2002

An Overview of Canadian Privacy Law for Pharmaceutical and Device Manufacturers Operating in Canada

Erika Lietzan
University of Missouri School of Law, lietzane@missouri.edu

John K. Fuson
Covington & Burling

An Overview of Canadian Privacy Law for Pharmaceutical and Device Manufacturers Operating in Canada

ERIKA KING *
JOHN H. FUSON **

On April 13, 2000, the Canadian Parliament enacted by Royal Assent the Personal Information Protection and Electronic Documents Act (PIPEDA).[1] The Act requires private organizations to comply with a code of "fair information practice," which mandates individual consent for the collection, use, and disclosure of personal information.[2] PIPEDA complements the Federal Privacy Act, which places similar obligations on government institutions.[3] On January 1, 2002, the Act began to apply to personal information (including personal health information) collected, used, or disclosed by a federal work, undertaking, or business, and personal information (including personal health information) disclosed by any organization for consideration outside the province in which it was collected.

This article describes PIPEDA and explains how it will apply to pharmaceutical companies and device manufacturers operating in Canada. Section I provides an overview of privacy legislation in Canada. Section II discusses the new Act's scope, the obligations it imposes, and the rights it creates. Section III discusses enforcement of the Act. Section IV considers the relationship between PIPEDA and other privacy laws in Canada, the European Union (EU), and the United States. Finally, Section V describes the transition periods before the Act is fully effective.

It is not entirely clear how PIPEDA will affect pharmaceutical and device manufacturers in Canada. PIPEDA is based on a privacy code drafted by private industry. The healthcare sector was not a significant participant in the drafting of that code, and the statute, therefore, is not tailored to address the specific concerns of pharmaceutical and device manufacturers. Also, the new Privacy Commissioner, who lacks a medical or scientific background, has said little about how he intends to apply the legislation to the healthcare sector. This article offers some speculation. Guidance and decisions issued in the next year may resolve some of the uncertainties.

---

* Ms. King is Assistant General Counsel at PhRMA, Washington, D.C. When this article was written, she was an Associate with the law firm of Covington & Burling, Washington, D.C.

** Mr. Fuson is an Associate with the law firm of Covington & Burling, Washington, D.C.

[1] 1999-2000 S.C. 2000, ch. 5 (Can.). Part 1 of the Act (Personal Information Protection) establishes rules governing the collection, use, and disclosure of personal information in the private sector. Part 2 (Electronic Documents) addresses the use of electronic alternatives to paper records. This article addresses only Part 1.

[2] Bruce Phillips, Privacy Commissioner of Canada, The Evolution of Canada's Privacy Laws, Address to the Canadian Bar Association–Ontario Institute 2000 (Jan. 28, 2000), *available at* http://www.privcom.gc.ca/speech/archive/02_05_a_000128_e.asp (last visited June 19, 2002). According to its statement of scope, the Act establishes rules governing "the collection, use, and disclosure" of information. The Model Code on which it is based and which is incorporated as its "Schedule 1" distinguishes between "use" and "retention." The statute plainly applies to both. This article uses the "collect, use, and disclose" convention except where the use of "retention" will clarify the discussion.

[3] Bruce Phillips, Privacy Commissioner of Canada, 1999 Annual Report of the Privacy Commissioner (July 1999), *available at* http://www.privcom.gc.ca/information/ar/02_04_07_e.asp (last visited June 19, 2002).

I. BACKGROUND

A. *Prior Privacy Legislation*

On July 1, 1983, the Federal Privacy Act went into effect. The Privacy Act protects personal information collected and held by over 150 designated public agencies and institutions.[4] These agencies and institutions vary in size and scope, and range from the Departments of State and Finance to the Northwest Territories Water Board.[5] The Privacy Act prohibits each from collecting personal information not related directly to its operating programs or activities,[6] and from making unrelated uses or disclosures of such information without the individual's consent.[7] These agencies and institutions must also provide individual data subjects access to their personal information stored in government data banks.[8]

The Privacy Act also established the Office of the Privacy Commissioner.[9] The Privacy Commissioner is appointed by the Governor in Council and approved by Parliament,[10] and is charged with investigating complaints from individuals about the government's use and handling of their personal information.

Several Canadian provinces also have passed privacy legislation. The most comprehensive provincial legislation is Quebec's Personal Information Protection Act, passed in 1994, which governs the collection, use, and disclosure of personal information by private organizations in Quebec.[11] Other provinces, including Alberta and Manitoba, have passed healthsector-specific statutes limiting the collection, use, and disclosure of personal information by healthcare professionals and facilities.[12]

B. *The CSA Model Code for the Protection of Personal Information*

PIPEDA's core provisions were based on the Model Code for the Protection of Personal Information, approved in 1996 by the Canadian Standards Association.[13] The Model Code describes ten interrelated principles deemed essential for the protection of personal privacy. They are:

- Accountability

  An organization is responsible for personal information under its control and shall designate an individual or individuals who are ac-

[4] Office of the Privacy Commissioner, Privacy Legislation in Canada: Two Federal Laws, *available at* http://www.privcom.gc.ca/fs-fi/fs2001-02_e.asp (last visited June 19, 2002).

[5] Privacy Act, Schedule (§ 3).

[6] *Id.* Collection, Retention and Disposal of Personal Information.

[7] *Id.* Protection of Personal Information.

[8] *Id.* Access to Personal Information.

[9] *Id.* Office of the Privacy Commissioner.

[10] The Office is currently held by George Radwanski, a former journalist. He was approved by Parliament in October 2000 for a seven-year term. *See* Privacy Commissioner of Canada, About the Office of the Privacy Commissioner, *available at* http://www.privcom.gc.ca/au_e.asp (last visited June 19, 2002).

[11] R.S.Q. Ch. P-39.1, An Act Respecting the Protection of Personal Information in the Private Sector.

[12] Alberta Health and Wellness, *available at* http://www.health.gov.ab.ca (last visited June 19, 2002); Manitoba Access and Privacy Division, *available at* http:www.ombudsman.mb.ca (last visited June 19, 2002).

[13] The Canadian Standards Association is an independent not-for-profit organization of business, industry, government, and consumer groups. *See* The Canadian Standards Association Homepage, *available at* http://www.csa.ca (last visited June 19, 2002).

countable for the organization's compliance with the following principles.[14]

- Identified Purposes

  The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.[15]

- Consent

  The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.[16]

- Limited Collection

  The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.[17]

- Limited Use, Disclosure, and Retention

  Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.[18]

- Accuracy

  Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.[19]

- Security

  Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.[20]

- Openness

  An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.[21]

---

[14] CSA Model Code Principle 1—Accountability; PIPEDA Schedule 1, § 4.1.

[15] CSA Model Code Principle 2—Identifying Purposes; PIPEDA Schedule 1, § 4.2.

[16] CSA Model Code Principle 3—Consent; PIPEDA Schedule 1, § 4.3.

[17] CSA Model Code Principle 4—Limiting Collection; PIPEDA Schedule 1, § 4.4.

[18] CSA Model Code Principle 5—Limiting Use, Disclosure, and Retention; PIPEDA Schedule 1, § 4.5.

[19] CSA Model Code Principle 6—Accuracy; PIPEDA Schedule 1, § 4.6.

[20] CSA Model Code Principle 7—Safeguards; PIPEDA Schedule 1, § 4.7.

[21] CSA Model Code Principle 8—Openness; PIPEDA Schedule 1, § 4.8.

- Right of Access

  Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.[22]

- Compliance

  An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.[23]

The Canadian Parliament incorporated the ten Model Code principles, with only minor modifications, directly into the Act.[24]

C. *Enactment of PIPEDA*

An earlier version of the Act was introduced in October 1998 as Bill C-54 but the House failed to take final action on it before recessing. The Act was reintroduced in October 1999 as Bill C-6 and this time, the House took prompt action and passed the bill, sending it to the Senate.

Responding to the health sector's concern that it would need extra time to implement appropriate policies and procedures to protect personal health information, the Senate added an amendment to delay the bill's application to personal health information by one year.[25] Health sector representatives pointed out that the health sector had not participated in the drafting of the Model Code on which the proposed privacy legislation was based. The resulting code was designed primarily to encourage electronic commerce and did not focus on privacy issues that might be significant in the medical context. The Canadian Medical Association (CMA) was quick to note that "the world of healthcare [is] very different from that of commerce and consequently require[s] distinct rules."[26] It criticized the Act's failure to take into account any of the health-sector specific modifications added in the CMA's version of the Model Code.[27]

The House passed the Act without further changes. Although it adopted the Senate's amendment delaying the Act's application to personal health information, it did not add a separate code to govern that information.[28]

---

[22] CSA Model Code Principle 9—Individual Access; PIPEDA Schedule 1, § 4.9.

[23] CSA Model Code Principle 10—Challenging Compliance; PIPEDA Schedule 1, § 4.10.

[24] Second Report of the Standing Senate Committee on Social Affairs, Science and Technology (Dec. 6, 1999); Phillips, 1999 Annual Report of the Privacy Commissioner, *supra* note 3.

[25] *See* John Cannis, Parliamentary Secretary to the Minister of Industry, House of Commons Debate (Feb. 14, 2000), *available at* http://www.privcom.gc.ca./information/02_06_com_000214.e.asp (last visited June 19, 2002) (commenting on the Senate amendments).

[26] Canadian Medical Association, Listening to Our Patient's Concerns: Comments on Bill C-54, Submitted to the House Standing Committee on Industry (Mar. 18, 1999), *available at* http://www.cma.ca/cma/common/displayPage.do?pageId=/StaticContent/HTML/NO/I2/where_we_stand/political/1999/03-18/index.htm (last visited June 19, 2002).

[27] *Id.* The CMA's Health Information Privacy Code granted patients strict control over personal health information, without the exceptions provided in the Act for "expediency, practicality, public good, research, offence investigation, historic importance and artistic purpose." *Id.*

[28] A separate code was suggested in the House debate. *See* Keith Martin, House of Commons Debate (Feb. 14, 2000), *available at* http://www.privcom.gc.ca./information/02_06_com_000214.e.asp (last visited June 19, 2002) (calling for a code of conduct limiting access to personal health information).

D. *Interpretation of PIPEDA*

Parliament's decision to use the Model Code as separate provisions of this legislation creates some interpretive problems for affected parties. The Model Code is inherently vague—officials at the Office of the Privacy Commissioner concede this point[29]—and the Privacy Commissioner has significant discretion in interpreting its provisions. His statements in informal guidance on the Office's web site and in speeches provide some insight into how he will apply PIPEDA to the healthcare sector. In the only decision to date that related to the healthcare industry, the Privacy Commissioner indicated his willingness to take into account the practical business implications of his decisions. In that decision, the Commissioner rejected a complaint filed by physicians alleging that IMS Health Canada sold information about their prescribing habits without their consent. IMS collected prescription information such as drug identification numbers, insurance information, the patient's gender and date of birth, as well as the name and identification number of the prescribing physician. The Commissioner concluded that this information was not personal information, but rather more akin to work product. To find otherwise, he wrote, "would have the effect of precluding many kinds of legitimate commercial consumer reporting."[30]

Because its provisions formed the basis of PIPEDA, the CSA Model Code and accompanying commentary provide additional insight about the Act's likely application. Also, industry groups like the CMA used the Model Code to develop sector-specific privacy protection codes. The CMA Health Information Privacy Code, approved in 1998, modifies the ten Model Code principles to specifically promote "the privacy of patients, the confidentiality and security of their health information and the trust and integrity of the therapeutic relationship." It recognizes the "special nature of health information," including "its highly sensitive nature, the circumstances of vulnerability and trust under which it is confided or collected, and the fiduciary duties of health professionals in relation to this information."[31] Although PIPEDA did not incorporate sector-specific rules, the Privacy Commissioner may look to this industry code for guidance when evaluating whether a pharmaceutical or device manufacturer has taken reasonable steps to protect personal information.

Interpretation of the Act is further complicated by the fact that it is comprised of both mandatory provisions an organization must follow—"[o]rganizations *shall* put procedures in place to receive and respond to complaints"–and recommendations an organization may adopt to enhance privacy protections and ensure compliance—"[t]he complaint procedures *should* be easily accessible and simple to use."[32] This distinction may be of little practical import, however, because the Commissioner may audit an organization he believes is not following a recommendation.[33]

---

[29] Anne Rooke, The New Wave of Privacy Protection in Canada, Address to the FIPA Conference (Mar. 9, 2000), *available at* http://www.privcom.gc.ca/speech/02_05_a_000309_e.asp (last visited June 19, 2002) ("As well intentioned as the CSA Model Privacy Code is, it is not a watertight legal text. Settling in its interpretation will not be easy.").

[30] Office of the Privacy Commissioner, Privacy Commissioner Releases His Finding on the Prescribing Patterns of Doctors (Oct. 2, 2001), *available at* http:www.privcom.gc.ca/media/an/wn_011002_e.asp (last visited June 19, 2002).

[31] CMA Health Information Privacy Code, *available at* http://www.cma.ca/cma/common/DisplayPage.do?pageId=/StaticContent/HTML/NO/I2/where_we_stand/1998/09-16.htm (last visited June 19, 2002).

[32] PIPEDA Schedule 1, § 4.10.2 (emphasis added). *See also id.* § 5(2) ("The word 'should' ... indicates a recommendation and does not impose an obligation.").

[33] *Id.* § 18(1).

II. RIGHTS AND OBLIGATIONS UNDER THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT

A. *Scope of the Act*

The Act requires "every organization" that "collects, uses or discloses" personal information "in the course of commercial activities" to take steps to protect individual privacy.[34] This requirement encompasses four basic points.

1. *Every Organization*

First, the Act applies to "every organization." An "organization" is an association, a partnership, a person, or a trade union.[35] It includes both "brick-and-mortar" and e-commerce businesses, and would clearly extend to physicians, pharmacies, and pharmaceutical and device manufacturers.[36]

2. *Collection, Use, and Disclosure*

Second, the Act applies to the collection, use, and disclosure of personal information.[37] "Use" is the "treatment and handling of personal information within an organization."[38] According to the Model Code, this occurs "any time data about an identifiable individual is accessed, manipulated, altered, deleted, or destroyed within the organization."[39] This would include the processing of payroll information about employees, for example, as well as the manipulation of data collected in a clinical trial. In contrast, "disclosure" involves the transfer of data outside the organization.[40] This would presumably include the transfer of clinical trial data or adverse event data pertaining to a marketed product to a foreign regulatory agency like the U.S. Food and Drug Administration (FDA).

The Privacy Commissioner emphasizes that collection, use, and disclosure are separate events.[41] For example, consent to collect names and addresses for billing purposes (a use) does not indicate consent to transfer that data to third-party advertisers (an unrelated disclosure). Analogously, consent to the collection and analysis of one's basic health information for epidemiological purposes does not contribute consent to the sale of that information by the collecting company to a third party for direct-to-consumer marketing of healthcare products. The organization must treat these activities as separate and obtain consent for each.

---

[34] *Id.* § 4(1).

[35] *Id.* § 2(1).

[36] Office of the Privacy Commissioner, Backgrounder: The Personal Information Protection and Electronic Documents Act, *available at* http://www.privcom.gc.ca/information/02_06_07_e.asp (last visited June 19, 2002).

[37] PIPEDA § 4(1)(a).

[38] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, YOUR PRIVACY RESPONSIBILITIES: A GUIDE FOR BUSINESSES AND ORGANIZATIONS 2 (2001) [hereinafter GUIDE FOR BUSINESSES].

[39] CANADIAN STANDARDS ASSOCIATION, MAKING THE CSA PRIVACY CODE WORK FOR YOU 10 (1996) [hereinafter CSA WORKBOOK].

[40] *Id.*; *see also* GUIDE FOR BUSINESSES, *supra* note 38, at 2.

[41] George Radwanski, Privacy Commissioner of Canada, Address to the Institute of Canadian Advertising (Feb. 27, 2001), *available at* http://www.privcom.gc.ca/speech/02_05_a_010227_e.asp (last visited June 19, 2002).

3. *Personal Information*

Third, the Act applies to "personal information," which is "information about an identifiable individual." Personal information may take many forms. It includes factual data such as an individual's name, age, identification numbers, income, ethnic origin, blood type, and genetic data.[42] The Commissioner may read this definition even more broadly to include tissue, blood, and other biological samples. In a recent speech, he argued that a code protecting the privacy of genetic information "must govern collection, analysis, retention, and disclosure of genetic *material*, not just the information derived from it."[43]

Personal information includes subjective data such as an individual's opinions, evaluations, comments, and social status.[44] It includes recorded data in employee files, credit records, loan records, medical records, disciplinary records, and records documenting disputes between a consumer and a merchant. It also includes unrecorded data such as an individual's oral expression of intent to acquire goods or services or to change jobs.[45]

a. *Identifiable Individual*

The Act governs information linked to an "identifiable individual." Data that have been made anonymous are exempt from the Act and may be used freely within an organization or disclosed to others outside the organization without the consent of the individual subject. The Privacy Commissioner has not clarified the meaning of "identifiable" or "anonymous," and no reported Privacy Commissioner decisions address the topic. If the identity of a data subject is apparent from the data (for instance, if the data include his name, or perhaps if they include a personal identification number), the Privacy Commissioner will undoubtedly consider the data subject "identifiable." It is less certain whether the Privacy Commissioner would consider a data subject to be "identifiable" if a recipient could, with some effort, identify the data subject through reference to other publicly-available information. It may be possible to persuade the Commissioner that data have been made anonymous if it would be extremely difficult (rather than impossible) to identify individuals. It is also unclear how the Privacy Commissioner would treat data that have been key-coded where the key has been separated from the data (for example, if a principal investigator codes clinical data prior to transferring the data to the trial sponsor).

b. *Personal Health Information*

Personal information includes personal health information about an individual, whether living or deceased.[46] Personal health information is:

---

[42] George Radwanski, Privacy Commissioner of Canada, Genetic Information and the Right to Privacy, Address to the UNESCO International Bioethics Committee (Sept. 13, 2001), *available at* http://www.privcom.gc.ca/speech/02_05_a_010913_e.asp (last visited June 19, 2002) ("Genetic information is personal health information.").

[43] *Id.*

[44] GUIDE FOR BUSINESSES, *supra* note 38, at 1.

[45] The Privacy Commissioner commended Parliament "for building in the flexibility to include collection of information that is not necessarily recorded" because it "allows individuals to challenge practices such as putting video cameras in change rooms even when the surveillance is not taped." Bruce Phillips, Privacy Commissioner of Canada, Comments Before the Standing Committee on Industry (Mar. 18, 1999), *available at* http://www.privcom.gc.ca/speech/archive/02_05_a_990318_e.asp (last visited June 19, 2002).

[46] Personal health information was excluded from the scope of the Act for the first year of its implementation.

- information about the physical or mental health of the individual;
- information about any health service provided to the individual;
- information about the donation by the individual of any body part or any bodily substance or information derived from the testing or examination of a body part or bodily substance;
- information collected in the course of providing health services to the individual; or
- information collected incidentally to the provision of health services to the individual.[47]

c. *Comparison With HIPAA*

The PIPEDA notions of "personal health information" and "identifiable individual" are consistent with, but more specific than, the definitions of "health information" and "individually identifiable health information" under the regulations issued by the U.S. Department of Health and Human Services (DHHS) pursuant to the Health Insurance Protection and Portability Act (HIPAA).[48]

Under the HIPAA privacy regulations, "health information" is any information that "relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual."[49] Although the U.S. definition is phrased differently than the Canadian definition, they should extend to the same data.

Health information is individually identifiable in the United States if it "identifies the individual" or provides "a reasonable basis to believe the information can be used to identify the individual."[50] Conversely, the U.S. privacy regulations do not apply to information that a covered entity has de-identified. Information is de-identified if it does not identify the individual and the covered entity has no reasonable basis to believe it can be used to identify the individual.[51]

There are two ways in which a covered entity may determine that it has met this standard. First, a person "with appropriate knowledge and experience applying generally accepted statistical and scientific principles and methods for rendering information not individually identifiable" may determine that the risk is "very small" that the information could be used by anticipated recipients to identify a subject.[52] Second, a covered entity may strip the information of eighteen enumerated identifiers; if, after having done so, the covered entity has "no actual knowledge" that the information could be used to identify a subject, the information is de-identified.[53] The enumeration of eighteen identifiers in the U.S. privacy regulations effectively creates a safe harbour that is technically not available under PIPEDA.

d. *Public Information*

Publicly-available information is not subject to the consent requirements of the Act. Accordingly, organizations do not need consent to collect, use, or disclose names, addresses, and telephone numbers appearing in a telephone directory, if the subscriber

---

[47] PIPEDA § 2(1).

[48] Pub. L. No. 104-191, Aug. 21, 1996, 110 Stat. 1936.

[49] 45 C.F.R. § 160.103.

[50] *Id.* § 164.501.

[51] *Id.* § 164.514.

[52] *Id.* § 164.514(b)(1).

[53] Enumerated identifiers include: biometric identifiers, full face photographic images, device identifiers and serial numbers, birth dates, and "any other unique identifying number, characteristic, or code." *Id.* § 164.514(b)(2).

may refuse to have this information appear in the directory. Contact information appearing in a business directory is similarly deemed public and may be collected, used, or disclosed for purposes related directly to the purpose for which the information appears in the directory. Personal information in court records is also considered public, as is information appearing in newspapers or other publications where the individual has provided the information.[54] Personal information collected under statutory authority and appearing in a public registry (e.g., directors ofcorporations listed under securities disclosure legislation) is also considered public.

4. *Commercial Activity*

Finally, the Act applies to "commercial activity," which includes "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character."[55] Neither the legislative history nor guidance from the Office of the Privacy Commissioner sheds further light on the phrase's meaning. Pharmaceutical and device manufacturers collect, analyze, and use personal health information for a variety of commercial purposes, including the preparation of applications for marketing authorization. This will constitute use "in the course of commercial activity" under PIPEDA. Accordingly, manufacturers will be subject to PIPEDA with respect to this personal information.

5. *General Exceptions From the Act*

PIPEDA does not apply to government organizations that are subject to the Federal Privacy Act. It does not apply to individuals collecting, using, or disclosing personal information only for domestic purposes (e.g., for personal address books). It does not apply to organizations collecting, using, or disclosing personal information only "for journalistic, artistic or literary purposes."[56]

The Act also excepts from the requirement of consent for use and disclosure information that is used or disclosed "for statistical, or scholarly study or research."[57] This exception applies if 1) the purposes cannot be achieved without using the information, 2) the organization takes steps to ensure confidentiality, 3) it would be "impracticable" to obtain consent, and 4) the organization gives prior notice to the Privacy Commissioner. The Commissioner has not discussed the scope of this exemption, but clearly it offers some possibilities for pharmaceutical and device manufacturers in Canada. On the one hand, it is unlikely that the classic research and development activities of a pharmaceutical or device manufacturer (e.g., research and development of a new chemical entity through clinical trials in order to prepare and submit an application for marketing authorization) would constitute "scholarly study or research" within the scope of this exception. For example, it will rarely be "impracticable" to obtain consent from clinical trial participants.[58] On the other hand, however, some medical research (e.g., retrospective epidemiological research unrelated to a particular product and conducted by researches at a university medical center) might fall within the exception. There may be room to argue for application of the exception at points along the spectrum between these examples.

---

[54] C.R.C. 2001-7(e), Regulations Specifying Publicly Available Information.

[55] PIPEDA § 2(1).

[56] *Id.* § 4(2).

[57] *Id.* § 7(2)(c).

[58] This exception could alleviate some of the burden imposed on pharmaceutical and device manufacturers by the supposed retroactivity of the Act. In some cases a company might conclude it is difficult or impossible to contact data subjects from long concluded trials in order to obtain consent to transfer. It may be possible to argue for application of this exception in that situation.

Provincial legislation providing "substantially similar" protection to personal information preempts the Act.[59] To date, only Quebec has implemented comprehensive privacy legislation. The Quebec statute is discussed in section IV of this article.

B. *Obligations of the Organization*

An organization subject to PIPEDA must identify the purpose(s) for which it collects, uses, and discloses personal information. It may not collect, use, or disclose that information except to fulfill those stated purposes, and may do so only with the consent of the data subject. It must keep the information as accurate and current as necessary to ensure that incorrect information is not used to make a decision about the individual. The organization is also subject to administrative requirements designed to protect personal information in its possession.

1. *Identifying Purposes for Collection, Retention, Use, and Disclosure*

Before collecting personal information, an organization must identify the purpose(s) for which the information will be used. An organization may collect personal information only for a purpose that a reasonable person would consider "appropriate."[60] Both the amount and the type of information collected must be "limited to that which is necessary to fulfill the purposes identified."[61] Any information that is no longer needed to fulfill a stated purpose should be "destroyed, erased or made anonymous."[62]

The organization may only make uses and disclosures of personal information that are consistent with its stated purpose. Although this would seem to suggest broadly worded consents are more effective, consent to a purpose stated without adequate precision may be deemed invalid.[63] To determine whether a use is consistent with a stated purpose, the organization must ask whether a reasonable person would consider the use reasonably related to the purpose consented to.[64]

If an organization wishes to use or disclose already-collected information for a purpose other than the purpose for which it was originally collected, the organization must inform the individual subject and secure his consent. Also, an organization collecting information must do so "by fair and lawful means."[65] Thus, it may not mislead or deceive individuals about the purpose for which it is collecting information.

2. *Consent*

Unless one of the express exceptions applies, as of January 1, 2002, no private sector organization subject to PIPEDA may disclose for consideration information in one province that was collected in another, without the data subject's consent. After January 1, 2004, no private sector organization covered under the law will be permitted to collect, use, or disclose personal information about someone without his consent.[66] Normally,

[59] PIPEDA § 26(2)(b).

[60] *Id.* § 5(3); GUIDE FOR BUSINESSES, *supra* note 38, at 6.

[61] PIPEDA Schedule 1, § 4.4.1.

[62] *Id.* Schedule 1, § 4.5.3.

[63] GUIDE FOR BUSINESSES, *supra* note 38, at 8.

[64] *Id.* at 6.

[65] PIPEDA Schedule 1, § 4.4.2.

[66] George Radwanski, Privacy Commissioner of Canada, ePrivacy–Transforming Customer Privacy into a Catalyst for Your Business, Address to the eCustomer World 2001 Conference (Oct. 9, 2001), *available at* http://www.privcom.gc.ca/speech/02_05_ a_011009_e.asp (last visited June 19, 2002).

the organization must obtain consent from the individual whose personal information is being collected. If, however, the individual is seriously ill, is mentally incapacitated, or is a minor, the organization may obtain consent from a legal guardian or a person having power of attorney.[67]

a. *Meaningful Consent Required*

An organization must obtain an individual's meaningful consent to collect, use, or disclose his personal information. For his consent to be meaningful, the individual must understand how the organization will use his personal information.[68] The organization must therefore "make a reasonable effort" to advise the individual of the purposes of the data collection in a manner that ensures "the individual can reasonably understand how the information will be used or disclosed."[69] According to the Privacy Commissioner, consent clauses should 1) be easy to find, 2) use clear and straightforward language, 3) not use blanket categories for purposes, uses and disclosures, and 4) be as specific as possible about which organizations handle the information.[70]

b. *Freely Given Consent*

Consent must be freely given. The organization may not make consent a condition of supplying a product or service "beyond that required to fulfill the explicitly specified, and legitimate purposes" for which it is collecting, using, or disclosing the information in the first instance.[71] Although the Privacy Commissioner has offered no guidance on this point, it is likely he would say a physician may not condition medical treatment on the patient's willingness to have his medical information sold to a pharmaceutical manufacturer. On the other hand, a pharmaceutical company or medical researcher presumably could condition participation in a clinical trial on the subject's willingness to have his data analyzed and included in an application for marketing authorization. The Privacy Commissioner has not addressed these questions, however, or the related question whether participation in a trial could be subject to a patient's willingness to waive his right of access to his data.

c. *Scope of Consent*

An organization may not construe consent to use personal information for a given purpose beyond "the reasonable expectations of the individual."[72] For example, an individual would reasonably expect that a publisher will use name and address information collected from new magazine subscribers for mailing and billing purposes and to solicit renewals.[73] An individual would not reasonably expect, however, that a healthcare provider, collecting personal information from persons seeking medical care, will give that information to a company selling healthcare products.[74] In this case, the healthcare provider would need to identify the second purpose and seek the individual's separate consent.

---

[67] GUIDE FOR BUSINESSES, *supra* note 38, at 9.
[68] *Id.*
[69] PIPEDA Schedule 1, § 4.3.2.
[70] GUIDE FOR BUSINESSES, *supra* note 38, at 9.
[71] PIPEDA Schedule 1, § 4.3.3.
[72] *Id.* Schedule 1, § 4.3.5.
[73] *Id.* Schedule 1, § 4.3.4.
[74] *Id.* Schedule 1, § 4.3.5.

d. *Means of Expressing Consent*

The statute permits implied as well as express consent, and oral as well as written consent.[75] It does not require any particular type of consent in any particular situation, and the Privacy Commissioner has explained that the type of consent required depends on the nature of the information collected and the circumstances under which consent is given.[76] An organization should seek express consent (i.e., "opt-in" consent),[77] either oral or written,[78] for information considered sensitive.[79] The statute does not define "sensitive data" and the Privacy Commissioner has not offered a definition. The phrase likely includes all personal health information. Implied consent (i.e., "opt-out" consent) may be sufficient for less sensitive data.[80] The current Privacy Commissioner, however, does not favor "opt-out" consent,[81] and a case pending before his office may provide an opportunity for him to articulate the situations, if any, where opt-out is permissible.[82]

e. *Withdrawal of Consent*

An individual may withdraw his consent for an organization's collection, use, or disclosure of his personal information at any time, "subject to legal or contractual restrictions and reasonable notice."[83] If there are consequences to withdrawing consent, the organization must explain them when it secures the data subject's initial consent.[84] It appears that a clinical trial informed consent form could state that, although a trial participant may withdraw from the trial, any data collected prior to withdrawal will continue to be used.

f. *Exceptions to the Consent Requirement*

Although consent is the cornerstone of the Act's privacy protections, it is not absolute. The Act provides specific exceptions from the consent requirement for the collection, use, and disclosure of information. Some of these exceptions are of particular importance to pharmaceutical and device manufacturers.

First, an organization need not obtain an individual's consent to *collect* personal information if the collection is clearly in the interests of the individual and the organization cannot obtain consent in a timely way.[85]

---

[75] *Id.* Schedule 1, § 4.3.7.

[76] GUIDE FOR BUSINESSES, *supra* note 38, at 9.

[77] The statute does not explicitly equate express consent with "opt-in" consent, or implied consent with "opt-out" consent. The writings of the Privacy Commissioner are, however, consistent with this reading.

[78] PIPEDA Schedule 1, § 4.3.7; GUIDE FOR BUSINESSES, *supra* note 38, at 9.

[79] PIPEDA Schedule 1, § 4.3.6; Radwanski, Address to the eCustomer World 2001 Conference, *supra* note 66.

[80] PIPEDA Schedule 1, § 4.3.6.

[81] Radwanski, Address to the eCustomer World 2001 Conference, *supra* note 66 ("Most privacy advocates, myself included, consider opt-out to be pretty poor privacy . . . . I suggest that you be cautious about what's known as 'opt-out' consent.").

[82] Public Interest Advocacy Center, Complaint re: Inadequate Approaches to Opt-Out Consent (Oct. 16, 2001), *available at* http://www.piac.ca/Complaint%20to%20PCC-LH.htm (last visited June 19, 2002) (charging that implied consent policies are insufficient to permit transfers for secondary marketing purposes).

[83] PIPEDA Schedule 1, § 4.3.8.

[84] CSA WORKBOOK, *supra* note 39, at 11.

[85] PIPEDA § 7(1). Other exceptions to consent for collection of personal information apply if: 1) the collection is reasonably related to a criminal investigation and the individual's knowledge or consent would compromise the availability or the accuracy of the information; and 2) the collection is solely for journalistic, artistic, or literary purposes.

Second, an organization need not obtain an individual's consent to *use* personal information if the information is used to respond to an emergency threatening the life, health, or security of an individual, or if the information is necessary for statistical, scholarly, or research purposes and obtaining consent for the use is impracticable. In such cases, the organization must ensure the information's confidentiality and give prior notice of the use to the Privacy Commissioner.[86]

Third, an organization need not obtain an individual's consent to *disclose* personal information if the disclosure is required by law. It may be possible to argue that the requirements of foreign law (e.g., event reporting requirements) trigger this exception. As noted earlier, an organization need not obtain an individual's consent to disclose personal information if the information is necessary for statistical, scholarly, or research purposes and obtaining consent for the disclosure is impracticable. In this case, the organization must give prior notice of the disclosure to the Privacy Commissioner. Further, an organization need not obtain an individual's consent to disclose personal information if the disclosure is made at the earlier of either a) 100 years after the organization collected the personal information, or b) twenty-five years after the death of the subject of the personal information. Finally, an organization need not obtain an individual's consent to disclose personal information if the disclosure is made to a person responding to an emergency threatening the life, health, or security of an individual. If the subject of the disclosed personal information is alive, the organization must promptly inform that person of the disclosure.[87]

g. *Retroactive Application*

The Privacy Commissioner has stated that personal information collected prior to the Act's effective date is subject to its provisions.[88] In his view, once the Act applies to an organization, the organization may not use or disclose information within its possession—no matter when it was collected—without legally valid consent. This retroactive effect is not apparent on the face of the statute.

The Privacy Commissioner could take the position, therefore, that identifiable data collected in a clinical trial prior to January 2002 may not be disclosed for consideration by an organization subject to PIPEDA unless the data subjects provided opt-in consent that complied with PIPEDA. He could similarly conclude that identifiable data collected prior to January 2004 may not be used unless it was collected in compliance with PIPEDA. At a minimum, this suggests the need to ensure on a prospective bases that all data collected are collected in conformity with PIPEDA. Companies also should review data within their possession to determine whether subjects adequately consented. As noted above, the exception for data necessary for research purposes, where obtaining consent is impracticable, could alleviate some of the burden posed by the Act's retroactive application.[89]

---

[86] *Id.* § 7(2). In addition, if, in the course of its activities, an organization determines that personal information in its possession might reasonably be useful to a criminal investigation, an organization need not obtain an individual's consent to use personal information.

[87] *Id.* § 7(3). Other exceptions to consent for disclosure of personal information apply if: 1) the disclosure is made to a barrister or solicitor representing the organization in the Province of Quebec; 2) the disclosure is for the purpose of collecting a debt owed by the individual to the organization; 3) the disclosure is required to respond to a subpoena or warrant issued by a court; 4) the disclosure is made to a government institution investigating criminal conduct or other security concerns; and 5) the disclosure is made to an institution whose functions include the conservation of records of historic or archival importance, and the disclosure is made for the purpose of such conservation.

[88] GUIDE FOR BUSINESSES, *supra* note 38, at 8.

[89] *See supra* note 58.

3. *Accuracy*

An organization must keep personal information as accurate and current as necessary "to minimize the possibility that inappropriate information may be used to make a decision about the individual."[90] The use of incomplete, wrong, or obsolete information for decisionmaking can result in "significant harm to the individual and lost opportunities for the company."[91] Accordingly, if an organization uses personal information on an ongoing basis or routinely shares information with third parties, it should ensure the information's accuracy. Drafters of the Model Code emphasized the importance of "updating, amending, or correcting" erroneous information "as expeditiously as possible."[92] At the same time, the Act specifically prohibits an organization from routinely updating personal information "unless such a process is necessary to fulfill the purposes for which the information was collected."[93] Organizations will in all likelihood need to rethink their data retention policies, including why they update certain data, and how they purge data that are no longer needed.

4. *Administrative Requirements*

The Act imposes various administrative obligations on organizations subject to its provisions.

First, an organization must develop a privacy policy and procedures that address each of the obligations imposed by PIPEDA.[94] These documents must state the organization's purpose for collecting data, prescribe methods for securing consent, impose limits on data use and disclosure, ensure accuracy and security, provide for individual access, and provide a framework for responding to inquiries and complaints.

Second, to oversee implementation of its privacy policy and practices, the organization must designate an individual or individuals responsible for the organization's compliance with the Act. The Office of the Privacy Commissioner urges organizations to assign oversight responsibilities to management employees, preferably senior executives.[95]

Third, an organization must make public its privacy policies and procedures and identify the persons responsible for implementing them. It must identify the type of personal information it holds and the purpose(s) for which it does so, and it must explain how the data subjects may access this information. It must describe the information that is made available to other organizations, including subsidiaries,[96] and, if requested, it must provide a list of any organizations to which it has disclosed such information.[97]

Fourth, an organization must adopt security safeguards commensurate with the sensitivity of the personal information in its possession.[98] Such measures should address

[90] PIPEDA Schedule 1, § 4.6.1.

[91] CSA WORKBOOK, *supra* note 39, at 18.

[92] *Id.* Because the organization continues to be responsible for personal information until it is destroyed, the organization is likely obligated to inform third party recipients of that information of any changes.

[93] PIPEDA Schedule 1, § 4.6.2.

[94] *Id.* Schedule 1, § 4.1.4.

[95] Anne Rooke, The Role of the Federal Privacy Commissioner, Presentation to Ottawa Conference on E-Commerce and Privacy: Implementing the New Law in the Public and Private Sector (Feb. 21, 2000), *available at* http://www.pivcom.gc.ca/speech/02_05_a_000221_2_e.asp (last visited June 19, 2002).

[96] PIPEDA Schedule 1, § 4.8.2; GUIDE FOR BUSINESSES, *supra* note 38, at 15.

[97] GUIDE FOR BUSINESSES, *supra* note 38, at 15.

[98] PIPEDA Schedule 1, § 4.7.2.

the manner in which the information is stored and should protect against loss or theft as well as unauthorized access, disclosure, copying, use, or modification of the data.[99]

5. *Transfers to Third Parties*

An organization is responsible for personal information "under its control."[100] Although the Act does not define when information is under the control of an organization, the Act's requirements logically apply to personal information in the organization's possession or custody.[101] They also apply to information the organization transfers to third parties for processing.[102] This suggests that an organization may be liable for any privacy offenses those parties commit. When contracting with third parties to handle personal information, an organization therefore should include provisions to ensure adequate privacy protection.[103] For example, the contract should ensure that the third party: 1) names a person to oversee privacy matters related to the contract; 2) limits use of the personal information to the purposes specified by the contract; 3) limits disclosure of the personal information to what is authorized by the collecting organization or required by law; 4) refers data subjects looking to access the personal information to the collecting organization; 5) returns or disposes of the personal information after completion of the contract; 6) uses appropriate security measures to protect the personal information; and 7) allows the collecting organization to audit the third party's compliance with the contract as necessary.[104] Inclusion of these provisions in a contract probably will not relieve the collecting organization from responsibility under the statute. It may provide some recourse, however, against a third party that commits a privacy offense.

The statute does not address transfers of personal information to parties outside of Canada and the Privacy Commissioner has not addressed the subject. In light of the Privacy Commissioner's view, however, that 1) the Act applies to conduct outside Canada,[105] and 2) an organization is responsible for the acts of its agents, an organization inside Canada should expect to answer to the Privacy Commissioner if a recipient in the United States fails to comply with the PIPEDA standards.

C. *Individual Rights Under PIPEDA*

A data subject has several rights enumerated in PIPEDA. First, subject to several significant exceptions, he has the right to access the personal information about him that an organization holds. Second, subject again to several exceptions, he has the right to demand that inaccuracies be corrected. Third, he has the right to complain about the organization's privacy practices either to the organization or to the Privacy Commissioner, and the right to take his grievance to federal court. This section addresses the

[99] *Id.* Schedule 1, § 4.7.1.

[100] *Id.* Schedule 1, § 4.1.

[101] *Id.* Schedule 1, § 4.1.3.

[102] *Id.* (requiring organizations to "use contractual or other means to provide a comparable level of protection while the information is being processed by a third party").

[103] *Id.*

[104] GUIDE FOR BUSINESSES, *supra* note 38, at 7.

[105] George Radwanski, Privacy Commissioner of Canada, Address to the Third Annual BNA Public Policy Forum: International eCommerce and Internet Regulation (Nov. 14, 2001), *available at* http://www.privcom.gc.ca/speech/02_05_a_011114_e.asp (last visited June 19, 2002) (noting that the effect of the Act "won't be limited by the Canada-U.S. border, because it's not just Canadians who have rights under the act, but anyone whose personal information is collected, used, or disclosed by an organization subject to the Act").

first two rights. The third is addressed in Part III of the article, which discusses enforcement of the Act.

1. *Access*

If asked by an individual, an organization must accurately report what personal information, if any, it holds about that person.[106] It must also provide assistance to any individual who needs help preparing a written request.[107] The organization also must provide an accounting of "the use that has been made or is being made of this information,"[108] and "third parties to which [the organization] has [or may have] disclosed personal information about an individual."[109] The organization must respond to requests "with due diligence and in any case not later than thirty days after receipt,"[110] and "at minimal or no cost to the individual."[111] Furthermore, it must provide the information "in a form that is generally understandable," that is, without unexplained codes or abbreviations.[112]

There are significant exceptions to the access requirement. First, the organization may choose to make "sensitive medical information" available only "through a medical practitioner."[113] Second, the organization may deny individuals access to information that is prohibitively expensive to provide, that contains references to other individuals, or that is privileged for legal, security, or commercial proprietary reasons. The scope of the exception for "commercial proprietary reasons" is not clear. It could extend to some information generated in a clinical trial or generated in the course of research on a biological sample. If an organization denies access to personal information, it must provide reasons for the denial upon request by the individual.

2. *Correction*

If an individual believes that personal information in an organization's records is inaccurate, he may ask the organization to correct it.[114] The individual must make this request in writing and attach documents demonstrating the data error.[115] If it agrees with the request, the organization must promptly amend its records. It may, however, dispute the request and leave its records unchanged. In that case, the individual may require the organization to attach a statement to his file noting the disagreement. The organization must pass this statement on if it discloses the data to a third party.[116]

---

[106] The request must be made in writing, *see* PIPEDA § 8(1), and must include enough detail to allow the organization to identify the desired data, e.g., it should include dates, account numbers, and the names and positions the person may have dealt with at the organization. *See* OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, YOUR PRIVACY RIGHTS: A GUIDE FOR CANADIANS (2001) [hereinafter GUIDE FOR CANADIANS].

[107] GUIDE FOR BUSINESSES, *supra* note 38, at 15.

[108] PIPEDA Schedule 1, § 4.9.1.

[109] *Id.* Schedule 1, § 4.9.3.

[110] *Id.* § 8(3). The organization may extend this time limit for a maximum of thirty additional days if "meeting the time limit would unreasonably interfere with the activities of the organization," or "the time required to undertake any consultations necessary to respond to the request would make the time limit impracticable to meet." *Id.* § 8(4)(a). Alternatively, the organization may extend the time limit for whatever period "is necessary to be able to convert the personal information into an alternative format." *Id.* § 8(4)(b). In either case, the organization must give notice of the extension to the individual within the original thirty-day period. *Id.*

[111] *Id.* Schedule 1, § 4.9.4.

[112] *Id.*

[113] *Id.* Schedule 1, § 4.9.1.

[114] GUIDE FOR CANADIANS, *supra* note 106.

[115] *Id.*

[116] *Id.*

III. ENFORCEMENT OF THE ACT

The statute requires every organization under its jurisdiction to establish a procedure for responding to complaints. A data subject may complain directly to the organization about its collection, use, or disclosure of his data. In addition, or in the alternative, a data subject may file a written complaint directly with the Privacy Commissioner. The Act allows recourse to the courts after review by the Privacy Commissioner. The Act also allows the Privacy Commissioner to act independently to audit the privacy policies and procedures of an organization suspected of committing violations.

A. *Complaint to the Organization*

An organization must have "easily accessible and simple to use" procedures in place for receiving and responding to complaints from individual data subjects respecting the organization's collection, use, or disclosure of personal information.[117] An organization must advise data subjects of available "avenues of recourse," including the organization's "relevant complaint procedures,"[118] any applicable industry association procedures, and the statutory provisions for filing complaints directly with the Privacy Commissioner. If an organization receives a complaint, it must investigate.[119] The organization must take appropriate measures, including amending its privacy policies and practices, if it finds the complaint is justified.[120]

The Privacy Commissioner offers several recommendations with respect to the handling of internal investigations. For example, he recommends opening a clear channel of communication with the individual to acknowledge receipt of the complaint, to clarify the nature of the complaint, and to provide prompt notification of the outcome when reached. He recommends assigning the investigation to a person with access to both the relevant records and the employees who handled the personal information. He also recommends keeping a record of decisions following investigations to "ensure consistency in applying the Act."[121]

B. *Individual Complaints Filed With the Privacy Commissioner*

An individual data subject may file a written complaint directly with the Privacy Commissioner. The Commissioner will review the complaint and, if "satisfied that there are reasonable grounds" to do so, may initiate an investigation.[122]

The Commissioner's investigative powers under the Act are broad. While pursuing an investigation, the Commissioner has the authority to "summon and enforce the appearance of persons before the Commissioner and compel them to give oral or written evidence on oath and to produce any records and things that the Commissioner considers necessary to investigate the complaint, in the same manner and to the same extent as a superior court of record." In other words, the Commissioner has subpoena power. He may also "administer oaths" and "receive and accept any evidence and other information, whether on oath, by affidavit or otherwise, that the Commissioner sees fit." The Commissioner may review this evidence "whether or not it is or would be admissible in

[117] PIPEDA Schedule 1, § 4.10.2.
[118] *Id.* Schedule 1, § 4.10.3.
[119] *Id.* Schedule 1, § 4.10.4.
[120] *Id.*
[121] GUIDE FOR BUSINESSES, *supra* note 38, at 16.
[122] PIPEDA § 11(2).

a court of law." The Commissioner or his staff may "enter any premises, other than a dwelling-house, occupied by an organization on satisfying any security requirements of the organization relating to the premises." They may question or converse with "any person in any premises" entered. Finally, they may "examine or obtain copies of or extracts from records found" on the premises if the records "contain any matter relevant to the investigation."[123] If in the course of an investigation the Commissioner finds evidence of an unrelated crime, he may report it to the appropriate authorities.[124]

The Privacy Commissioner has expressed a reluctance to use these powers, and in November 2001, his Office reported that all complaints to date had been "resolved without having to use these formal investigative powers, because voluntary cooperation with investigations has been forthcoming."[125] The Privacy Commissioner states that the focus of his staff is "to seek whenever possible to resolve disputes through investigation, persuasion, mediation, and conciliation."[126]

The Commissioner will prepare a report of findings and recommendations from his investigation. He may then try to mediate the controversy or resolve the complaint through some other method for dispute resolution. Although the Commissioner may not issue binding orders, he may make his findings public.[127] He may also include the audit report in his annual report to Parliament.[128] Alternatively, he may seek remedies in court, advise the complainant to "exhaust grievance or review procedures otherwise reasonably available," or advise him to pursue the complaint under a law other than the Act.[129]

It is a criminal offense to obstruct the Commissioner during an investigation or audit.[130] It is a criminal offense to knowingly dispose of information that is the subject of a request by an individual.[131] Anyone who obstructs the Commissioner or who destroys records before all recourse is exhausted is guilty of an offense and may be liable for fines of up to $100,000.[132] It is also a criminal offense for an employer to take retaliatory action against employees who report a violation of the Act.[133] Directors, officers, and employees may be made personally liable for fines.[134]

C. *Individual Complaints Filed With the Federal Court*

If not satisfied by the remedies afforded by the Commissioner, a complainant may take his grievance to federal court. A reviewing court might determine, for example, whether a company had properly identified and documented the purposes for which data were being collected,[135] or whether it had used or disclosed data for purposes other than those for which it the data were collected.[136] The Commissioner may represent the complainant at the hearing or, with leave of the court, appear on his own behalf.[137] If the

[123] *Id.* § 12(1).

[124] *Id.* § 20(5).

[125] About the Office of the Privacy Commissioner, *supra* note 10.

[126] GUIDE FOR BUSINESSES, *supra* note 38, at 19.

[127] George Radwanski, Privacy Commissioner of Canada, Privacy and Health Information, Address to the Canadian Medical Association (Nov. 24, 2000) (noting that the Commissioner is "free to make privacy abuses known to the media. The court of public opinion can be a powerful force.").

[128] PIPEDA § 19(2).

[129] *Id.* § 13(2).

[130] *Id.* § 28.

[131] *Id.*

[132] *Id.* § 28(b).

[133] *Id.* § 27.1.

[134] *Id.* § 28 (holding "[e]very person who knowingly contravenes" the Act responsible).

[135] PIPEDA Schedule 1, § 4.2.

[136] *Id.* Schedule 1, § 4.5.

[137] PIPEDA § 15(c).

court finds in favor of the complainant, it may order the organization to correct its practices in order to comply with the statute, order the organization to publish a notice of any action taken or proposed to be taken to correct its practices, and award damages to the complainant, including unlimited damages for any humiliation that the complainant has suffered.[138]

D. *Audits*

The Commissioner may "on reasonable notice" and "at any reasonable time," audit the personal information management practices of an organization if the Commissioner has "reasonable grounds" to believe that the organization is contravening a provision of the statute.[139] A complaint from a competitor or public interest group could presumably provide these "reasonable grounds." The powers available to the Commissioner during an audit are the same as his investigative powers.[140] If in the course of an audit the Commissioner finds evidence of an unrelated crime, he may report it to the appropriate authorities.[141] After an audit, the Commissioner must file a report with the organization, summarizing his findings and offering recommendations for revising privacy policies and procedures to ensure compliance with the Act.

IV. THE RELATIONSHIP BETWEEN PIPEDA AND OTHER PRIVACY LAWS

A. *Legislation in Canada*

1. *The Federal Privacy Act*

PIPEDA works in conjunction with the Federal Privacy Act. The Privacy Act applies to specific government institutions and imposes requirements of notice, choice, and access on their handling of personal information. When fully in force, PIPEDA will apply similar principles to the commercial sector. The two regimes are not, however, identical. For example, the Privacy Act does not require consent to collect personal information. Instead it requires that collected information relate directly to an activity of the collecting institution.[142] This may complicate transfers of personal health information from the public health sector to the private sector.

2. *Provincial Law*

Prior to enactment of PIPEDA, several provinces had enacted sector-specific privacy laws. Two such statutes are Manitoba's Personal Health Information Act and Saskatchewan's Health Information Protection Act.[143] Several more provinces have enacted sector-specific privacy laws since PIPEDA. In April 2001, for example, Alberta enacted a Health Information Act regulating information handled by healthcare providers.[144] Thus, an organization operating in a province that has enacted sector-specific

[138] *Id.* § 16; GUIDE FOR BUSINESSES, *supra* note 38, at 24.

[139] PIPEDA § 18(1).

[140] *Id.* § 18(1)(a)-(f).

[141] *Id.* § 20(5).

[142] Privacy Act § 4, Collection, Retention and Disposal of Personal Information.

[143] *See generally* Manitoba Access and Privacy Division, *available at* http://www.ombudsman.mb.ca; Saskatchewan Health, *available at* http://www.health.gov.sk.ca (last visited June 19, 2002).

[144] *See generally* Alberta Health and Wellness, *available at* http://www.health.gov.ab.ca (last visited June 19, 2002).

legislation may need to consider both the federal PIPEDA and provincial health privacy law.

Only one province has enacted comprehensive privacy legislation. In 1994, Quebec enacted the Personal Information Protection Act (PIPA),[145] which, like the federal Act, governs the collection, retention, use, and disclosure of personal information. PIPA defines personal information as "any information which relates to a natural person and allows that person to be identified,"[146] and it allows collection, use, or communication of such information only if the data subject consents and only for a specifically-identified purpose. Largely in deference to the existing Quebec law, PIPEDA includes a provision that

> the Governor in Council may, by order, . . . if satisfied that legislation of a province that is substantially similar to this Part applies to an organization, a class of organizations, an activity, or a class of activities, exempt the organization, activity, or class from the application of this Part in respect of the collection, use, or disclosure of personal information that occurs within that province."[147]

The legislative history makes it clear that Parliament intended this to reach the Quebec statute,[148] and the Privacy Commissioner has stated repeatedly that the government has concluded Quebec meets the "substantially similar" standard.[149]

B. *Foreign Law*

Organizations operating in the European Union and the United States, in addition to Canada, also will need to take into account the European Community's Data Protection Directive[150] and the regulations promulgated by DHHS under HIPAA.[151]

The EU, U.S., and Canadian laws reflect what have now become generally-accepted principles of privacy law—that data subjects should be told of the uses that will be made of their data (notice), that they will be asked to consent to these uses or will be given the choice to refuse those uses (choice and consent), that they will be allowed to see and to correct the data that are held (access), that organizations must safeguard personal data from unauthorized uses and accidental disclosures (security), and that organizations are accountable for privacy violations (accountability).

A comprehensive and detailed comparison of PIPEDA with the Directive and the HIPAA regulations is beyond the scope of this article. The schemes differ, however, in several key respects. For example, the EU distinguishes between sensitive data and nonsensitive data, requiring opt-in consent for collection, use, and disclosure of sensi-

---

[145] R.S.Q. Ch. P-39.1, An Act Respecting the Protection of Personal Information in the Private Sector.

[146] *Id.* Div. 1, § 2.

[147] PIPEDA § 26(2)(b).

[148] Phillips, 1999 Annual Report of the Privacy Commissioner, *supra* note 3 ("The federal government has stated that Quebec will be exempt from the federal law because Quebec's 1994 legislation covers the private sector and is substantially similar to Part 1.").

[149] *See, e.g., id.*; George Radwanski, Privacy Commissioner of Canada, Address to the Canadian Institute (Dec. 6, 2000), *available at* http://www.privcom.gc.ca/speech/02_ 05_a_001206_e.asp (last visited June 19, 2002) ("The federal government has already stated publicly that Quebec's law is substantially similar so, in all likelihood, that exemption will be forthcoming.").

[150] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. 1995 O.J. (L 281) 31.

[151] Pub L. No. 104-191, § 264(c)(l); *see* 65 Fed. Reg. 82,462 (Dec. 28, 2000).

tive data. While the Canadian legislation acknowledges the category of sensitive data, it does not define "sensitive" and does not expressly require opt-in choice. To give another example, the preamble to the DHHS regulations addresses exemption from consent for the reporting of adverse events to FDA. Although Canadian law provides an exception for disclosures required by law, the Privacy Commissioner has not offered any interpretation of the scope of this provision. Also, the DHHS regulations include a list of eighteen identifiers of personal health information. If, after having stripped the information of these identifiers, a covered entity has "no actual knowledge" that the information could be used to identify a subject, the information is "de-identified" and, therefore, is outside the scope of the DHHS regulations.[152] In contrast, neither the Directive nor PIPEDA provides such a list. Individual EU Member States and the Canadian Privacy Commissioner may take differing views on whether exclusion of a particular element renders the data subject nonidentifiable.

Although the schemes differ, we have not identified any instance in which a company operating in the United States, the EU, or Canada, or transferring health data from one jurisdiction to another, would face conflicting obligations. Companies operating in Canada and the EU may take comfort also in a recent decision of the European Commissioner. In addition to regulating the processing of personal data within Europe, the Directive prohibits the transfer of data outside the European Economic Area unless the data will receive "adequate" protection in the importing country.[153] The Canadian Parliament's enactment of PIPEDA was prompted by a desire to satisfy the "adequate protection" standard and in December 2001, the European Commission found that it complied.[154] Accordingly, the EU now permits transfers between member states and organizations in Canada subject to the Act's provisions. The finding of adequacy suggests it should be feasible for a multinational corporation to derive a policy that satisfies both regimes. (The U.S. health privacy regulations do not address transfer to foreign jurisdictions.) Nevertheless, pharmaceutical and device manufacturers operating in multiple jurisdictions should review these frameworks more closely to confirm the absence of conflict. In the EU, individual Member State laws also should be taken into account. Similarly, individual U.S. state privacy laws will come into play, and Canadian provincial legislation could apply.

V. EFFECTIVE DATE AND TRANSITION PROVISIONS

From January 1, 2001, to January 1, 2002, PIPEDA applied to works, undertakings, and businesses within the legislative authority of Parliament. Examples of such works include interprovincial or international transportation by land or water, airports, aircraft or airlines, telecommunications, radio and television broadcasting, banks, grain elevators, nuclear facilities, and offshore drilling operations. The Act also applied to the entire commercial private sector in the Yukon, Northwest Territories, and Nunavut because all local businesses in the territories are considered federal works, undertakings, and businesses and are under the jurisdiction of the federal Parliament.[155] In addition, the Act applied to personal information disclosed for consideration outside the province in which it was collected. During this first year of its operation, however, the Act did not apply to personal health information.[156]

[152] 45 C.F.R. § 164.514(b)(2).

[153] 95/46/EC, Art. 25.

[154] Commission Decision 2002/02/EC of 20 December 2001, Art. 1.

[155] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, FEATURE: CANADA'S PRIVACY LAW AND THE NORTH (June 11, 2001).

[156] PIPEDA § 30(1.1), (2.1).

As of January 1, 2002, the Act also applies to personal health information collected, used, or disclosed by these organizations and to personal health information disclosed for consideration outside the province in which it was collected. After January 1, 2004, the Act will apply to the collection, use, and disclosure of personal information, including personal health information, by any organization in the course of commercial activity within a province. It also will apply to all personal information, including personal health information, in all interprovincial and international transactions by all organizations subject to the Act in the course of commercial activities.

VI. CONCLUSION

The Privacy Commissioner has thus far demonstrated his willingness to work with organizations to resolve privacy disputes fairly and in a manner that takes into account business concerns. But organizations must be wary of the consequences that might flow from a failure to follow the requirements or even recommendations of the new law. These consequences include considerable adverse publicity and apparently unlimited money damages. Particularly in light of the apparent retroactive nature of the statute, pharmaceutical and device manufacturers that collect, use, or disclose personal information in Canada, or that intend to do so, should undertake now 1) to ensure that all collection, use, and disclosure henceforth complies with PIPEDA, and 2) to take stock of the impact of the statute on already-collected data that may need to be used or disclosed after the transition period ends. Companies that operate in Canada, the EU, and the United States will need to take into account multiple legal frameworks that overlap, but are not identical.