relationship between hospitals and their associated foundations are PHIPA and FIPPA
- If hospitals are intending to share personal information with their associated foundations this must be done in accordance with these two pieces of legislation
- Although FIPPA does not directly apply to hospital foundations, it is important for foundations to address the indirect impact of FIPPA on their relationship with hospitals
- Hospital foundations should work with associated hospitals and legal counsel to develop policies for the sharing of foundation information generally, as well as the exchange of records between foundations and hospitals

www.carters.ca www.charitylaw.ca

28

- This can help to clarify and standardize information-sharing practices and minimize the risk that sensitive foundation records will be unnecessarily or unintentionally disclosed
- FIPPA provides that a hospital may use personal information for fundraising if the use is “reasonably necessary” for its fundraising
- FIPPA outlines requirements that the hospital must abide by in using personal information for fundraising, including:
  - notice requirements for the hospital and foundation; and
  - that hospitals have fundraising agreements with any persons to whom personal information will be disclosed for fundraising (e.g., hospital foundation)
- The application of PHIPA will be discussed in the next example

www.carters.ca www.charitylaw.ca

29

## 5. Fundraising In The Health Sector

- For fundraisers in the health sector, PHIPA is the key focus
- Sets out preconditions pursuant to which a health information custodian may collect, use or disclose personal health information for “fundraising activities”
- Ontario Privacy Commissioner defines “fundraising activities”:
  - any activity undertaken for a charitable or philanthropic purpose re operations of the HIC, including contacting patients or former patients through mailings
- PHIPA is structured on key principle of:
  - Circle of care = implied consent
  - Other use (e.g., disclosure to a non-health information custodian or to another health information custodian not for the purposes of providing health care) = express consent

www.carters.ca www.charitylaw.ca

30

- But, special rules apply for fundraising
- Personal information may be collected, used, or disclosed for the purpose of fundraising activities undertaken for charitable or philanthropic purpose related to the health information custodian’s operations, if:
  - Consent is obtained
    - Express consent - “gold standard” and recommended form of consent
    - Implied consent is sufficient provided the personal information consists only of the individual’s name and mailing address - Note that where the information is more than name and mailing address (e.g. telephone number, or email address), express consent is required

www.carters.ca www.charitylaw.ca

31

- Notice requirements are met as applicable
- The individual has not withheld or withdrawn consent
- The solicitations for fundraising provide the individual with an easy way to opt-out of receiving future solicitations
- Fundraising communication must not include any info about individual's health care or state of health
  - Note that this latter requirement can pose some challenges, in that it means that the communication cannot reference the fact that the solicited individual recently received treatment at the hospital and therefore might wish to contribute

www.carters.ca www.charitylaw.ca

32

- Recall, PHIPA applies to a "health information custodian" and to "a person who is not a health information custodian and to whom a health information custodian disclosed the information" - a foundation would fit this category
- This would suggest that a foundation can only use and disclose the information for fundraising to the extent that their sponsoring hospital can also do so under PHIPA
- A foundation could also be characterized as an "agent" acting for its associated hospital and thus subject to PHIPA
- Health care charities, hospitals, and their associated foundations should be vigilant of PHIPA requirements in the context of fundraising

www.carters.ca www.charitylaw.ca

33

### 6. Posting On Social Media

- 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 includes personal information and may be subject to privacy laws
- To help manage risk charities and NFP should consider:
  - Implementing a social media policy
  - Requiring consent for the posting of photographs and videos

www.carters.ca www.charitylaw.ca

34

### 7. Employees Snooping Into Health Records

- Several legal consequences :
  - Employee discipline
  - Professional regulatory discipline
  - Offence prosecutions, fines (FIPPA, PHIPA)
  - Statutory (PHIPA) or common law (tort) proceedings
- Privacy Commissioner makes it clear that hospitals are liable for actions of its "rogue" staff
- Privacy Commissioner has ordered hospitals to upgrade its systems to permit auditing and detection of snooping

www.carters.ca www.charitylaw.ca

35

- Privacy Commissioner has referred six individuals to Attorney General for PHIPA offence prosecutions:
  - 2011: nurse at North Bay Health Centre
  - 2015: two radiation therapists at Toronto's UHN
  - 2015: social worker at a family health team
  - 2016: regulated professional at a Toronto hospital
- In deciding whether to refer to the Attorney General, the Privacy Commissioner considers the following which are strategies hospitals should use to prevent snooping:
  - Recent privacy training
  - Recently signed confidentiality agreement
  - Privacy warnings on the system
  - Number of occurrences
  - Disciplinary action taken

www.carters.ca www.charitylaw.ca

36

### 8. Using Cloud Computing And/ Or Servers Outside Of Canada

- With the emergence of cloud technology, a huge amount of our personal and business information has migrated from hard drives we own to remote servers managed by various companies
- In particular, since cloud computing almost inevitably involves 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 and NFPs 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

37

- 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

38

- 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 and NFPs 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

www.carters.ca www.charitylaw.ca

39

**BUT... WAIT...**

- Importantly, the *Income Tax Act* states that books and records must be kept "at an address in Canada recorded with the Minister"
- CRA's position is that servers outside of Canada are problematic
- 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/2015/8rains/booksandrecords.pdf>

www.carters.ca www.charitylaw.ca

40

**9. Failure To Manage Data Breaches Properly**

- One of the fastest growing areas of class actions involves data breaches - this includes insecure disposal of records, lost or stolen devices, unauthorized access, etc.
- Lost or stolen data from organizations is now, unfortunately, a regular occurrence
- Most charities and NFPs have vast amounts of stored electronic data, and typically, that data will include confidential or private information about individuals
- 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 defeat, and mitigate the organization's exposure to liability

www.carters.ca www.charitylaw.ca

41

- Some prudent steps to help mitigate the chances of a data breach:
  - Implement written information security and privacy policies
  - 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
  - Use anti-virus software and stay current with security patch updates
  - Use strong passwords that are often changed

www.carters.ca www.charitylaw.ca

42

- Best practices for responding to a data breach to help mitigate liability:
  - 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



43

**CONCLUSION**

- With the advent of modern technologies and social media, Canadian courts are continually carving out new privacy laws to keep up with the changing landscape
- In order to avoid potential privacy pitfalls, charities and NFPs should be aware of their privacy obligations and implement a proactive approach to privacy compliance

[www.carters.ca](http://www.carters.ca) [www.charitylaw.ca](http://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](http://www.carters.ca) [www.charitylaw.ca](http://www.charitylaw.ca) [www.antiterrorismlaw.ca](http://www.antiterrorismlaw.ca)