

# GETTING PERSONAL with privacy

Privacy legislation that will apply to provincially-regulated organizations that collect, use or disclose personal information is only months away. Plan administrators need to prepare now.



By Karen Kahansky

**P**rivacy is an issue of growing importance for the administrators of employee benefit plans. And the impact of emerging privacy protection laws—a multi-jurisdictional patchwork—is potentially enormous. As privacy law develops, there are many issues for benefit plan administrators to consider. What form of consent is required and when must it be secured? How should personal information be retained? How can confidentiality be maintained and information secured?

Broad legislation protecting the privacy of personal information in the private sector currently exists in Quebec and at the federal level. Quebec's legislation, *An Act Respecting the Protection of Personal Information in the Private Sector*, has been in effect since 1994 and applies to every business enterprise in Quebec receiving, holding, using or disclosing personal information in relation to Quebec residents. Proposed amendments to the Quebec law will broaden its application to the personal information of any individual,

regardless of that individual's province of residence.

The federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) came into effect for federally-regulated employers on Jan. 1, 2001, while its application to personal health information commenced on Jan. 1, 2002. PIPEDA is based on the 10 principles of the Canadian Standards Association's Model Code for the Protection of Personal Information. Commencing Jan. 1, 2004, PIPEDA will apply to provincially-regulated organizations that collect, use or disclose personal information in the course of commercial activities. PIPEDA will not apply if information is collected, used or disclosed within a single province if that province has enacted legislation that is substantially similar.

Some provinces are expected to enact privacy legislation prior to Jan. 1, 2004 in lieu of PIPEDA. For example, Ontario released draft legislation for consultation, though it was later withdrawn. Alberta and British Columbia

both tabled draft privacy legislation earlier this year. Other provinces may follow suit.

A potentially complex patchwork of legislation may therefore emerge, with broad and onerous requirements, and significant penalties for non-compliance. This patchwork opens the possibility that companies doing business in more than one province will be subject to both federal and provincial privacy legislation.

In light of these developments, plan administrators and employers need to consider the existing requirements and should begin to prepare now for what may be made law later in the jurisdictions in which they operate. Many employers that have U.S. parent companies are undoubtedly watching with interest as the parent company complies with American privacy initiatives in relation to the *Health Insurance Portability and Accountability Act* of 1996 and otherwise.

## ISSUES FOR ADMINISTRATORS

The legislation differs in detail, but generally speaking, plan administrators need to address issues of consent, file retention, security, disclosure to third-parties, employee communications and training.

**1. Consent** - How do you determine when consent is required? Consent is generally needed in order to be able to collect, use or disclose personal information, although some exceptions do apply.

What type of consent is required? Once you understand the extent to which consents are required from employees, you then need to determine whether you need express consent or whether implied consent will be sufficient. Express consent is a more direct form of consent; for example, explicit permission given by the individual to use their personal information in certain ways. Obtaining express consent is more onerous (e.g., the need to collect signatures).

Implied consent is assumed from the circumstances—such as a “negative option” where individuals are deemed to have consented to the use of their personal information for particular purposes unless they indicate otherwise. On this point, existing legislation offers some flexibility, although under PIPEDA, organizations are required to take into account the sensitivity of the information in determining the type of consent to use. Personal financial information and health information is often considered sensitive, which may lead administrators to require express consents.

When should you obtain consent? The easiest time to obtain consent is on initial enrolment. However, this will cover only new entrants, and additional effort will be required for existing members. The employer may want to use an omnibus consent that applies to more than benefit plan information. A key issue in omnibus consents is that

the organization must identify the purposes for which it is collecting the information. However, even with this type of consent, further authorizations may be required in the future if additional purposes are identified.

How should a consent be worded? Consent must be informed, meaning that at the time of giving it, the individual must have reasonable information about the purpose of the collection, use or disclosure. Consent language requires a clear indication of what personal information is collected, how it is used, who it is shared with, and for what purpose. A key issue is whether consent is needed to share information with service providers and even parent or other related companies. In drafting consent language, legal advice should be obtained.

What additional consents may be required and when? A single consent may not cover all circumstances, so new consents may be required at times. Administration staff will need to be aware of the circumstances in which additional consent is required. For example, non-member spouses, financial advisors and lawyers might directly communicate with the plan administrator. Generally, it will be necessary to ensure that a specific consent is secured from the member before disclosing any personal information about the member to a third party, although there may be extraordinary circumstances in which the legislation does not require consent.

Once any type of consent is obtained, there must be a mechanism for keeping track of it and any revocations of that consent.

**2. File Retention** - What should be retained? You will clearly want to retain information that is necessary for the identified purposes. Once a purpose is articulated, there may be a legal obligation to retain the information for the necessary period. This can be challenging, given the various ways in which personal information might be collected, retained and disclosed, including via electronic means. An appropriate method of storage is particularly important if an individual wishes to exercise the right of access.

What should be destroyed? Destruction of personal information should be in accordance with a documented retention schedule. Such schedules must be developed with care, taking into account the purposes of the information, the contingencies which may arise and any legislative requirements. For example, a member file is set up under a pension plan for the purposes of administering their entitlements under the plan. Is the file no longer needed once the member terminates employment and is fully paid out? What if the member or a surviving spouse/beneficiary questions the entitlements at a later date? What if the member is later included in a plan wind-up? These questions must be considered as part of the privacy process.

**3. Security** - Personal information must be protected so that confidentiality is maintained. Appropriate safeguards depend on a number of factors, including the sensitivity of the information and the storage medium. The legislation does not consider cost of storage. There are numerous areas to review, including:

- Storing files and documentation in a secure manner.
- Limiting access to personal information within your organization.
- Ensuring appropriate security measures for personal information sent over the Internet or intranet.
- Ensuring paper and electronic data are disposed of in a secure manner.
- Ensuring that third-party providers use appropriate security measures for personal information you give them.

**4. Disclosure to third-parties** - A member's death, marriage breakdown or lack of capacity, for example, may necessitate disclosure of personal information to a third party. As a result, it is important to understand the range of special situations that may arise and the extent to which there are exceptions to the general rule of no disclosure without consent. Specific procedures should be established to address these.

**5. Employee communications** - Privacy laws require organizations to provide information about privacy policies and practices. This means routinely revisiting existing policies or developing new ones. The wording of such policies should be approached carefully, since it may be scrutinized later if an employee complains that their privacy rights have been violated.

An employee must be given access to their personal information on request. Organizations need to implement a process for handling such requests. Given that employees may review their files, care must be taken to ensure that personal information of other individuals is not also in the file. Great care must be taken to ensure that the content of the file is personal information of the individual (e.g., the opinions of others may or may not qualify as personal information about the individual). In addition, it is necessary to ensure that all information is included in the file, including records of electronic documents, handwritten notes and so on.

**6. Training** - Now is the time for your organization to start educating staff working with personal information about the importance of privacy and about your organization's policies and procedures in this regard.

In terms of next steps, some key things to consider include:

**1. Determine what legislation, if any, currently applies to your organization.** Employers that are federally regulated or operating in Quebec are already subject to the privacy laws of those jurisdictions. Employers operating exclusively in other jurisdictions are not yet subject to private sector privacy statutes, although this is expected to change.

**2. Appoint individuals within your organization to be responsible for privacy issues.** It will be most effective to focus responsibility on a small group of people who are knowledgeable or who can learn about privacy issues. The nature of your organization and the types of personal information in question will determine the appropriate number and types of resources. It will also be critical to obtain senior management support of this significant effort.

**3. Audit information practices.** It is impossible to know what needs to be done until you have a good grasp of the organization's existing information practices. This can only be done through a comprehensive audit process, which identifies what personal information the organization currently collects, uses and discloses. Audits may be done by internal staff, or by external auditors.

There are numerous issues and steps that must be taken relating to privacy requirements. Addressing these issues now is important as the road to ensuring privacy may prove to be a long one.

**BC**

---

*Karen Kabansky is the national compliance leader for Towers Perrin Administration Solutions in Mississauga, Ont. karen.kabansky@towers.com*