Privacy 101: A Guide to Privacy Legislation for Fundraising Professionals and Not-For-Profit Organizations in Canada (Version I)

This guide was prepared by a cross-sector working group representing:

Association of Fundraising Professionals (AFP): Represents 26,000 members in 170 chapters around the world working to advance philanthropy through advocacy, research, education and certification programs.

Association for Healthcare Philanthropy (AHP): A not-for-profit international organization with more than 3,400 members dedicated exclusively to advancing philanthropy in health care institutions and systems.

Association of Professional Researchers for Advancement (APRA): Represents more than 2,000 development professionals around the world who are dedicated to meeting the data and information needs of the nonprofit community.

Canadian Centre for Philanthropy (CCP): A national charity with more than 1,200 members and a mandate to advance the role and interests of the charitable and voluntary sectors for the benefit of Canadian communities.

With thanks to **The Hospital for Sick Children Foundation** and **University Health Network.**

Privacy 101 Table of Contents:

I. Introduction 3

II. History 3

III. Is my organization covered by privacy legislation? 4

IV. What do all the terms mean? Understanding privacy jargon/definitions 5

V. Preparing for PIPEDA 6

VI. Understanding the CSA Model Code 10

VII. A Quick Review – privacy questions for your next management meeting 13

Appendix A– Provincial Updates 14

Appendix B– Sample Purpose Statement 16

Appendix C– Draft Privacy Policy Statement 17

Appendix D– Sample Opt-Out Language 18

Appendix E– Definition of Information in the "Public Domain" 19

Appendix F– Duties & Responsibilities of a Chief Privacy Officer (CPO) 20

Appendix G– Useful Links and Sample Online Privacy Statements 21

I. Introduction

Whether as a result of provincial or federal legislation, or as a result of donor expectations, the issue of privacy of personal information should be considered carefully by all fundraising organizations. This guide provides practical examples of how organizations can prepare for PIPEDA, the *Personal Information Protection and Electronic Documents Act*.

If you plan to comply with the national privacy standard set out in Schedule 1 of PIPEDA, it is likely that you will be in compliance with other provincial legislation, such as “health information acts” in Alberta and Manitoba, Quebec private sector legislation, or “son of PIPEDA legislation” in such provinces as British Columbia and Alberta.

Privacy legislation affects how your organization collects, uses, discloses and retains personal information about an individual.

II. History

Global concern over the protection of personal data has led to the adoption of privacy legislation in countries around the world.

- The Organization for Economic Cooperation and Development (OECD) established a set of protections called Fair Information Practices in 1980, which were endorsed by the Government of Canada.

- The European Union (EU) wanted to harmonize their privacy laws, and in 1995 it created a common standard for privacy protection through the EU Directive on Data Protection. It dictates that EU countries are prohibited from exporting personal data to other non-EU countries unless adequate standards for the protection of personal data are in place.

- The Canadian Standards Association (CSA) Model Code for the Protection of Personal Information was adopted as a voluntary national standard by businesses, consumer organizations and government in 1996. This was a direct result of the EU Directive, and the CSA Code is based on the same Fair Information Practices as the OECD guidelines.

- Canada’s Federal Privacy Law, the *Personal Information Protection and Electronic Document Act* (PIPEDA) was adopted in 2000 and went into effect on January 1, 2001. The source of this privacy legislation is the voluntary CSA Code.

- In 2002, the European Commission ruled that Canada’s Federal Privacy Legislation meets the adequacy standards of the EU Directive.

III. Is my organization covered by privacy legislation?

There are various privacy and data protection laws in force across Canada. The federal government enacted the *Personal Information Protection and Electronic Document Act* (PIPEDA) in 2000. PIPEDA extended privacy protection to personal information collected, used and disclosed for commercial purposes in the private sector and voluntary sectors. Full application of PIPEDA goes into effect on January 1, 2004, although the Act already applies to certain federally-regulated and inter-provincial transactions. For information on current application of PIPEDA to your organization's activities, check the website of the Privacy Commissioner of Canada (http://www.privcom.gc.ca/) or consult your legal counsel.

As a federal Act, PIPEDA complements treatment of personal information under "substantially similar" provincial legislation (either existing or subject to enactment), and so the federal law provided for staged implementation. Broadest application was delayed until January 1, 2004 to give provinces a chance to put their legislation in place, however, many provinces have yet to enact similar laws. In some cases statutes are in force (Quebec) and others have been drafted and/or introduced into legislatures (British Columbia and Alberta.)

Organizations should consult their legal counsel and/or the office of the privacy commissioner in the appropriate jurisdiction to determine what privacy legislation they may be subject to given their activities. Note that some voluntary sector organizations may be subject to public sector privacy legislation owing to their ties with government. In some cases, more than one statute will apply depending on the nature and location of the transaction. For an update on provincial legislation, please refer to Appendix A.

As of January 1, 2004, PIPEDA provides that in jurisdictions where there is no "substantially similar" local legislation, the federal law applies where a transaction occurs entirely within a single jurisdiction. To be subject to PIPEDA, however, a transaction would still have to fall within the general applicability of the Act. For instance, it must a) meet the definition of personal information under the Act; b) not be exempted from the consent requirement owing to the nature of the activity (such as collection for journalistic purposes); and c) satisfy the description of commercial activity or employee criteria set out in the applications section of the Act.

Remember that privacy legislation is evolving and it is your organization's responsibility to keep up to date on provincial and federal legislation and the effects it will have upon your organization. This guide is intended to get the process started and to give you some suggestions on how to begin to address privacy issues related to fundraising. The legislation is much broader than simply fundraising, and your organization may be affected in other ways. It is clear that at minimum, PIPEDA will impact how we deal with the "selling, bartering or leasing of donor, membership or other fundraising lists."

IV. What do all the terms mean? Understanding privacy jargon/definitions

CSA Model Code: The Canadian Standards Association Model Code for the Protection of Personal Information was developed for use as a voluntary code by businesses and organizations. It contains 10 principles to be respected and forms the backbone of PIPEDA and other privacy legislation. The 10 principles are accountability; identifying purpose; consent; limiting collection; limiting use, disclosure and retention; accuracy; safeguards; openness; individual access; and challenging compliance. See Section VI for an expanded description of each principle.

Commercial Activity: As defined in PIPEDA (federal legislation) commercial activity is: "any particular transaction, act or conduct or any regular course of conduct that is of commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists." There is not a precise list of exactly what transactions would fall under the definition of commercial activity. You can expect the federal privacy commissioner and the courts to further develop the list of activities covered by the legislation.

Consent: Permission to collect, use and share personal information for a stated purpose. (See also definitions of implied and express consent.)

Express Consent: Permission that is explicitly sought and applied to the collection, use or disclosure of information, particularly for sensitive information (i.e. health information) or when there has been a significant change from the original purpose for which information was collected. For example, where an organization has a long-standing practice of not sharing its mailing list(s) and has taken the decision to change the practice, seeking express consent is advisable. (See also: opt-in.)

Grandfathering: The term refers to the treatment of data already in an organization's possession prior to legislation. Data already in an organization's possession when legislation comes into effect will be subject to the same rules as data you begin to collect following legislation. The data, therefore, is not being grandfathered. In some instances, however, it may be reasonable to continue using the information for the original purpose for which it was collected with an opt-out option.

Implied Consent: Consent that can be inferred either through an ongoing relationship or through reasonable expectation. For example, consent could be implied for continuing to send a regular mail donor direct mail solicitations or for using the return address on a donation cheque to send a donor a receipt for income tax purposes.

Opt-in: The use of express consent to collect, use or disclose personal information.

Opt-out: The practice of giving individuals the opportunity to be removed from selected or all contacts with your organization.

Personal Information: Information that can be used to identify, distinguish or contact a specific individual. Specifically, “personal information” means information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization. This information would include opinions and beliefs, in addition to financial information, birthdates and other identifying data. Business contact information (title/position, company name, address, etc.) and certain publicly available information is excluded from the definition and therefore from the legislation.

Personal Information Protection and Electronic Documents Act or “PIPEDA”: Is the federal legislation introduced in phases starting January 1, 2001, which sets out ground rules for how organizations (including charities) may collect, use or disclose personal information in the course of commercial activities. As of January 1, 2004, where provinces have not yet enacted substantially similar legislation, PIPEDA will apply to the collection, use and disclosure of personal information within a province for commercial purposes.

Public Domain: Pertains to information that is accessible to the general public, such as telephone directories, and as such is excluded from the federal legislation if used for the purposes for which it was collected. There is still some confusion about what other information might be considered public domain and therefore excluded, including the wide range of government data available on the Internet (land registry listings, etc.). See Appendix E for the regulations specifying publicly available information.

Purpose Statement: The stated purpose for which personal information is being collected, used or disclosed. These may appear on a variety of materials including donor reply coupons, raffle tickets, websites, registration forms, etc.

Substantially Similar: A test that “will interpret substantially similar to mean equal or superior to the *PIPED* Act in the degree and quality of privacy protection provided. The federal law is the threshold or floor. A provincial privacy law must be at least as good, or it is not substantially similar.”

V. Preparing for PIPEDA

There are many steps you can take to help your organization prepare for PIPEDA and to meet growing public concerns with respect to privacy of personal information. In fact, you may already be demonstrating a commitment to privacy.

Are your professional colleagues and employees members in good standing of their respective professional organizations, such as AFP, AHP, APRA and others?
If so, they are required to comply with certain professional codes. Consider making membership in professional associations mandatory. See Appendix G for links to these organizations’ websites where you can find information on their professional codes.

Has your organization adopted the Donor Bill of Rights?
This bill outlines the expectations individuals should have of organizations in whose trust they place their donations. Developed by the American Association of Fund-Raising Counsel (AAFRC), Association for Healthcare Philanthropy (AHP), Council for Advancement

and Support of Education (CASE), and the Association of Fundraising Professionals (AFP), board acceptance of this bill demonstrates your commitment to donors.

Has your organization adopted the Canadian Centre for Philanthropy's Ethical Fundraising and Financial Accountability Code?

Many organizations from all sectors (hospitals, arts, environment, social services, etc.) have adopted this code and in so doing have agreed to abide by certain clear standards and practices. In addition, by adopting the code, organizations must have a complaints policy in place which is a required element in complying with PIPEDA.

What are our next steps?

Your organization will be well on its way to preparing for the impact of PIPEDA if you have already undertaken any, or all of the above initiatives. There are, however, additional steps to consider to prepare now for the possible impact of PIPEDA on your organization.

The first step involves understanding the personal information you currently collect. Bring together a small task force of individuals involved in every step of the collection, use, disclosure and retention of personal information (intake workers, receptionists, data entry staff, program staff, fundraising staff, etc.) to provide the most complete answers possible to the following list of questions. These questions are adapted from resources available from the Canadian Standards Association (CSA) and will assist you in responding to the 10 principles contained in the Model Code (many of which may have the force of law.)

What personal information do we collect and how do we collect it?

Make a list. Look at every field on every form your organization uses in print and online. Don't forget intake, registration, raffle ticket, website donation or info request form, donor reply coupons, pledge/sponsorship forms, memorial cards, comment cards, etc.

Why do you collect it and what do you use it for?

In some cases this will be obvious. You ask for donor address information on a direct mail coupon in order to send a tax receipt and thank you note. But, if you have a field for e-mail addresses on direct mail coupons, consider why that information is being collected. If the answer is that you want to create a complete information file on every donor in the event some day you decide to use e-mail to contact donors, don't do it without consent. On the other hand, if you have a plan to introduce e-receipts or an e-newsletter in the next few months, that may be reasonable.

Think about your need to know the information you are requesting. Privacy legislation is based on the expectation of a "reasonable person" that you collect only the information required to carry out that particular transaction. For instance, individuals may request specific information from your website. If your practice is to send information via e-mail, collecting the individual's e-mail address is reasonable. If, however, you never send information from online requests by mail, why are you asking for a complete mailing address? Just because you want to add that individual to your mailing list is not reason enough unless you make it clear that this is why you are requesting (not requiring) the information. Identifying response lines as "optional" would be useful in this regard.

Be particularly aware when collecting the following types of information and understand clearly why you collect it: birthdays, ages, gender, relationships (i.e. sometimes requested for the next-of-kin on a memorial card), etc. It may be perfectly reasonable to collect any of these pieces of personal information, but each organization will be different.

Where do we keep the information we collect and how is it secured?
Personal information must be treated with respect. This means understanding the various methods your organization has of keeping personal information, for example: hard copy files, files on a computer database, in offices, in a corridor cabinet, etc.

There are three distinct means of securing information. The first is physical. You can lock filing cabinets and restrict access to offices both during business and after hours. The second is organizational. This means implementing security clearances and providing access on a “need-to-know” basis only. Does the individual doing data entry need to know the previous giving history of a donor? Finally, there are technological means of securing information through passwords and encryption.

Don’t forget the simple things. Does the person who prepares tax receipts in your organization print them off on a machine to which others have access? If so, how do you ensure that names, addresses and gift amounts are kept confidential? Are ticket order forms, complete with credit card information, kept on a desk or in an unlocked file? These seem like obvious concerns, so think about the unique nature of your organization’s work and where you keep personal information. Start with your own desk—what information do you leave accessible on your desk when you step away or leave for the evening?

Who has access to it and to whom is it disclosed?
Think about the personal information your organization collects. Be sure you have answered the question about how you secure information. Knowing that you have taken the appropriate steps to restrict unauthorized access, consider who you willingly share this information with and why? Does the chair of the board need to know the size of each individual board member’s donation? If the board has a policy that each director must make a certain level gift, then the chair may need to know if the directors have met this obligation or not. In other cases, it might be enough to report total board giving to the board chair.

For some organizations, the issue of disclosure of personal information for fundraising purposes may pose one of the biggest challenges to complying with privacy legislation. Who better to solicit for support than those individuals who purchased season’s tickets to your theatre? What about the parents of students who attend the private school or the summer camp for which you raise funds? Why not solicit by mail those individuals who attended your gala fundraiser last year? Or, what about sending your annual report or newsletter to all your donors? An appropriate privacy notice at the time of original data collection can quickly settle these questions.

Privacy legislation does not mean that you can no longer raise funds by these means, however, it does mean that individuals must be informed that their personal information may or will be used for purposes that could be seen as different than the original purpose for which it was collected (i.e. registering for camp, buying theatre tickets, attending a gala, etc.) Furthermore, individuals must have a means of opting out of these additional uses of their personal information. Receiving direct mail solicitations or even newsletters must not be a prerequisite for attending summer camp or buying theatre tickets.

Organizations such as hospitals have a heightened duty of confidentiality due to the sensitivity of the personal information they collect, and in some cases increased legislative requirement to protect personal information. Particular care must be taken in disclosing personal information from hospitals to their foundations. Given that the admission process to hospital may be a stressful time, it may not be possible to gain consent from an individual to share their contact information with the foundation at this time. In fact, draft Ontario legislation (as of May 2003) proposed waiting 60-90 days post-discharge before contacting an individual as part of a “grateful patient” program.

What is important for your organization is to consider the sensitivity of the information you have access to and to treat this information accordingly. This goes beyond hospitals to include the sensitive nature of information pertaining to clients of a mental health organization, a cancer support organization, an addiction treatment facility and many more.

In addition to being clear about the purposes for which you are collecting information you should consider the appropriateness of the following:

1. If you use an outside supplier such as a mailhouse or data processing company, you must ensure that they adhere to the privacy legislation. You remain responsible for personal information even when you use an outside contractor. Have suppliers sign a contract stipulating that they are current with and adhere to all privacy legislation, rules and regulations.

2. If you are a foundation separate from the operating organization, consider sending the first solicitation letter from the CEO or other appropriate representative of the operating organization. Names and contact information only become part of the foundation’s database when a donation is received. Be sure to include an opt-out opportunity on this first solicitation.

3. Create purpose statements to provide information to individuals about how their personal information will be used and how individuals may request a change to the use of their personal information. We have provided some sample purpose statements you may wish to consider adapting for your organization. Note: each purpose statement provides a simple means of opting out. See Appendix B for sample purpose statements.

When and how is information disposed of?
What happens to the personal information in your possession when you no longer need it? For many organizations, this previously meant boxes of archived files and databases of prospect information. There may be legislative requirements (Canada Customs and Revenue Agency, for instance) that require you to retain certain information, however, you should develop retention and disposal policies and practices. Disposal of any records containing personal information must leave no recoverable trace of personal data.

VI. Understanding the CSA Model Code

Now that you understand the range of personal information that your organization collects, it's time to review the CSA Model Code and to determine what, if any, steps your organization should take to bring itself into compliance with the model code.

Remember, if compliance with PIPEDA is your goal, adopting the model code need only apply as it relates to commercial activities as defined in the legislation or employees covered under the Act.

The Model Code for the Protection of Personal Information forms the backbone of the PIPEDA. The code was developed by the Canadian Standards Association and contains 10 principles to be respected. In brief, these are:

1) Accountability: Organizations are responsible for all personal information under their control and remain responsible when personal information is processed by third parties on their behalf.

- Appoint an individual (staff or volunteer) to be a "Chief Privacy Officer." This person might not be a fundraiser, and the CPO role only part of their overall responsibilities. They don't need to have this title, just the responsibilities that it suggests. All staff must know who this person is. The CPO has responsibility for understanding the broad impact of privacy, for the implementation of policies and procedures, and is responsible for handling complaints. See Appendix F.
- Ensure third party contracts contain a provision explicitly requiring adherence to privacy legislation.

2) Identifying purpose: Organizations are required to document purposes before they can collect and use personal information.

- The purpose for which personal information is collected must be clear and obvious. Use purpose statements (Appendix B) where multiple purposes are planned.
- Don't forget that information already in your possession can only be used for the original purpose for which it was collected. If you want to add a purpose (i.e. new newsletter to all donors) you must inform individuals of the change.
- Many fundraising related activities may not fall under the definition of commercial activity and therefore consent would not be required prior to collecting information.

3) Consent: Knowledge and consent of the individual are required to collect, use or disclose personal information.

- Consent must be meaningful. That is it must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.
- See sample purpose statements (Appendix B). Post statements related to the purpose of collecting, using and disclosing personal information wherever you can: on your website, in newsletters, on posters and brochures, etc.
- Appropriate consent varies with the sensitivity of the personal information. See definitions of implied and express consent.
- Consent may be given in many ways. Consent may be given orally. A signed form that contains a clear purpose statement is a means of providing express consent. A check-off box on a direct mail coupon may be used to allow individuals to request that their names and addresses are not given to other organizations. Individuals who do not check off the box may be assumed to have consented to the transfer of this information to third parties.
- An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. You must have a means to allow individuals to easily opt out and the procedures in place to record and respect this request.

4) Limiting collection: The amount and type of information is limited to what is necessary for identified purpose.

- Information collected must be limited to that which is necessary to fulfill the purposes identified. Why do you collect birthdays on donor reply coupons?
- New purposes require new consent.

5) Limiting use, disclosure and retention of personal information: Information can only be disclosed or used for the purposes for which it was collected.

- Personal information that is no longer required should be destroyed, erased or made anonymous. You should have guidelines for the destruction of personal information.

6) Accuracy: Personal information has to be accurate, complete and as up to date as is necessary for the purposes for which it is to be used.

- Information must be sufficiently accurate, complete and up to date to minimize the possibility that inappropriate information may be used to make a decision about the individual.
- An organization must not routinely update personal information unless such a process is necessary to fulfill the purposes for which the information was collected.

7) Safeguards: Organizations must take steps to protect personal information from theft and loss, as well as unauthorized access, disclosure, copying or use.

- Physical measures (locked filing cabinets, restricted access to offices, etc.), organi-

zational measures (security clearances, “need-to-know” access, etc.) and technological measures (passwords, encryption, etc.) must all be used.
- Staff and volunteer training are also key elements in a sound privacy policy. Have all staff and volunteers sign an annual statement related to maintaining the confidentiality of personal information.

8) Openness: Organizations must provide the public with general information on their personal information protection policies and practices and must make it easy to identify and contact the person responsible for personal information protection.

- Give individuals easy access to your privacy policies and practices. Use newsletters, posters, brochures, websites, etc. to post information.
- Make the information clear and understandable – think about your audience.
- Again, train staff – particularly reception staff.
- Be sure to provide the name and contact information of the individual you have identified as your “Chief Privacy Officer.”

9) Individual access: Upon request, individuals must be informed of the existence, use and disclosure of all their personal information and be given access to that information. An individual has the right to challenge the accuracy and completeness of the information and have it amended as appropriate.

- Individuals have the right to be given access their personal information (exceptions should be limited and specific and may include information that contains references to other individuals, or information that cannot be disclosed for legal, security or other reasons.) Individuals may correct inaccuracies in their own personal information.
- Requests for access must be responded to within a reasonable time – no more than 30 days and at minimal or no cost to the individual.
- Think about the information in your files. If someone asked to access their file, what would they find and how would you feel about that individual seeing this information?

10) Challenging compliance: An individual can challenge an organization’s compliance to the code, and an organization must develop procedures to handle complaints.

- Again, you need a complaints policy. The legislation is a complaint driven process. You must be able to demonstrate that you have policies and procedures in place that are being followed.
- Your “Chief Privacy Officer” should receive and respond to all privacy complaints.
- You must be prepared to amend policies and procedures if the complaint has validity.

In general, if an organization is operating under these 10 principles, it will tend to be in compliance with PIPEDA.

VII. A Quick Review – privacy questions for your next management meeting

Preparedness Issue	Comments
1. Are members of your staff knowledgeable about the 10 CSA principles in place? a) Accountability; identifying purpose; consent; limiting collection; limiting use, disclosure and retention; accuracy; safeguards; openness; individual access; and challenging compliance.	
2. What information do we collect? a) What personal information do we have and why? b) How did we collect it? c) Is it securely kept? d) Who has access to it? e) How is it disposed and to whom?	
3. Is there a Privacy Policy in place? a) Does it include a complaints process?	
4. Are the Privacy Statements easily visible/ accessible? a) Where are they posted – website, public areas, registration forms, newsletters, etc.?	
5. Is there an opt-out for donors/prospects? a) Where is it posted – website, public areas, registration forms, newsletters, etc.?	
6. Is there a privacy clause in third party contracts?	
7. Have you developed staff and volunteer educational sessions?	
8. Who is the organization's privacy officer?	

Appendix A – Provincial Updates (as of June 2003)

Alberta:
Alberta is currently subject to a Freedom of Information and Protection of Privacy Act, and a Health Information Act (which came into force April 25, 2001). In May 2003, the provincial government introduced new privacy legislation after working closely with British Columbia to develop a similar and consistent policy.

The Information Management, Access and Privacy Division oversees the regulation of the Freedom of Information and Protection of Privacy Act. The Division's website is www3.gov.ab.ca/foip/, and its Help Desk Line is (780) 427-5848. The Health Information Act is regulated by Alberta Health and Wellness at: www.health.gov.ab.ca.

British Columbia:
In May 2003, the Minister of Management Services introduced legislation to protect personal information held by the private sector. The federal privacy commissioner has stated that the legislation would not meet the substantially similar test. For additional information, see the website of the Office of the Information and Privacy Commissioner for British Columbia: http://www.oipcbc.org/.

Manitoba:
Manitoba is governed by a Freedom of Information and Protection of Privacy Act and a Personal Health Information Act. The government agency responsible for oversight is the Ministry of Culture, Heritage and Tourism, Information Resources Division at www.gov.mb.ca/chc/fippa/index.html. Manitoba is in the beginning stages of developing privacy legislation substantially similar to the PIPEDA.

New Brunswick:
The province's Protection of Personal Information Act came into force in April 2001. A text of this bill can be found at the official website of the New Brunswick Statutes: www.gnb.ca/acts/acts/p-19-1.htm. The Ombudsman is responsible for oversight, and that office can be reached at (506) 453-2789.

Newfoundland:
The province is subject to its Freedom of Information Act and its Privacy Act. Oversight is in the hands of the Department of Justice, whose website is www.gov.nf.ca/just/.

Northwest Territories:
Currently the Northwest Territories is subject to the Access of Information and Protection of Privacy Act. Oversight is governed by the Information and Privacy Commissioner of the Northwest Territories, who can be reached at (867) 669-0976.

Nova Scotia:
Nova Scotia's current privacy law is the Freedom of Information and Protection of Privacy Act. The law is overseen by the Freedom of Information and Privacy Review Officer, whose

website is: www.gov.ns.ca/foiro/.

Ontario:

The government developed draft legislation and a discussion paper, *Privacy of Personal Information Act 2002*, that would have dramatically expanded privacy protections far beyond the federal law. Organizations commented on the proposed legislation regarding its potential impact upon charitable fundraising. A pending election call has delayed introduction of the Act.

Ontario is currently governed by the Freedom of Information and Protection of Privacy Act and the Municipal Freedom of Information and Protection of Privacy Act. Oversight is handled by the Information and Privacy Commissioner of Ontario at www.ipc.onca/. Additional privacy information can be found at Ontario's Information Privacy Office at: www.gov.on.ca/MBS/english/fip.

Prince Edward Island:

In PEI, the Freedom of Information and Protection of Privacy Act received Royal Assent on May 15, 2001 and was set to come into force in November 2002. The province has a website devoted entirely to the bill: www.gov.pe.ca/foipp/index.php3.

Quebec:

The Act Respecting the Protection of Personal Information in the Private Sector came into effect in January 1994 and is currently the only provincial law that is substantially similar to the federal PIPEDA. Consequently, this provincial law supercedes the PIPEDA and applies to charities in Quebec. The law sets out detailed provisions that enlarge upon and give effect to the information privacy rights in Articles 35-41 of the Civil Code of Quebec. The website of the Commission d'accès à l'information du Québec is www.cai.gouv.qc.ca/eng/index_en.htm.

Saskatchewan:

The province is subject to the Freedom of Information and Protection of Privacy Act, the Local Freedom of Information and Protection of Privacy Act, and the Health Information Protection Act. Oversight is handled by the Information and Privacy Commissioner of Saskatchewan, and information can be found at: www.saskjustice.gov.sk.ca/legislation/summaries/freedomofinfoact.shtml.

Yukon:

Yukon is subject to the Access to Information and Protection of Privacy Act. Oversight is handled by the Ombudsman and Information and Privacy Commissioner of the Yukon. The website is www.ombudsman.yk.ca/.

Appendix B – Sample Purpose Statements

The following draft purpose statements should be adapted to the unique needs of your organization as they are suggestions only.

1. An organization that conducts its own fundraising might use the following statement, which could appear on registration forms, websites, newsletters, etc.:

“ABC Charity respects your privacy. We protect your personal information and adhere to all legislative requirements with respect to protecting privacy. We do not rent, sell or trade our mailing lists. The information you provide will be used to deliver services and to keep you informed and up to date on the activities of ABC Charity, including programs, services, special events, funding needs, opportunities to volunteer or to give, open houses and more through periodic contacts. If at any time you wish to be removed from any of these contacts simply contact us by phone at (800) 555-5555 or via e-mail at info@abccharity.org, and we will gladly accommodate your request.”

2. For a foundation wishing to use the personal information collected by its operating entity the following statement could appear on registration forms, websites, newsletters, etc.:

“Help Charity respects your privacy. We protect your personal information and adhere to all legislative requirements with respect to privacy. We do not rent, sell or trade our mailing lists. We use your personal information to provide services and to keep you informed and up to date on the activities of Help Charity, including programs, services, special events, funding needs, opportunities to volunteer or to give, open houses and more through periodic contacts from Help Charity and Help Charity Foundation. If at any time you wish to be removed from any of these contacts simply contact us by phone at (800) 555-5555 or via e-mail at info@helpcharity.org, and we will gladly accommodate your request.”

3. For a raffle, door prize ballot, sponsor sheet etc.:

“We appreciate your support of the Run Around the World in support of Making the World Better Foundation. We treat your personal information with respect. We do not rent, sell or trade our mailing lists. The information you provide will be used to provide tax receipts, to contact prize winners where applicable and keep you informed of other events and fundraising opportunities in support of MWB. If at any time you wish to be removed from our list, simply contact us by phone at (800)-555-5555 or via e-mail at info@mwb.org.”

Appendix C – Draft Privacy Policy Statement

Our commitment

Our organization is committed to protecting the privacy of the personal information of its employees, members, customers and other stakeholders. We value the trust of those we deal with, and of the public, and recognize that maintaining this trust requires that we be transparent and accountable in how we treat the information that you choose to share with us.

Inform stakeholders in general terms of your organization's awareness of privacy concerns and the need to address those concerns

Transparency and accountability are key principles. Privacy legislation is typically based on complaints-based enforcement; if you are open and responsive in your practices, your organization is apt to be viewed in a much more favourable light.

During the course of our various projects and activities, we frequently gather and use personal information. Anyone from whom we collect such information should expect that it will be carefully protected and that any use of or other dealing with this information is subject to consent. Our privacy practices are designed to achieve this.

Defining personal information

Although the public is generally aware that privacy is an issue, most people do not have a very solid understanding of the scope of what is covered, or of the exceptions that apply.

Personal information is any information that can be used to distinguish, identify or contact a specific individual. This information can include an individual's opinions or beliefs, as well as facts about, or related to, the individual. Exceptions: business contact information and certain publicly available information, such as names, addresses and telephone numbers as published in telephone directories, are not considered personal information.

Where an individual uses his or her home contact information as business contact information as well, we consider that the contact information provided is business contact information, and is not therefore subject to protection as personal information.

In some cases, privacy legislation is ambiguous; if the law is unclear, you should consider explaining your interpretation. This will both let your stakeholders know what to expect, and contribute to setting an industry standard that may help defend the practice if it is challenged.

Privacy practices

A key principle in privacy protection is limiting collection and disclosure; make this the norm in your organization, and let your stakeholders know you have done so.

Personal information gathered by our organization is kept in confidence. Our personnel are authorized to access personal information based only on their need to deal with the information for the reason(s) for which it was obtained. Safeguards are in place to ensure that the information is not disclosed or shared more widely than is necessary to achieve the purpose for which it was gathered. We also take measures to ensure the integrity of this information is maintained and to prevent its being lost or destroyed.

We collect, use and disclose personal information only for purposes that a reasonable person would consider appropriate in light of the circumstances. We routinely offer individuals we deal with the opportunity to opt not to have their information shared for purposes beyond those for which it was explicitly collected.

Reasonableness is another key test. Exactly what is reasonable may at times be difficult to determine, but at the least you should be able to provide a logical rationale for your practice, rather than justifying it merely as convenient. Widely-adopted industry practice won't determine if you have been reasonable but is a consideration.

Offering individuals the opportunity to opt out of further use or sharing of their information has long been common practice. In some cases, legislation may require that an individual opt-in (i.e. actively consent) to use or sharing. Exactly when and where this will be required in not yet clear.

Website and Electronic Commerce

We use password protocols and encryption software to protect personal and other information we receive when a product or service is requested and/or paid for online. Our software is routinely updated to maximize protection of such information.

Organizations are expected to take reasonable steps to protect information integrity and security In doing so, the sensitivity and vulnerability of the information needs to be taken into account. Practice should also be regularly reviewed.

Updating of privacy policy

We regularly review our privacy practices for our various activities, and update our policy. Please check this website on an on-going basis for information on our most up-to-date practices.

Contact Information

Question, concerns or complaints relating to the Centre's privacy policy on the treatment of personal information should be e-mailed to: general@---.ca

Attention: Privacy officer

Legislation requires that you designate an individual in your organization (either staff or volunteer) to be responsible for privacy compliance issues. Your policy should identify who in your organization is responsible for privacy issues and provide contact information for those with queries or complaints.

Further information on privacy and your rights in regard to your personal information may be found on the website of the Privacy Commissioner of Canada at www.privcom.gc.ca/

Depending on your organization's mandate, it may be subject to either federal or provincial legislation or both. Some provinces do not yet have legislation in place. Where legislation exists, the law is typically administered through the office of the Privacy Commissioner. Most of these offices maintain excellent websites with resource and compliance information. Stakeholders should be referred to the appropriate site or sites.

Appendix D – Sample Opt-Out Language

The following language should be adapted to your organization. This is sample language to guide you in developing your own opt-out statements:

“We do not sell, trade or otherwise share our mailing lists. We hope that you find the attached information helpful. However, if at any time you wished to be removed from this or another mailing, simply contact us by phone at (800) 555-5555 or via e-mail at info@heretohelp.org. Please allow 15 business days to allow us to update our records accordingly.”

Appendix E – Definition of Information in the “Public Domain”

Regulations Specifying Publicly Available Information

INFORMATION

1. The following information and classes of information are specified for the purposes of paragraphs 7(1)(d), (2)(c.1) and (3)(h.1) of the Personal Information Protection and Electronic Documents Act:

(a) personal information consisting of the name, address and telephone number of a subscriber that appears in a telephone directory that is available to the public, where the subscriber can refuse to have the personal information appear in the directory;

(b) personal information including the name, title, address and telephone number of an individual that appears in a professional or business directory, listing or notice, that is available to the public, where the collection, use and disclosure of the personal information relate directly to the purpose for which the information appears in the directory, listing or notice;

(c) personal information that appears in a registry collected under a statutory authority and to which a right of public access is authorized by law, where the collection, use and disclosure of the personal information relate directly to the purpose for which the information appears in the registry;

(d) personal information that appears in a record or document of a judicial or quasi-judicial body, that is available to the public, where the collection, use and disclosure of the personal information relate directly to the purpose for which the information appears in the record or document; and

(e) personal information that appears in a publication, including a magazine, book or newspaper, in printed or electronic form, that is available to the public, where the individual has provided the information.

Source: Privacy Commissioner of Canada website, Regulations for PIPEDA

Appendix F – Duties & Responsibilities of a Chief Privacy Officer (CPO)

The role of a chief privacy officer is multi-disciplinary. This leadership role involves the interpretation of privacy law and the creation of privacy programs that ensure the protection of personal data and compliance with current legislation across an organization.

This individual can be expected to be responsible for ensuring that some or all of the following duties are addressed as is appropriate to your organization:

- Leadership of the privacy program
- Conduct privacy risk assessments and audits
- Develop and implement corporate privacy policies and procedures
- Create and deliver educational, training and orientation programs
- Monitor systems development and operations for security and privacy compliance
- Ensure compliance related to privacy, security and confidentiality
- Audit and administer privacy programs
- Provide counsel relating to business contracts and partnerships
- Track and report on compliance related to privacy, security and confidentiality
- Resolve allegations of non-compliance
- Maintain current knowledge of federal and provincial privacy legislation and regulations
- Manage public perception of data protection and privacy practices for the organization
- Liaise with government agencies and the privacy commissioner's office

Ideally, a CPO should bring a breadth of experience and knowledge to the organization. This expertise would allow him/her to interpret the legislation and develop privacy compliance programs that would integrate well within the organization, ensuring the continued flow of business operations and profitability while convincing clients and stakeholders that data is handled with discretion and confidentiality and, above all, that security measures are in place to comply with current legislation.

Some of the skill set required to fill the CPO position can be defined as the following:

- Demonstrated skills in change management and project management
- Demonstrated organization and facilitation skills
- Communications and public relations skills
- Knowledge of relevant privacy laws, regulations and standards
- Experience in policy development and training
- Knowledge of information systems with some technology background
- Background in compliance, legal or quality assurance would be helpful
- Crisis management skills

In many organizations this level of experience may not be possible. However, the organization must provide the CPO with resources (time, training and authority) to be successful in the role.

Appendix G – Useful Links and Sample Online Privacy Statements

Association of Fundraising Professionals
http://www.afpnet.org/

Association of Healthcare Professionals
http://www.ahpcanada.com/govtissues.htm

Association of Professional Researchers for Advancement
http://www.aprahome.org/advancement/privacy.htm

Canadian Centre for Philanthropy
http://www.ccp.ca/

An Introduction to Protecting Personal Information Collected by Charities (AFP 2003)
http://www.afpnet.org/content_documents/Canada_privacy_guide_final_version_II_6-12-2003.pdf

Donor Bill of Rights
http://www.afpnet.org/ethics/ethics_and_donors

Ethical Fundraising and Financial Accountability Code

http://www.ccp.ca/display.asp?id=36

Privacy Commissioner of Canada
http://www.privcom.gc.ca/index_e.asp

Canadian Standards Association
http://www.csa.ca/default.asp?language=English

Sample Online Privacy Statements:

World Wildlife Fund
http://www.wwf.ca/AboutWWF/WhoWeAre/WhoWeAre.asp?page=security

London Health Sciences Centre Foundation
http://www.lhsf.ca/

United Way of Greater of Toronto
http://www.unitedwaytoronto.com/

Ontario Lung Association
http://www.on.lung.ca/global/privacy.html