Prepared for: The Ottawa Estate Planning Council
Tuesday, March 2, 2004, Rideau Club

Jeffrey H. McCully, BA, LL.B.
jmccully@privacy-consulting.com
www.privacy-consulting.com

HOW WILL THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT (PIPEDA) AFFECT MY PRACTICE?

A STRATEGIC GOVERNANCE PERSPECTIVE FOR COMPLIANCE.

General Overview

PIPEDA applies to all organizations that collect, use or disclose personal information in the course of commercial activities intra-provincially, inter-provincially and internationally.

The only circumstance in which PIPEDA will not apply is if your principal place of operation is in a province, which has its own "substantially similar" legislation. Ontario does not. Quebec does.

PIPEDA is a federal statute, which establishes rules to regulate the collection, use and disclosure of personal information associated with commercial activity.

Some Relevant Definitions:

"Commercial activity" – any transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists. (So, does apply to charities, contrary to popular belief).

"Governance" – authoritative care and control over an organization; relates to accountability for the activities of an organization [CBCA 102(1); OBCA 115(1)]

"Grandfathering" – (retroactivity) – this term refers to the treatment of information already in the organization's possession prior to PIPEDA. Data already there is subject to the same rules.

"Personal information" – information about an identifiable individual, but does *not* include the name, title, and business address or telephone number of an *employee* of an organization.

"Privacy" – the right of individuals to control the collection, use and disclosure of their own information.

"Whistle-blowing" – Section 27 of the PIPEDA protects persons who inform the Commissioner that a person or organization has or intends to contravene the Act. Such persons cannot be retaliated against, either by fines, punishment, disciplinary actions, etc.

Jeffrey H. McCully, BA, LL.B.
jmccully@privacy-consulting.com
www.privacy-consulting.com

The 10 Principles (The Heart of the Legislation – The CSA Code)

1. Accountability: This is the concept that requires your organization to take responsibility for the information that is under its control. It also encompasses the idea that you must delegate the responsibility for dealing with compliance issues relating to privacy to an individual within the organization (the Chief Privacy Officer). Ensure third party contracts contain a provision requiring allegiance to PIPEDA.

2. Identifying Purposes: This principle requires your organization to inform individuals of all purposes for which personal information is collected. Also, such identification must take place at or before the time the information is collected by you. The use of a "Purpose Statement" is recommended, for clarity.

3. Consent: You must obtain the consent of an individual for the collection, use or disclosure of personal information relating to the individual. Most importantly, the person may withdraw consent at any time. The sensitivity of the information that is collected must be taken into account when determining the form of consent needed. (express vs. implied consents). Before personal information is disclosed within or outside the organization, consent must be obtained.

4. Limiting Collection: Your organization may only collect personal information that is necessary for the purposes identified by the organization. This rule is important for all staff persons to be aware of. Information cannot be collected indiscriminately. If organization is collecting information from a party for a *new* purpose, it must obtain a new consent. If you collect information from a third party, you have to ensure that the third party has gained consent from their client/customer/contact.

5. Limiting Use, Disclosure and Retention: Your organization may not use or disclose personal information for purposes other than those for which it was collected. (Except those consented to and those allowed by law). Personal information no longer required should be destroyed, erased or made anonymous.

6. Accuracy: Your organization is responsible to ensure that personal information under your control is accurate, complete and up-to-date as is necessary for the purposes for which it is to be used. Do you document how and when personal information is updated to ensure its accuracy? Do you ensure that information received from a third party is accurate and complete?

7. Safeguards: Your organization shall protect personal information under your control using the security safeguards appropriate to the sensitivity of the information. (physical, organizational and technological). Many safeguards can and should be implemented, such as ensuring that the records management system has user accounts and access rights, such as having personnel sign simple confidentiality agreements, such as better practices with respect to leaving files open, computer screens on.

Jeffrey H. McCully, BA, LL.B.
jmccully@privacy-consulting.com
www.privacy-consulting.com

8. Openness: Your organization shall ensure that there is public availability of information relating to your privacy practices and policies and its compliance with PIPEDA.

9. Individual Access: Essentially, you must have a process by which persons can access the personal information you hold concerning them. Such information must be provided to the person. Also, they must be able to challenge the accuracy and completeness of the information and to amend it, if necessary. Staff is the key here. Responses to enquiries should be made at little or no cost, and within 30 days. Of course, there is the issue of properly identifying appropriate "askers". Does that person have a right to the personal information?

10. Challenging Compliance: Your organization must ensure that there is a process in place that permits individuals to challenge your organization's compliance with the privacy rules under PIPEDA. Again, staff is the key. All must recognize that it is a complaints-driven process, so proper (adequate and timely) responses are important. Can one easily find out how to file a complaint?

Jeffrey H. McCully, BA, LL.B.
jmccully@privacy-consulting.com
www.privacy-consulting.com

Governance and Privacy – Where the Strategic & Proactive Leader Should Begin

1. Does your organization have a Chief Privacy Officer and a Privacy Policy?

2. Does your organization collect personal information and use it for commercial purposes?

3. In your organization, is the purpose for the collection of personal information explained to clients, at the time of its collection?

4. Is the personal information that is collected, used or disclosed limited to only that which is necessary to achieve the stated purpose?

5. Have requisite consents been obtained for the collection, use or disclosure of personal information?

6. Is the form of consent (implied, express) appropriate for the level of sensitivity of the personal information?

7. Is the form of consent in conformity with the level of *reasonable expectations* of the individual involved?

8. Is personal information under your organization's control complete and accurate?

9. Are security safeguards in place appropriate for the level of sensitivity of information?

10. Is there an open line of communication with your clientele, to enable them to access and correct their personal information as necessary?

11. Is there a mechanism through which your clientele or the public can make an inquiry or complain about personal information management practices?

12. Has an *employee* privacy policy been implemented?

13. Does your firm have a privacy breach crisis management protocol in place? How quickly can your firm's management act to limit damage to clientele?

14. Is privacy training available to employees, including junior front-line employees?

15. Are privacy requirements and other legal protections part of your firm's third-party contracts and partnership arrangements? (E.g., indemnities, assurances of compliance with PIPEDA, Confidentiality Agreements, audit rights)

16. Are privacy requirements part of employment contracts?

17. Does your firm conduct a privacy impact assessment prior to implementing new technologies, partnerships, programs and products/services that could impact on personal information privacy?

18. Is on-going privacy training available?