Personal Information Protection and Electronic Documents Act

QUESTIONS AND ANSWERS FOR HEALTH RESEARCHERS

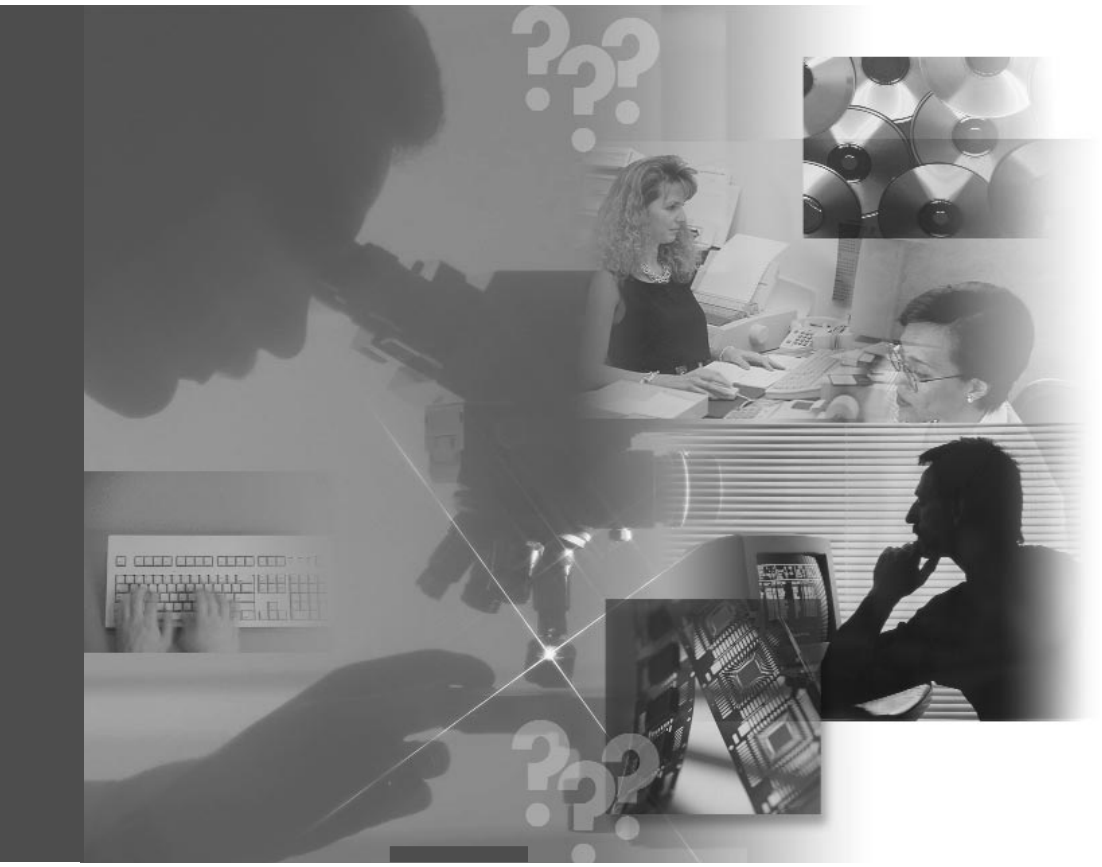
CIHR IRSC
Canadian Institutes of Health Research
Instituts de recherche en santé du Canada

Canadian Institute for Health Information
Institut canadien d'information sur la santé

Canada

Personal Information Protection and Electronic Documents Act

QUESTIONS AND ANSWERS FOR HEALTH RESEARCHERS



CIHR IRSC
Canadian Institutes of Health Research
Instituts de recherche en santé du Canada

CIHI ICIS
Canadian Institute for Health Information
Institut canadien d'information sur la santé

Canada

Canadian Institutes of Health Research (CIHR)
410 Laurier Avenue West
9th Floor, Address Locator 4209A
Ottawa ON
K1A 0W9

Canadian Institute for Health Information (CIHI)
377 Dalhousie Street, Suite 200
Ottawa ON
K1N 9N8

Cat. No. MR21-25/2001
ISBN 0-662-65741-1

Table of Contents

Preface

The Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5) received Royal Assent on April 13, 2000. Part 1 of the Act, entitled "Protection of Personal Information in the Private Sector", is intended to cover (a) personal information that an organization collects, uses or discloses in the course of commercial activities or, (b) employee information that an organization collects, uses or discloses in connection with a federal work, undertaking or business. The Act was proclaimed in force on January 1, 2001. However, its application is suspended in two respects:

<u>One year suspension for personal health information</u>

On recommendation of the Senate Standing Committee on Social Affairs, Science and Technology (the "Committee"), the application of Part 1 to personal health information has been suspended for one year following proclamation (January 1, 2002). After hearing testimony from the health sector, the Committee noted that the health sector was not part of the broad consensus supporting the bill and there was no consensus even within the health sector itself as to an appropriate solution.

In its Second Report dated December 6, 1999, the Committee identified a significant degree of uncertainty surrounding the application of Part 1 to personal health information. The Committee was of the view that, while Part 1 may be adequate in setting minimum legal standards for protecting the personal information of Canadians in the commercial arena, the adequacy of the CSA Code as a baseline standard for the health sector was open to question. In particular, the Committee stated that more specific provisions regarding informed consent and secondary use of personal health information should be developed. The Committee also observed considerable uncertainty around the nature of the consent required for the collection, use and disclosure of personal health information and the meaning of the term "in the course of commercial activities," particularly in the health sector. Accordingly, the Committee recommended suspending the application of Part 1 to personal health information for an additional year to "motivate stakeholders and governments to formulate a solution that is appropriate for the protection of personal health information".

On February 14, 2000, the Parliamentary Secretary to the Minister of Industry concurred with the recommendation of the Committee to suspend the application of Part 1 to personal health information. His proposal was to "allow the health sector one extra year from the time of proclamation to meet the requirements of the bill." He also stated that:

> *[d]uring this additional transition period, Industry Canada is ready to work with the entire health care sector, including commercial organizations, the provinces, Health Canada and other stakeholders to clarify any uncertainties on how Bill C-6 applies to them. Reasonable and practical solutions exist within the framework provided by the*

bill to ensure that the personal health information that is collected, used and disclosed in the course of commercial activities is protected by law.

More recently, on March 1, 2001, a motion was brought before the Senate to authorize the Senate Standing Committee on Social Affairs, Science and Technology to examine and to report, no later than June 30, 2001, on the developments of the PIPED Act since it received Royal Assent in April 2000.

Three year suspension for provinces

The application of Part 1 to: a) any organization that does not disclose personal information outside provincial or national boundaries for profit or some other benefit; or b) any organization that does not collect, use or disclose personal information in connection with a federal business, is suspended for a period of three years following proclamation (January 1, 2004). If within those three years, provinces adopt legislation substantially similar to Part 1, the Governor in Council may exempt from Part 1 all organizations or activities covered by that provincial law. This, in effect, gives provinces an additional three years to adopt substantially similar legislation before Part 1 applies to non-federal, intra-provincial, commercial activity. When the Act was before the Senate Standing Committee on Industry, Science and Technology on December 2, 1999, the then Minister of Industry, John Manley, described substantially similar legislation as "...legislation that provides a basic set of fair information practices which are consistent with the CSA Standard, oversight by an independent body and redress for those who are aggrieved." At that time, only Quebec had provincial legislation in place that the Minister would have considered "substantially similar."

Resulting from the combination of both of these suspensions, a flurry of policy-making and legislative activity can be expected within the next few years as jurisdictions attempt to promulgate the principles of Part 1 and apply them to the health sector. CIHR has undertaken several initiatives with a view to fostering discussion around more specific issues pertaining to the collection, use and disclosure of personal information for health research purposes. These Qs and As, prepared by CIHR, with CIHI, constitute one of these initiatives.

Terms

Throughout this document:

CIHI means Canadian Institute for Health Information;

CIHR means Canadian Institutes of Health Research;

CSA Code means the Canadian Standards Association's *Model Code for the Protection of Personal Information* CAN/CSA-Q830-96;

Commissioner means the Office of the Privacy Commissioner of Canada;

Compendium means the *Compendium of Canadian Legislation respecting the Protection of Personal Information in Health Research;*

PIPED Act or **the Act** means the *Personal Information Protection and Electronic Documents Act*, (S.C. 2000, c.5).

Introduction

These questions and answers (Qs & As) have been prepared by Canadian Institutes of Health Research (CIHR) and Canadian Institute for Health Information (CIHI) for the benefit of the health research community. The purpose of this document is to raise awareness of the new federal legislation governing the protection of personal information and its possible implications for health researchers. We would like to thank the Office of Health and the Information Highway (Health Canada), the Electronic Commerce Branch of Industry Canada and the Office of the Privacy Commissioner of Canada for their helpful consultation throughout this project.

It is important to note that, in addition to the new federal *Personal Information Protection and Electronic Documents Act*, provincial legislation continues to govern wherever applicable. For a review of federal and provincial legislation relevant to the collection, use and disclosure of personal information for health research purposes, see CIHR's *Compendium of Canadian Legislation respecting the Protection of Personal Information in Health Research (Public Works and Government Services Canada: Ottawa, 2000)* (the "*Compendium*").

While we have tried to be as specific as possible about the application of the new federal legislation, researchers should be aware that some answers to the following questions remain somewhat vague and ambiguous. Many concepts introduced in the new legislation simply cannot be ascertained at this stage, as they have yet to be defined through interpretations by the Federal Privacy Commissioner (the "Commissioner") and the courts. Over time, these interpretations will lend greater certainty to the meaning of the law and its application in the area of health research.

Despite the current uncertainty, you may consider the following factors as you prepare yourselves for the application of the new federal legislation:

- **the purpose of your research and the data needed to fulfil that purpose;**
- **the nature of the data you are collecting, using and/or disclosing;**
- **any commercial aspects of your research activity;**
- **any connection with the operation of a federal business;**
- **the geographic scope of your research;**
- **the general requirement for consent, its nature and its form;**
- **your general data management practices; and,**
- **the potential long-term impact of those practices on data subjects.**

These factors will be revisited in the "**TAKE HOME MESSAGES**" following the Qs & As below.

Q1. What is the new federal Act about?

The *Personal Information Protection and Electronic Documents Act* (the "PIPED Act") consists of several Parts (see Appendix A). Of particular relevance for health researchers is Part 1 of the Act.

The purpose of Part 1 is to establish rules for the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need for organizations to access personal information for purposes that a reasonable person would consider appropriate in the circumstances (section 3). What a "*reasonable person would consider appropriate in the circumstances*" is the legal standard against which health researchers will be measured when they purport to access personal information. It is an objective standard as opposed to a subjective one. In other words, it will not be sufficient for a health researcher simply to act on what he or she personally thinks is reasonable. Rather, what a "*reasonable person would consider appropriate in the circumstances*" is an objective assessment of the conduct that will be expected of those who collect, use and disclose personal information under the PIPED Act. Whether that standard will be viewed as a common practice of the trade, a standard of the profession, the perspective of a member of the general public or of a specific community, or the viewpoint of a typical data subject – and at what threshold – remains a question for interpretation by the Commissioner and the courts. What a "*reasonable person considers appropriate in the circumstances*" therefore, is the lens through which the provisions of Part 1 will be read and interpreted.

Q2. What does Part 1 consist of?

Part 1 consists of five Divisions. Part 1 also incorporates Schedule 1 as a part of the Act itself, thereby giving Schedule 1 force of law, with certain modifications (see discussion below). Schedule 1 consists of the ten fair information principles extracted from the Canadian Standards Association's *Model Code for the Protection of Personal Information* CAN/CSA-Q830-96 (the "CSA" Code).

Schedule 1 - The CSA Code

The CSA Code is modeled after the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* developed by the Organization for Economic Cooperation and Development (OECD) in 1980. The CSA Code was originally formulated by Canadian businesses, consumer groups and governments. It was recognized as a national standard in 1996.

The CSA Code enunciates ten fair information principles. In essence, these are:

Principle 1 - Accountability: An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following (fair information) principles.

Principle 2 - Identifying Purposes: The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

Principle 3 - Consent: The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information except where inappropriate.

Principle 4 - Limiting 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.

Principle 5 - Limiting 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 fulfilment of those purposes.

Principle 6 - 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.

Principle 7 - Safeguards: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

Principle 8 - Openness: An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

Principle 9 - Individual 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.

Principle 10 - Challenging 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.

The CSA Code further elaborates on each one of these fair information principles through a series of clauses. Although the Act incorporates these clauses into law, subject to certain modifications, it does not incorporate the explanatory notes of the CSA Code which accompany those clauses. In particular, the Act does not incorporate the explanatory notes accompanying clauses 4.3 and 4.9 of the CSA Code.

Division I - Protection of Personal Information

Division 1 requires every organization, as defined by the Act (see Q6 below), to comply with the fair information principles set out in Schedule 1, subject to certain limitations, modifications or additions. Namely, Division 1 dictates that the Schedule be read and interpreted according to the Act's basic precept that an organization may collect, use or disclose personal information *only for purposes that a reasonable person would consider appropriate in the circumstances*. Also, Division 1 qualifies the fundamental consent principle of Schedule 1 by allowing organizations to collect, use and/or disclose personal information without knowledge or consent of the individual, in some exceptional cases, for certain limited purposes and under certain conditions (see sections 7(1), 7(2) and 7(3)). In particular, there are exceptions allowing the use and/or disclosure of personal information for "statistical, or scholarly study or research, purposes" without knowledge or consent under certain conditions (see Q11 and Q12 below). Further, Division 1 departs from the content of Schedule 1 by expressly providing that wherever Schedule 1 uses the word "should", it indicates a recommendation only and does not impose a mandatory obligation.

Division 2 - Remedies

Division 2 affords individuals the possibility of filing, with the Commissioner, a written complaint against an organization for contravening a provision of Division 1 or for not following a recommendation of Schedule 1. The Commissioner may likewise initiate a complaint against such an organization.

The Commissioner shall, in accordance with the powers given under Division 2, investigate the complaint. The Commissioner's investigative powers include the power to summon the appearance of persons and compel them to give evidence on oath and produce necessary records, administer oaths and enter any premises occupied by an organization at any reasonable time. The Commissioner may attempt to resolve complaints by way of alternative dispute resolution mechanisms such as mediation and conciliation. Where the Commissioner is satisfied that circumstances so require, the Commissioner prepares a report of findings. The complainant and/or the Commissioner may then apply to the Federal Court for a hearing in respect of certain specific matters. The Federal Court may order the organization to correct its practices and publish a notice to that effect. In addition, the Federal Court may award damages to the complainant, including damages for any humiliation suffered.

Division 3 - Audits

Division 3 allows the Commissioner to audit the personal information management practices of an organization if the Commissioner has reasonable grounds to believe that the organization has contravened a provision of Division 1 or is not following a recommendation of Schedule 1. In so doing, the Commissioner may invoke all of the Commissioner's investigation powers under the Act. The Commissioner then provides a report of findings and recommendations to the audited organization. This report may be included in the Commissioner's annual report to Parliament.

Division 4 - General

Division 4 contains a series of general provisions. Among these are:

- the Commissioner shall not disclose any information that comes to the knowledge of the Commissioner while performing powers or duties under the Act, such as conducting audits and/or investigations;
- the Commissioner may, however, disclose information relating to the personal information management practices of an organization if:
  - the Commissioner considers it in the public interest to do so;
  - the Commissioner considers it necessary to conduct an investigation or an audit or,
  - the disclosure is made during the prosecution of an offence or a hearing before the Court;
- the Commissioner is vested with an educational, research and support function to promote the purposes of Part 1 of the Act;
- regulations may be made in respect of certain specific matters under the Act;
- organizations or activities may be exempted from Part 1 of the Act if they are otherwise covered by provincial legislation which is substantially similar to Part 1;
- whistle blowers are afforded special protection under the Act;
- i) every organization who knowingly destroys information that is the subject of a request; ii) every employer who dismisses, suspends, demotes, disciplines, harasses, or otherwise disadvantages a whistle-blower; or iii) every person who obstructs the Commissioner's investigation, is guilty of an offence and liable to a fine of up to $100,000;
- Part 1 shall be reviewed by parliamentary committee every five years after its coming into force on January 1, 2001.

Division 5 - Transitional Provisions

This last division contains provisions which set out several different phases for the application and coming into force of Part 1. (See Q8 below.)

Q3. How is "personal information" defined in the PIPED Act?

Under Part 1 of the Act, "**personal information**" is defined simply as "information about an identifiable individual, excluding the name, title or business address or telephone number of an employee of an organization".

Note, the term "identifiable" is not defined any further in the PIPED Act. Identifiability of personal information is not a black and white concept, but rather, a matter of degree. Where the PIPED Act situates itself on this spectrum of identifiability is not specified in the legislation. However, varying definitions of identifiability provided in some provincial legislation, though limited, might serve to guide the Commissioner's and the courts' interpretation of this term.

See, for example the definitions of "individually identifying" and "non-identifying" information in Alberta's *Health Information Act* (3rd Sess., 24th Leg., Alberta, 1999 - Royal Assent 9 December 1999 - not yet proclaimed in force):

> "*Individually identifying, when used to describe health information, means that the identity of the individual who is the subject of the information can be readily ascertained from the information*;"

> "*Non-identifying, when used to describe health information, means that the identity of the individual who is the subject of the information cannot be readily ascertained from the information*;"

Also of interest is the definition of "de-identified personal health information" in Saskatchewan's *Health Information Protection Act* (S.S. 1999, c. H-0.021 - Royal Assent, 6 May 1999 - not yet proclaimed in force):

> *"De-identified personal health information means personal health information from which any information that may reasonably be expected to identify an individual has been removed."*

Most recently, Ontario's Bill 159, *Personal Health Information Privacy Act, 2000*, (1st Sess., 37th Leg., Ontario, 2000 – since died on the order paper) in its definition of personal health information, refers to information that,

> *"i) identifies the individual,*
> *ii) can be used or manipulated by a reasonably foreseeable method to identify the individual or,*
> *iii) can be linked or matched by a reasonably foreseeable method to other information that identifies the individual or that can be used or manipulated by a reasonably foreseeable method to identify the individual..."*

Q4. How is "personal health information" defined in the PIPED Act?

"Personal health information" is defined as:

a) information concerning the physical or mental health of the individual;

b) information concerning any health service provided to the individual;

c) information concerning the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual;

d) information that is collected in the course of providing health services to the individual; or

e) information that is collected incidentally to the provision of health services to the individual.

Q5. To whom will Part 1 of the PIPED Act apply?

The provisions of Part 1 will eventually apply to every organization (see further discussion on the meaning of "organization" in Q6 below) that collects, uses or discloses:

- personal information, when done in the course of commercial activities (see further discussion on the meaning of "commercial activities" in Q7 below), or
- employee information, when done in connection with the operation of a federal business (such as, banking, telecommunications, radio broadcasting, interprovincial railways, ships, airlines etc.).

Part 1 does **not** apply to:

- federal government departments or agencies to which the federal *Privacy Act* (R.S.C. c. P-21) applies (see the government institutions listed in Appendix C);
- any individual who collects, uses or discloses personal information for purely personal or domestic purposes; or
- any organization that collects, uses or discloses personal information solely for journalistic, artistic or literary purposes.

Part 1 is not binding on:

- provincial government departments or provincial agencies of her Majesty.

Q6. What constitutes an "organization" within the meaning of the Act?

An "**organization**" is defined very broadly in the PIPED Act as "an association, partnership, person and trade union".

Note, the organization is the relevant unit of compliance for the purposes of Part 1 of the PIPED Act. However, it is the commercial nature of the organization's activities that will trigger the application of the Act (see Q7 below). Each purported collection, use or disclosure of personal information by an organization may lead to different results depending on the particular transaction and the parties to the transaction. Following are various possible permutations:

Example 1: Suppose the activities of organization "A" are commercial in nature and covered by the Act. Suppose the activities of organization "B" are also commercial and covered by the Act. If organization A discloses personal information to organization B, organization A will be subject to the disclosure provisions of the Act, whereas organization B will be subject to the collection provisions.

Example 2: Suppose the activities of organization "A" are commercial and covered by the Act. Suppose the activities of organization "B" are not commercial and therefore not covered by the Act. If organization A discloses personal information to organization B, organization A will be subject to the disclosure provisions of the Act, whereas organization B will not be subject to the Act at all.

Example 3: Suppose the activities of organization "A" are not commercial and therefore not covered by the Act. Suppose the activities of organization "B" are commercial and covered by the Act. If organization A discloses personal information to organization B, organization A will not be subject to the Act at all, whereas organization B will be subject to the collection provisions of the Act.

Example 4: Finally, suppose the activities of organization "A" are not commercial and therefore not covered by the Act. Suppose the activities of organization "B" are not commercial and also not covered by the Act. If organization A discloses personal information to organization B, organization A is not subject to the Act at all, and neither is organization B.

Q7. What constitutes "commercial activity" within the meaning of the Act?

"**Commercial activity**" means "any particular 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 fund-raising lists".

Note, commercial activity and non-commercial activity are not necessarily synonymous with private sector and public sector respectively. It is the nature of the activity, rather than the nature of the organization that seems to prevail as the determining criterion. Therefore, whether research activity is carried out with or without a profit motive, whether it is funded by a private or public source of funding, or whether it is conducted for private or public benefit, are factors which, among others, might be weighed by the Commissioner and the courts on a case-by-case basis.

There are some important activities in the health sector, the nature of which cannot yet be clearly determined one way or another. For example, whether the services of a health professional carried out in a private clinic reimbursed by the public purse will be considered "commercial activity" within the meaning of the PIPED Act is not yet known. Whether the activities of private, not-for-profit organizations and/or cost-recovery activities constitute "commercial activity" is likewise impossible to ascertain at this stage and will likely be circumscribed over time through judicial interpretation.

Furthermore, the activities of health researchers themselves will be difficult to categorize as either commercial or non-commercial in nature. Increasingly, academia, private sector, voluntary charitable organizations and government are joining forces to engage in innovative research partnerships and to transform this new knowledge into forms which are beneficial to the population. In an era where such partnerships are actively encouraged, a whole spectrum of public-private arrangements have begun to emerge. More and more often, university researchers receive salary support and/or funding from various sponsors. In some cases, the support is provided to conduct research that may directly or indirectly enhance the competitiveness of Canadian businesses; in other cases, it is provided to support peer-reviewed, academic research to advance general knowledge about the health and/or health system of Canadians; more commonly, support is intended to sustain both these objectives.

Example 1: Recently, CIHR, McMaster University and three research based pharmaceutical companies (King Pharmaceuticals, SmithKline Beecham and Aventis Pharma Inc) joined forces for a $25 million dollar, five-and-a-half year clinical trial of two drugs to determine their effectiveness at preventing type 2 diabetes. The application for this project received the highest peer-reviewed ranking of any new

CIHR (and before it, Medical Research Council) clinical trial application in over ten years. It is called the DREAM study (**D**iabetes **RE**duction **A**pproaches with ramipril and rosiglitazone **M**edications). The study involves researchers from McMaster University, Centre hospitalier universitaire de l'Université de Montréal, Université de Laval, Heritage Medical Research Centre (Edmonton) and the University of Toronto/Mount Sinai Hospital. Type 2 diabetes afflicts 142 million people world wide and treatment costs $7-10 billion annually in Canada. If successful, this trial could greatly reduce the number of new cases of type 2 diabetes, thus lowering the treatment costs.

Example 2: CIHR, together with the National Cancer Institute of Canada (NCIC), Health Canada, the Canadian Cancer Society, Avon Canada (originally through the Breast Cancer International Centre and now through Avon Flame Foundation), the Canadian Breast Cancer Network and the Canadian Breast Cancer Foundation are funding partners in the Canadian Breast Cancer Research Initiative (CBCRI).

> *With major financial commitments from the partners and support from the private sector, CBCRI is the primary funder of breast cancer research in Canada... During its first seven years, CBCRI allocated $61.8 million to 217 different breast cancer research projects across the entire spectrum of breast cancer research, including prevention, early detection, treatment, fundamental laboratory investigations, quality of life and health services... Avon Canada... contributed $3.7 million during the first five years through the sales of pins, key chains and pens, [and has committed] another $5 million over the next five years... The Royal Bank contributed $1 million, in addition to spearheading a campaign to raise funds for breast cancer research from the corporate sector.*[1]

Example 3: A further example of multi-partner, multi-sector, cross-regional research initiatives with varying objectives are the Network Centers of Excellence (NCE).

> *The NCE program has been operating successfully for ten years and was made permanent by the federal government in 1997, with an annual budget of $47.4 million. On February 16, 1999, the federal government announced that the NCE Program budget would be increased by $90 million over the next three years starting in 1999-2000. NCEs are unique partnerships among industry, universities and government designed to develop the economy and improve quality of life. These nation-wide networks connect excellent research with industrial know-how and practical investment. In 1999-2000, a total of 563 companies, 138 provincial and federal government departments and agencies, 46 hospitals, 98 universities, and more than 266 other organizations from Canada and abroad were involved in the NCE program. The active involvement of Canadian industry provides stimulating training environments and employment opportunities for students. In fact, about 90 per cent of network graduates are successful at finding jobs. In 1999-2000, the networks stimulated outside investments of over $70 million, including more than $41 million by the participating private sector companies.*[2]

[1] Breast Cancer Research Initiative website, www.breast.cancer.ca/english/cbcri/intro_ec.htm.

[2] Network Centers of Excellence website, www.nce.gc.ca/en/abouteng.htm.

All three of the above examples illustrate the complexity of applying the commercial/non-commercial distinction to the activities of health researchers today.

Finally, it is important to note that, in order for a particular transaction to constitute a "commercial activity" within the meaning of the Act, the collection, use or disclosure of personal information must have occurred in the course of commercial activity. Yet, the degree of connection between the collection, use or disclosure of personal information, on the one hand, and the commercial activity, on the other, is uncertain.

Consider for example, if you are an academic health researcher seeking to purchase data from a third party in order to carry out your study for scholarly purposes, are you acting in the course of commercial activity? What if the data was secured on a cost-recovery basis? While your research activity is of a non-commercial nature, the transaction through which you purport to collect personal information may be of a commercial nature. Whether that, by itself, is sufficient to bring you within the purview of the Act will be a question of interpretation by the Commissioner and the courts.

Q8. Will I be subject to Part 1 of the Act, and if so, when?

Part 1 of the Act will take effect in three different stages:

As of January 1, 2001, Part 1 applies to:

- an organization that collects, uses or discloses personal information (*other than personal health information*) in connection with the operation of a federal business (such as, banking, telecommunications, radio broadcasting, interprovincial railways, ships, airlines etc.). This includes personal information about the employees of such organizations.

- an organization that discloses personal information (*other than personal health information*) *outside provincial borders* for "consideration", ie., some economic or other benefit (eg. any organization that sells, trades or leases personal information across provincial or national borders in return for money or some other form of gain).

As of January 1, 2002, Part 1 will apply:

- in the same circumstances as above, *but now include personal health information*.

As of January 1, 2004, Part 1 will apply to:

- any organization that collects, uses or discloses personal information, including personal health information, in the course of commercial activity, *whether outside provincial borders or entirely within provincial borders*.

Where the collection, use or disclosure is carried out entirely within a province, the organization and/or its activities may be exempted from the application of Part 1 in January 2004, if the organization and/or its activities are otherwise subject to a provincial law which is deemed to be substantially similar to Part 1 of the Act. Therefore, in order to gain such an exemption for organizations and/or activities within their jurisdictions, provinces effectively have three more years to develop substantially similar legislation. Substantially similar legislation may include sector-specific legislation such as health information protection legislation.

When the PIPED Act was being considered by the Senate Standing Committee on Industry, Science and Technology on December 2, 1999, the then Minister of Industry (John Manley) described substantially similar legislation as "...legislation that provides a basic set of fair information practices which are consistent with the CSA Standard, oversight by an independent body and redress for those who are aggrieved". At that time, only Quebec had provincial legislation in place that the Minister would have considered "substantially similar". (See relevant excerpts of Quebec's *Act respecting the Protection of Personal Information in the Private Sector*, R.S.Q. c. P-39.1, in the Compendium).

Note, however, even if an exempted organization in one province were to transfer personal information to another exempted organization in another province, the PIPED Act is still intended to apply to that inter-provincial transfer of information.

Q9. What does collection, use and disclosure mean under the PIPED Act?

The PIPED Act does not define the terms "collection", "use" or "disclosure" and neither does Schedule 1 of the Act. However, the fuller *CSA Model Code for the Protection of Personal Information*, of which Schedule 1 contains only an excerpt, does define these terms as follows:

collection - *"the act of gathering, acquiring, or obtaining personal information from any source, including third parties, by any means".*

use - *"refers to the treatment and handling of personal information within an organization".*

disclosure - *"making personal information available to others outside the organization".*

Although these definitions are not in the PIPED Act itself, nor in the Schedule to the Act, they do help inform the excerpt of the CSA Code which is incorporated into the Act and therefore, may guide the interpretation of the Commissioner and the courts.

Example: The activities of Organization "A" are covered by the Act. Organization A communicates personal information to a health researcher who is employed by organization A, acting in that capacity and in the interests of the organization. In this case, organization A does not technically "disclose" personal information to any third party outside the organization. That specific communication would not, therefore, trigger the "disclosure" provisions of the Act. However, that same communication may nonetheless trigger the "use" provisions of Part 1 if the health researcher purported to use the personal information within the organization for a purpose different from that for which it was originally collected.

Q10. If I collect, use and disclose personal (health) information, do I need to obtain consent?

If the information you collect, use and/or disclose in the course of your research is not *identifiable* (see discussion about the complexity of this term in Q3 above), your research activity would not be subject to the PIPED Act and therefore, you would not be required to obtain consent under this Act, *whether or not you are engaged in commercial activity*.

If, however, you wish to collect, use or disclose personal (health) information that is *identifiable,* in a situation which *is* covered by the PIPED Act, then, according to Principle 3 in the CSA Code (Schedule 1 of the Act), you are, as a general rule, required to inform the individual about it and seek his or her consent. In more specific terms:

"*4.3 Principle 3 - Consent*

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

"*4.3.1 Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, an organization will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when an organization wants to use information for a purpose not previously identified).*"

"*4.3.2 The principle requires "knowledge and consent". Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner*

that the individual can reasonably understand how the information will be used or disclosed."

"4.3.3 An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes."

Q11. Where consent is required under the Act, what form must it take?

There are various interpretations of the PIPED Act which, in each case, yield a different answer to this question. Two possible interpretations follow:

A ***liberal*** reading of sections 4.3.5 and 4.3.7 of the CSA Code (Schedule 1) would seem to suggest that consent need not always be in writing, but may, in certain circumstances be given orally, or may even be implied depending on the context. On this interpretation, the form of consent and the method for obtaining it would appear to be quite flexible.

"4.3.5 In obtaining consent, the reasonable expectations of the individual are also relevant. For example, an individual buying a subscription to a magazine should reasonably expect that the organization, in addition to using the individual's name and address for mailing and billing purposes, would also contact the person to solicit the renewal of the subscription. In this case, the organization can assume that the individual's request constitutes consent for specific purposes. On the other hand, an individual would not reasonably expect that personal information given to a health-care professional would be given to a company selling health-care products, unless consent were obtained. Consent shall not be obtained through deception."

"4.3.7 Individuals can give consent in many ways. For example:
(a) an application form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses;
(b) a checkoff box may be used to allow individuals to request that their names and addresses not be given to other organizations. Individuals who do not check the box are assumed to consent to the transfer of this information to third parties;
(c) consent may be given orally when information is collected over the telephone; or
(d) consent may be given at the time that individuals use a product or service."

Yet, a ***strict*** reading of sections 4.3.4 and 4.3.6 of the CSA Code (Schedule 1), combined, would not appear to be as flexible. On this second interpretation, express (written) consent should generally be sought when the personal information is considered sensitive and medical records are but one example of information which is almost always considered to be sensitive.

> "4.3.4 *The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context*."

> "4.3.6 *The way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive*."

Industry Canada, as original drafter of the PIPED Act, has consistently taken the position publicly that the "liberal" interpretation is a viable one. However, whether or not express written consent will be required on a case-by-case basis is ultimately a matter for interpretation by the Commissioner and the courts. Greater certainty may be achieved through such interpretation over time.

Q12. Who may provide substitute consent under the PIPED Act?

The PIPED Act, as currently formulated, is completely silent on the question of substitute consent, most likely because substitute consent was seen by the drafters as a matter of civil rights falling within provincial jurisdiction. It is likely that the laws of the province in which the data subject is domiciled will be referred to by the Commissioner and the courts when determining the decision-maker who can legally consent to the collection, use or disclosure of personal information on the subject's behalf.

Q13. Are there any circumstances in which I may use and/or disclose personal (health) information for research purposes under the Act without the knowledge or consent of the individual or his/her substitute decision-maker?

Yes. According to section 7(2)(c), health researchers, whose activities are or eventually become subject to Part 1 of the Act, may, without the knowledge or consent of the individual, **use** personal information for statistical, or scholarly study or research, purposes if:

- the purpose cannot be achieved without using the information;
- the information is used in a manner that will ensure its confidentiality;
- it is impracticable to obtain consent; and,
- the organization informs the Commissioner of the use before the information is used.

Similarly, section 7(3)(f) provides that health researchers, whose activities are or eventually become subject to Part 1 of the Act, may, without the knowledge or consent of the individual, **disclose** personal information for statistical, or scholarly study or research, purposes if:

- the purpose cannot be achieved without disclosing the information;
- it is impracticable to obtain consent; and,
- the organization informs the Commissioner of the disclosure before the information is disclosed.

For further details on the process for informing the Federal Privacy Commissioner, see the contact information included at the end of this document. With the exception of informing the Federal Privacy Commissioner, the other criteria in both sections 7(2)(c) and 7(3)(f) are a matter for factual determination on a case-by-case basis.

Q14. Are there any circumstances in which I may collect personal (health) information for research purposes under the Act without the knowledge or consent of the individual or his/her substitute decision-maker?

The Act does not, under any conditions, exempt the collection of personal (health) information for "statistical, or scholarly study or research, purposes" from the consent rule. Therefore, to the extent an organization's activities fall within the ambit of the Act, the organization cannot – even for research purposes – prospectively collect any new personal (health) information, nor collect any personal (health) information originally collected by another organization for a different primary purpose, *without* the knowledge and consent of the individuals involved.

If, however, the organization seeking to collect personal (health) information for research purposes is not subject to the Act (i.e., it does not do so in the course of commercial activity, nor does it collect employee information in connection with a federal work), there is no requirement to obtain consent (though there may be a similar requirement to do so under other legislation).

The exemption allowing the disclosure of personal (health) information for "statistical, or scholarly study or research, purposes" under certain conditions in section 7(3)(f) (see Q13 above), serves only to exempt the data holder from the requirement to obtain consent before disclosing the information to a third party outside the organization for such purposes. It does not serve to exempt the collector of that information from having to obtain consent on the receiving end, if the collector is also subject to the Act. Unlike other data protection legislation, the PIPED Act does not contain a general correlative provision allowing for the collection of personal information without consent, for the same purposes and under the same conditions as disclosure is permitted without consent under the Act.

Example 1: Suppose a data management company, normally engaged in commercial activity, were seeking to disclose personal (health) information to a health researcher for scholarly study or research purposes. Under those circumstances, it would seem that the data management company would be exempted from having to obtain consent before disclosing the personal (health) information under the specific conditions of section 7(3)(f). If the academic health researcher was in no way engaged in commercial activity (eg., was employed by a public institution, was funded only with public monies, had no private sector partners, had no profit motive, was not purchasing the data for money, etc...), the researcher would, in all likelihood, not be

subject to the PIPED Act, and therefore, could collect the personal (health) information from the data management company without having to obtain consent (unless required to do so under some other legislation).

Example 2: Suppose the same data management company were to disclose personal (health) information, this time to a pharmaceutical company for marketing purposes. It would seem that the data management company would not be disclosing for "statistical, scholarly study or research purposes" in this case, and therefore, could not benefit from the exemption under section 7(3)(f). Therefore, the data management company would have to obtain prior consent of the data subjects to disclose their personal (health) information to the pharmaceutical company for marketing purposes. For its part, the pharmaceutical company collecting the information would be engaged in commercial activity, and therefore, it too would have to obtain consent before collecting the personal (health) information. Will the PIPED Act be interpreted in a sufficiently flexible manner so that the consent originally obtained by the primary collector (in this example, the data management company) could carry forward and constitute valid consent also for the secondary collector (in this case, the pharmaceutical company)? If the primary collector sought consent from the data subjects to collect personal information specifically for the reason of disclosing it to the secondary collector for marketing purposes, it seems reasonable that the secondary collector could then receive the data from the primary collector, without itself having to also obtain consent directly from each data subject. If this interpretation were upheld, it could simplify matters for the secondary collector since the secondary collector could stipulate, as a condition in its agreement with the primary collector, that the primary collector obtain the necessary consent on its behalf. How these relevant provisions of the PIPED Act will actually be interpreted by the Commissioner and the courts remains to be seen.

Example 3: Suppose the same data management company were to disclose personal (health) information to an academic health researcher for scholarly study or research purposes. The research will be peer-reviewed and the intention of the researcher is to publish the research results in an academic or scholarly journal to advance the general state of knowledge about a certain illness or disease. The academic health researcher who is conducting scholarly study or research is partly funded by a federal research agency and partly funded by a pharmaceutical company. The researcher receives a finder's fee for each research subject he or she recruits in the research protocol and has committed to provide a report of the research findings to the pharmaceutical company for a certain minimum period in advance of publication. If, in the eyes of the Commissioner or a judge, the data management company here were seen to be disclosing personal (health) information for scholarly study or research purposes, it would benefit from the disclosure exemption and therefore, could proceed to disclose the information without consent under the conditions of section 7(3)(f). However, if, also in the eyes of the same Commissioner or judge, the academic health researcher's

activity here were sufficiently colored by commercial elements to constitute commercial activity, the researcher would be subject to the PIPED Act. Because there is no exemption for collecting personal (health) information for scholarly study or research purposes without consent under the PIPED Act, the health researcher would necessarily have to obtain consent before collecting the personal (health) information from the data management company.

On one interpretation of the PIPED Act, the above paradox could never occur. This is because scholarly study or research purposes, on the one hand, and commercial activity, on the other, are seen as mutually exclusive. In this view, it is implied that if Organization A were disclosing personal (health) information to Organization B for scholarly study or research purposes, Organization B could not, precisely because it were conducting scholarly study or research, ever be seen to be collecting it in the course of commercial activity.

However, on a different interpretation of the PIPED Act, these terms are not mutually exclusive. In this view, the current wording of the Act could sustain a situation where disclosure of personal (health) information might be for scholarly study or research purposes, yet collection of that information by an academic health researcher might, because of various elements, be considered sufficiently commercial in nature. Viewed from this perspective, the PIPED Act would apply and the researcher would be required to obtain consent before collecting the personal information. Where uncertain about whether or not their activities might be considered commercial, health researchers should make all reasonable efforts to obtain consent before collecting the personal information.

Q15. What type of regulations does the Act allow for?

Subsection 26(1) of the Act provides that the Governor in Council may make regulations for, among other things:

- determining what constitutes an investigative body for the purposes of Part 1,
- determining what constitutes publicly available information that may be collected, used and/or disclosed without knowledge or consent under Part 1 of the Act, and more generally,
- carrying out the purposes and provisions of Part 1.

In January 2001, three new regulations came into effect defining "publicly available information", defining "investigative bodies", and binding certain agents of Her Majesty to the Act (see Appendix B). Of particular interest for health researchers is the definition of "publicly available information":

A: the name address and telephone number of a subscriber appearing in a publicly available directory, where the subscriber can refuse to have such information appear;

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

C: personal information appearing in a registry collected under a statutory authority, to which public access is authorized by law, where the collection, use and disclosure of the personal information relate directly to the purpose for which the information appears in the registry;

D: personal information appearing in a record or document of a judicial or quasi-judicial body which is publicly available, where the collection, use and disclosure of the personal information relate directly to the purpose for which the information appears in the record or document; and,

E: personal information appearing in a publication, including a magazine, book or newspaper, in printed or electronic form, which is publicly available, where the individual concerned has him or herself provided the information.

Note that, in paragraphs B, C and D above, the regulations require, as an additional criterion, that the purported collection, use or disclosure has to relate directly to the specific, primary purpose for which the information was made publicly available in the first place.

Q16. How long may I retain the data according to the PIPED Act and under what circumstances?

Principle 5 of Schedule 1 *requires* that personal information be retained only as long as necessary for the fulfilment of the purposes for which the personal information was collected, except with the consent of the individual or as required by law. Moreover, Schedule 1 *recommends* that organizations develop guidelines and implement procedures regarding the retention of personal information and that these guidelines include minimum and maximum retention periods.

Schedule 1 also *requires* that personal information used to make a decision about an individual be retained long enough to allow the individual access to the information after the decision has been made. (Note, other legislative requirements setting out retention periods may apply.)

Schedule 1 further *recommends* that personal information no longer required to fulfil the identified purposes be destroyed, erased, or made anonymous. Schedule 1 *requires* organizations to develop guidelines and implement procedures governing the destruction of personal information.

Part 1 of the Act in no way modifies the above requirements and/or recommendations on retention and destruction. Therefore, these provisions, whether mandatory or optional, would apply as are.

Q17. What happens if I am covered by the PIPED Act, but do not comply with its requirements and/or recommendations?

While the Act contains both mandatory requirements and recommendations, a complaint may be initiated in both cases. Where a complaint is filed with the Commissioner or is initiated by the Commissioner, the provisions in Division 2 will apply and the Commissioner will proceed to investigate the complaint in accordance with the powers conferred under the Act. (See Q2 above).

Furthermore, if the Commissioner has reasonable grounds to believe that an organization is contravening a mandatory requirement or is not following a recommendation, the Commissioner may conduct an audit on the personal information management practices of the organization. In such an event, the provisions in Division 3 will apply. (See Q2 above).

Take home messages:

In light of the above Qs & As, researchers may wish to consider the following:

1. Think about the purpose of your research and try to articulate it for yourselves and for the benefit of others. What data will you need to fulfill that purpose? Is every data element essential for your research? Are the data you are seeking to access really necessary or are they superfluous? Can you justify your data needs?

2. Think about the nature and the form of the data you are proposing to collect and use. What is the degree of identifiability of the data? If you are proposing to use only anonymous data, how anonymous is it? Can the information be matched to make it readily identifiable?

3. Think about any commercial aspects of your research. Who is your employer? Who is funding you? Who are your research partners? What is your motive in conducting the research? What and whom are you committed to? What is the potential for economic gain or profit? Who are your data sources? Are you purchasing the data from them?

4. Think about any connection to the operation of a federal work, business or undertaking. Are you employed by a federal work, business or undertaking? Are you purporting to use information about employees of a federal work, business or undertaking?

5. Think about the geographic scope of your research. Where will your research be conducted? Entirely within provincial borders? Or will your study extend beyond provincial or even national borders? If your research activity involves disclosure of personal information outside provincial or national borders, will it be in return for some economic or other benefit? What other data protection or privacy or confidentiality laws might apply in the jurisdiction(s) in which your research activity is being carried out?

6. Think about the general requirement for consent. Have you obtained consent? If so, was it given freely and properly informed? Was the data subject, or his/her substitute decision-maker, legally capable of consenting? In what form did you obtain consent? If you did not obtain consent, why not? If you say that consent is impracticable to obtain, can you justify your position beyond demonstrating mere inconvenience? Have you met all the other conditions under the PIPED Act or other legislation exempting you from the consent requirement?

7. Think about your general data management practices. Have you made any attempt to strengthen those practices in accordance with the spirit of the CSA principles in Schedule 1 of the PIPED Act? Are you considering both the mandatory requirements, as well as the recommendations made in Schedule 1, which may or may not be the subject of an audit or complaint?

8. Think about the need for openness and transparency even if your research activity is not strictly caught by the mandatory provisions or the recommendations of the PIPED Act. If exposed, what might be the long-term impact of your information practices on the trust and confidence of data subjects and the public in general?

USEFUL CONTACT INFORMATION:

Canadian Institute for Health Information (CIHI)
377 Dalhousie Street, Suite 200
Ottawa ON
K1N 9N8
Telephone: 1-613-241-7860 x 4155
Fax: 1-613-241-8120
Web site: www.cihi.ca
E-mail: communications@cihi.ca

Canadian Institutes of Health Research (CIHR)
410 Laurier Avenue West
9th Floor, Address Locator 4209A
Ottawa ON
K1A 0W9
Telephone: 1-613-941-2672
Fax: 1-613-954-1800
Web site: www.cihr.ca
E-mail: info@cihr.ca

Industry Canada
Electronic Commerce Branch
300 Slater Street
Ottawa, ON
K1A 0C8
Telephone: 1-613-991-4029
Fax: 1-613-941-1164
Web site: www.e-com.ic.gc.ca

Office of Health and the Information Highway - Health Canada
Information Analysis & Connectivity Branch
Jeanne Mance Building, Tunney's Pasture,
4th floor
Postal Locator 1904D1
Ottawa ON
K1A 0K9
Fax: 1-(613)-952-3226
Web site: www.hc-sc.gc.ca/ohih-bsi
e-mail: ohih-bsi@www.hc-sc.gc.ca

Privacy Commissioner of Canada
112 Kent Street
Ottawa ON
K1N 1H3
Telephone: 1-(613)-995-8210
Toll-Free: 1-800-282-1376
Fax: 1-(613)-947-6850
Web site: www.privcom.gc.ca
E-mail: info@ privcom.gc.ca

USEFUL LINKS:

Canadian Institutes of Health Research (CIHR), *A Compendium of Canadian Legislation Respecting the Protection of Personal Information in Health Research, 2000*
http://www.cihr.ca/about_cihr/ethics/compendium_e.pdf

Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada, Social Sciences and Humanities Research Council of Canada, *Tri-Council Policy Statement Ethical Conduct for Research Involving Humans, 1998*
http://www.nserc.ca/programs/ethics/english/ethics-e.pdf

Canadian Institutes of Health Information (CIHI), *Privacy and Confidentiality Guidelines on Health Information at CIHI: Principles and Policies for the Protection of Health Information*,
http://www.cihi.ca/weare/pcsmain.shtml

Office of Health and the Information Highway - Health Canada, *Canada's Health Infoway: Paths to Better Health, 1999*
http://www.hc-sc.gc.ca/ohih-bsi/whatdo/achis/fin-rpt/fin-rpt_e.pdf

Office of the Privacy Commissioner of Canada, *Backgrounder on the PIPED Act*:
http://www.privcom.gc.ca/english/02_06_07_e.htm

Office of the Privacy Commissioner of Canada, *A Guide for Businesses and Organizations: Your Privacy Responsibilities*
http://www.privcom.gc.ca/english/02_06_06_e.pdf

Canadian Standards Association (CSA), *Model Code for the Protection of Personal Privacy, 1996*
http://www.csa.ca/english/product_services/ps_privacy.html_

Canadian Medical Association (CMA), *CMA Health Information Privacy Code, 1998*
http://www.cma.ca/inside/policybase/1998/09-16.htm

Industry Canada, Electronic Commerce Branch, Privacy pages
http://www.strategis.ic.gc.ca/privacy