PRIVACY RESPONSIBILITIES

KAREN WESLOWSKI
MILLER THOMSON LLP
VANCOUVER, BRITISH COLUMBIA
MAY 12, 2003

I. INTRODUCTION

Information disclosed by individuals in the course of obtaining healthcare or information generated as a result of that process is confidential, personal and sensitive information and ought to be treated as such. However, an individual's personal health information may be of great value to pharmaceutical companies seeking to develop and market drugs, governments seeking to develop health programs or insurance companies seeking to set premiums, to name a few. Businesses, governments or other organizations may be interested in personal healthcare information generated within the Aboriginal community for a variety of reasons. For instance, such information may reveal inappropriate usage or abuse of prescription of drugs, a topic of interest in the Aboriginal community, and the healthcare community generally.

Individuals and organizations involved in the management of healthcare in Aboriginal communities may have legal obligations with respect to the collection, use and disclosure of personal information. This paper will:

- Provide a summary of federal and provincial protection of privacy and access to information legislation, which governs the collection, management, use and disclosure of personal information;

- Discuss particular privacy issues that may arise with respect to the collection, use and disclosure of personal health information for those individuals or organizations involved in the management of healthcare in aboriginal communities;

- Discuss ways of fulfilling legal obligations pertaining to the protection of privacy and access to personal information; and

- Provide an overview of consent to the disclosure of personal information.

II. OVERVIEW OF PROTECTION OF PRIVACY & ACCESS TO INFORMATION LEGISLATION

A. Public Sector Privacy Legislation

At the federal level, the *Privacy Act,* R.S. 1985, c. P- 21 and the *Access to Information Act,* R.S. 1985, c. A-1 regulate the collection, use and disclosure of personal information held by federal government institutions and provide individuals the right to access and correct personal

information held by those institutions. At the provincial level, all provinces have enacted legislation similar to the *Privacy Act* and the *Access to Information Act*, which regulate the collection, use and disclosure of personal information by provincial government institutions[1]. In British Columbia, the *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c. 165 has been in place since 1993. Notably, however, none of this legislation applies to regulate the collection, use and disclosure of personal information in the private sector.

B. Private Sector Privacy Legislation

The need for legislation to protect personal information in the private sector has become more significant with the emergence of e-commerce and electronic data keeping practices[2]. As well, developments in information technology and management are changing the manner in which hospitals and physicians are collecting, storing, accessing and sharing personal health information, with electronic record systems gradually replacing traditional paper record systems[3]. These changes are significant as, before computers, when records were kept in paper form, much effort was generally required to access, retrieve and compile one's personal information. With electronic records becoming the norm, barriers to access information are diminishing, and the risk of invasion of privacy due to the mismanagement and misuse of personal information is increasing.

In 2000, the federal government, recognizing the need to protect personal information in the private sector, enacted the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 ("PIPEDA"). PIPEDA seeks to minimize the misuse of personal information by imposing obligations on organizations that gather and use personal information in a commercial context by stipulating, with a few exceptions, that no organization can collect, use or disclose personal information about an individual without that individual's consent. PIPEDA states its purpose as follows:[4]

---

1 Newfoundland has enacted, but not yet proclaimed, the *Access to Information and Protection of Privacy Act*, S.N.L. 2002, c. A-1.1

2 W. Charnetski, P. Flaherty & J. Robinson, *The Personal Information Protection and Electronic Documents Act* (Aurora: Canada Law Book, 2001) at iii

3 D.A. Crolla, M.K. O'Brien & D. Sloan, *the Challenge of Electronic Records: Protecting Privacy in an Increasingly Paperless World* 2002-03 *Telehealth* at 21

4 PIPEDA, s. 3

> The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern 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 of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

PIPEDA is based on ten principles initially developed by the Organization for Economic Cooperation and Development and Incorporated into the Model Code for the Protection of Personal Information developed by the Canadian Standards Association ("CSA"). The CSA Model Code is incorporated into PIPEDA and includes the following requirements:

1. To require organizations collecting, using or disclosing personal information to be accountable for such activity;

2. To ensure that individuals receive an explanation of the purposes underlying any collection, use or disclosure of their personal information;

3. To require organizations to obtain informed consent from individuals prior to the collection, use or disclosure of their personal information;

4. To limit the collection of personal information;

5. To limit the use, disclosure and retention of personal information;

6. To ensure that personal information holdings are accurate;

7. To require organizations to implement appropriate safeguards to protect personal information holdings;

8. To encourage openness regarding the personal information management practices of organizations;

9. To facilitate an individual's access to their personal information; and

10. To establish means by which individuals can challenge an organization's compliance with PIPEDA.

British Columbia has announced its intention to introduce private sector privacy legislation in the spring of 2003. The British Columbia legislation would cover personal information held by all organizations and businesses in the province that are not currently subject to the *Freedom of Information and Protection of Privacy Act*.

Alberta has also indicated that it intends to introduce private sector privacy legislation in the spring of 2003. Ontario announced its intention to table the *Privacy of Personal Information Act* in the Legislative Assembly in late September 2002, however, the bill has yet to be introduced[5]. Quebec has already enacted private sector legislation, the first jurisdiction in Canada to do so. None of the other provinces have enacted comprehensive private sector privacy legislation, or announced any intention to do so, although Saskatchewan, Alberta and Manitoba have passed legislation that applies to personal health information held by provincial government ministries, hospitals, regulated health professions, such as physicians, pharmacists, dentists, registered nurses, laboratories and other healthcare facilities.

C. The *Personal Information Protection and Electronic Documents Act*

Application

The application of PIPEDA is graduated into three stages. As of January 1, 2001, PIPEDA applied only to works, undertakings or businesses in the federally regulated private sector, such as banks, telecommunications companies, airlines, railways and interprovincial trucking companies, as well as to organizations that disclose personal information for consideration outside a provide or the country. As of January 1, 2001, PIPEDA also applied to employee information that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business.

Since January 1, 2002, PIPEDA has applied to personal health information for organizations and activities already covered in the first stage of application.

Commencing January 1, 2004, PIPEDA will apply to every organization that collects, uses or discloses personal information in the course of a commercial activity within a province, whether

---

[5] Given the impending provincial election in Ontario, it is unlikely that any private sector privacy legislation will be introduced before January 1, 2004.

federally or provincially regulated, unless a province enacts substantially similar legislation by that date[6]. As such, each province must have its own private sector privacy legislation in place by January 1, 2004, or it will be covered by PIPEDA. If the British Columbia legislation is in force by January 1, 2004, it will apply to the private sector, rather than PIPEDA. The proposed content of the British Columbia legislation is unknown, however, it is expected that the British Columbia legislation will be substantially similar to PIPEDA or even more stringent with respect to the protection of personal information. It is expected that the British Columbia legislation will apply to organizations not covered by PIPEDA, including unions, non-profit societies, clubs, and professional organizations and, likely, healthcare organizations[7].

PIPEDA sets out its application as follows[8]:

> (1) This Part applies to every organization in respect of personal information that
>
> a) the organization collects, uses or discloses in the course of commercial activities; or
>
> b) is about an employee of the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business

PIPEDA defines "organization" to include "any association, partnership, a person or a trade union"[9]. Corporate entities are included in the definition of "person"[10] and are, accordingly, subject to PIPEDA.

---

6 The Privacy Commissioner of Canada has indicated that in assessing whether provincial legislation is substantially similar, he will interpret substantially similar to mean equal or superior to the Act in the degree and quality of privacy protection provided. The federal law is to be the threshold and the provincial privacy law must be at least as good, or it is not substantially similar: Privacy Commissioner of Canada, *Report to Parliament Concerning Substantially Similar Provincial Legislation* (March 17, 2003).

7 Ministry of Management Services Corporate Privacy and Information Access Branch, *Privacy Protection in the Private Sector*, Consultation Paper, 2002 at 8

8 PIPEDA, s. 4

9 PIPEDA, s. 2

10 *Interpretation Act*, R.S. 1985, c. – I-21, s. 35

Notably, however, because of the limitation on federal powers contained in the *Constitution Act, 1867*, PIPEDA does not apply to employee data of provincially regulated employers, unless such information was collected for use in a commercial activity.

"Commercial activity is defined in PIPEDA as follows:

> "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 fundraising lists.

Courts have yet to define "commercial activity" as it relates to PIPEDA. Organizations, such as charities, engage in predominantly non-commercial activities, with perhaps a few commercial activities on the side. It is unclear whether the Courts will consider the commercial activity conducted by such organizations to be the determining characteristic of the organization, such that PIPEDA applies, or whether the Courts will sever the commercial activity, so that PIPEDA does not apply.

"Personal Information"

PIPEDA protects "personal information", which is defined as "information about an identifiable individual"[11], and includes the following[12]:

- age, ID numbers, income, ethnic origin, or blood type;
- opinions, evaluations, comments, social status, or disciplinary actions; and
- employee files, credit records, loan records, medical records, existence of a dispute between a consumer and a merchant, intentions (for example, to acquire goods or services, or change jobs)

However, the definition of "personal information" excludes "contact" information for employees of organizations, including a person's name, title, business address or telephone number.

---

[11] PIPEDA, s. 2

[12] Privacy Commissioner of Canada: *Your Privacy Responsibilities: Guide for Businesses and Organizations to Canada's Personal Information Protection and Electronic Documents Act*: http://www.privcom.gc.ca/information/guide_e.asp

Personal information may be contained in a variety of formats, as evidenced by the definition of "record" contained in PIPEDA:

> "record" includes any correspondence, memorandum, book, plan, map, drawing, diagram, pictorial or graphic work, photograph, film, microform, sound recording, videotape, machine-readable record and any other documentary material, regardless of physical form or characteristic, any copy of any of those things.

In a paper presented to a privacy and employment law conference[13], T. Murray Rankin, Q.C. stated that even "unrecorded" personal information is subject to PIPEDA and that tissue information, blood and urine samples would likewise constitute one's "personal information".

PIPEDA also protects "personal health information", which is defined as follows[14]:

> "personal health information", with respect to an individual, whether living or deceased, means:
>
> (a) information concerning the physical and 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.

Individuals and organizations involved in healthcare will likely collect information from patients that falls within the scope of "personal health information".

In complaints made by an individual and a physician, the federal Privacy Commissioner found that physicians' prescriptions are not "personal information" and thus not protected by

---

[13] T. Murray Rankin, Q.C, *Document Keeping, Consent and Disclosure – What, When, Where, How Long, To Whom?*, paper presented at Privacy Laws & Effective Workplace Investigations, April 23-24, 2003 at 6, Insight Information Co., Vancouver

[14] PIPEDA, s. 2

PIPEDA[15]. The individual and the physician complained that IMS Health Canada ("IMS"), a U.S. based international marketing firm was improperly disclosing personal information by gathering and selling data on physicians' prescribing patterns without their consent. IMS had gathered the following information from Canadian pharmacies, which it used to produce customized information products for sale to pharmaceutical companies:

- store number, transaction date;
- drug identification number, drug name, form, strength, manufacturer, quantity, cost, selling price, whether a new or refill prescription, prescription number, repeat authorizations, reference codes identifying reason for us, reasons for a "no substitution" order;
- prescriber first and last name, identification number, phone number;
- information regarding the insurance carrier (if any) including deductible, form of payment, co-payment;
- patient gender, date of birth.

The federal Privacy Commissioner stated the following in determining that physicians' prescribing habits are not "personal information" under PIPEDA:

> Clearly a prescription directed to a pharmacist to dispense a certain medication in a certain dosage to an identified patient, is personal health information about that patient. By extension, all of the prescriptions directed to pharmacists by a physician are also the personal health information of the patients. But is this prescription information–whether an individual prescription or the totality of prescriptions- anonymized as far as the patient is concerned, also personal information about the prescribing physician?
>
> It is certainly difficult to discern how an individual prescription can constitute personal information about the physician who wrote it. While it can be revealing with regard to the patient–the nature of an illness or condition, for instance, and

---

[15] *PIPED Act* Case Summary #14 and *PIPED Act* Case Summary #15. The individual complainant is seeking judicial review of the Privacy Commissioner's decision: *Maheu v IMS Health Canada and the Privacy Commissioner of Canada.* The Federal Privacy Commissioner's decision has been subject to strong criticism – See: Paul Jones, *Just What is Your "Personal Information"? Has the Privacy Commissioner Struck the Right Balance in IMS Health?*, *The Law Times*, December 10, 2001

> perhaps its severity–it discloses little or nothing about the physician as an individual. Indeed, a prescription is not normally treated as personal information about himself or herself by the prescribing physician. The patient is not enjoined to secrecy, remaining entirely free to show it to anyone at will or to leave it unattended in a public place.
>
> This is not surprising, because the prescription is not, in any meaningful sense, "about" the physician. It does not tell us how he goes about his activities, whether he is casual or formal, whether he works mornings or afternoons, whom he meets, where he goes, what views he holds, or any of the other myriad details that might constitute personal information. Rather, a prescription is the outcome of the professional interaction between the physician and the patient: the physician meets the patient, carries out an examination, perhaps reviews the results of tests, and then issues the prescription. Hence, the prescription can perhaps most appropriately be regarded as a "work product." I find it to be information not about the physician, but about something once removed, namely the professional process that led to its issuance.
>
> If an individual prescription is not personal information about the physician, can the prescribing patterns deduced from analyzing a multiplicity of prescriptions nevertheless constitute such personal information?
>
> …
>
> For that matter, in the case of federal works, undertakings or businesses covered under the *Act*, interpreting personal information so broadly as to encompass work products could have the effect of including under the rubric of personal information about employees such things as letters written by employees in the course of their employment, legal opinions, or reports prepared by employees for use by management.
>
> I do not believe that such results would be consistent with the stated purpose of the *Act*. Rather, it is my view that the balance is properly struck by establishing whether the information is indeed about the individual, or rather about the tangible result of his or her work activity, namely the work product.
>
> In the case of the present complaint, I find the latter to be true. Accordingly, I find that prescription information–whether in the form of an individual prescription or in the form of patterns discerned from a number of prescriptions–is not personal information about the physician.

In Alberta, the Alberta Privacy Commissioner has ruled that pharmacists and pharmacies are violating the *Health Information Act*, H-5, R.S.A. 2000 by disclosing physicians' names in the course of selling prescribing information to IMS. The Commissioner ordered pharmacists and pharmacies not to disclose the prescriber's first and last name to IMS, unless consent is

obtained[16]. However, that decision was not made on the basis that prescribing information was "personal information" protected by the Alberta legislation.

Exceptions to the Application of PIPEDA

PIPEDA does not apply to the following[17]:

- The collection, use or disclosure of personal information by federal government institutions listed under the *Privacy Act*;
- Provincial or territorial governments and their agents;
- An employee's name, title, business address or telephone number;
- An individual's collection, use or disclosure of personal information strictly for personal purposes; and
- An organization's collection, use or disclosure of personal information solely for journalistic, artistic or literary purposes.

III. APPLICATION OF PIPEDA TO ORGANIZATIONS INVOLVED IN THE MANAGEMENT OF HEALTHCARE IN ABORIGINAL COMMUNITIES

Individuals or organizations that collect, use or disclose personal information in the course of commercial activities will be subject to PIPEDA. PIPEDA's application in the healthcare sector is somewhat uncertain as the Courts have not yet interpreted the meaning of "commercial activity". In particular, it is unclear whether healthcare organizations fall within the definition of "commercial activity". Hospitals, physicians or other healthcare organizations may perform activities which could be characterized as "commercial" or quasi-commercial, thus bringing them within the scope of PIPEDA. There is a constitutional argument that PIPEDA cannot apply to hospitals because the *Constitution Act, 1867* specifically assigns the provinces the exclusive

---

16 IMS is seeking judicial review of the Alberta Privacy Commissioner's decision.

17 As identified by the Privacy Commissioner of Canada in, *Your Privacy Responsibilities: Guide for Businesses and Organizations to Canada's Personal Information Protection and Electronic Documents Act:* http://www.privcom.gc.ca/information/guide_e.asp

jurisdiction to establish, maintain and manage hospitals[18]. However, hospitals or healthcare organizations run by Aboriginals would likely be considered federal undertakings within the scope of section 91(24) of the *Constitution Act, 1867* such that PIPEDA would apply.

The proposed British Columbia legislation will likely apply to hospitals and healthcare organizations in any event, and is expected to be substantially similar to PIPEDA. As such, it is recommended that British Columbia hospitals, healthcare providers, managers and organizations comply with PIPEDA, as that will set up the healthcare organization for compliance with the anticipated British Columbia legislation.

There are many ways in which PIPEDA, or similar provincial legislation, could potentially apply to organizations involved in the management of healthcare in Aboriginal communities. For instance, such organizations may be involved in conducting research based on personal health information collected or they may be approached by third parties wanting to conduct research using the personal health information gathered by the organization. Many organizations involved in the management of healthcare in Aboriginal communities, both on and off reserve, provide health-related programs such as men's and women's therapy groups, spiritual retreats, drug and alcohol treatment programs, crisis prevention programs, programs targeted at helping youth maintain healthy lifestyles, and so on. These programs are often funded by Band Councils, governments and/or charitable agencies who request reports with respect to the services provided in order to establish how much funding they will provide.

III. COMPLYING WITH PIPEDA

The Federal Privacy Commissioner, George Radwanski, has published a guide which provides compliance advice for organizations subject to PIPEDA[19]. The Privacy Commissioner recommends that organizations do the following:

---

[18] Alan Belaiche, *Privacy Update: Where We've Been, Where We Are and Where We are Going? Does Anybody Really Know for Sure?* Miller Thomson LLP Comminique, April 28, 2003

[19] G. Radwanski, *Your Privacy Responsibilities*: Guide for Businesses and Organizations to Canada's Personal Information Protection and Electronic Documents Act: http://www.privcom.gc.ca/information/guide_e.asp#004

(1) Be Accountable

In order to comply with PIPEDA, an organization should appoint a Compliance Officer who will be in charge of the collection, use and disclosure of personal information. The Compliance Officer will be responsible for analyzing the personal information handling practices of the organization and subsequently developing and implementing a policy plan that ensures compliance with PIPEDA. The Federal Privacy Commissioner indicates that a policy plan should address the following:

(a) implementing procedures to protect personal information;

(b) establishing procedures to receive and respond to complaints and enquiries;

(c) training staff and communicating to staff information about the organization's policies and practices;

(d) developing information to explain the organization's policies and procedures; and

(e) ensuring the accuracy of the personal information held by the organization; and updating and retention policies.

(2) Identify the Purpose

The organization should identify the reasons for collecting personal information, before or at the time of collection. The Federal Privacy Commissioner recommends that the purposes for collecting be clearly and narrowly defined so the individual can best understand how the information will be used or disclosed.

Examples of purposes for which personal information may be collected include[20]:

- opening an account
- verifying creditworthiness

---

[20] *Ibid*

- providing benefits to employees
- processing a magazine subscription
- sending out association membership information
- guaranteeing a travel reservation
- identifying customer preferences
- establishing customer eligibility for special offers or discounts

(3) Obtain Consent

PIPEDA requires that the individual is informed, in a meaningful way, of the purposes for the collection, use or disclosure of the personal information. Consent should be obtained before or at the time of collection. When a new use for the personal information is identified, the individual's consent to that new use must be obtained. Where an organization has collected personal information prior to the implementation of PIPEDA, the organization must obtain consent in order to continue to use the information[21].

Section 7 of PIPEDA contains several exceptions to the requirement for consent in the collection, use and disclosure of personal information.

(4) Limit Collection

One of the simplest strategies to ensure compliance with PIPEDA is to limit, as much as possible, personal information collected and retained. Organizations should be very clear about what information they need for their particular purpose and be sure to only collect that information. By reducing the amount of information gathered, an organization can lower the cost of collecting, storing, retaining and ultimately archiving the data. Similarly, if the organization holds information that it no longer needs, the organization should destroy that information in accordance with their retention policy.

---

[21] *Ibid*

(5) Limit Use, Disclosure & Retention

Personal information should be used or disclosed only for the purpose for which it was collected, unless consent has been obtained, or the use or disclosure is authorized by PIPEDA. Personal information should be kept only as long as required and an organization should develop a policy and procedures for the retention and destruction of personal information.

(6) Be Accurate

Personal information collected should be accurate, complete and up to date. The Federal Privacy Commissioner recommends that one way to determine if information needs to be updated is to ask whether the use or disclosure of out of date or incomplete information would harm the individual[22].

(7) Use Appropriate Safeguards

An organization should protect personal information against loss or theft and safeguard the information from authorized access, disclosure, copying, use or modification. Ways in which to accomplish this include[23]:

- locked cabinets, restricted access, alarms
- passwords, encryption, firewalls, anonymizing software
- organizational controls such as security clearances, limiting access on a "need to know" basis, staff training, confidentiality agreements

(8) Be Open

An organization should inform customers, clients and employees of its policies and practices for the collection, use, management and disclosure of personal information and should publicize the name of its Compliance Officer.

---

[22] *Ibid*

[23] *Ibid*

(9) Give Individuals Access

Individuals should be allowed access to their personal information upon request and provided an opportunity to correct that information if necessary.

Section 9 of PIPEDA contains exceptions to an individual's right to access personal information held by an organization. Organizations **must** refuse an individual access to personal information where:

- It would reveal personal information about another individual, unless there is consent or a life threatening situation.
- The organization has disclosed information to a government institution for law enforcement or national security reasons. Upon request, the government institution may instruct the organization to refuse access or not to reveal that the information has been released. The organization must refuse the request and notify the Privacy Commissioner. The organization cannot inform the individual of the disclosure to the government institution, or that the institution was notified of the request, or that the Privacy Commissioner was notified of the refusal.

Organizations **may** refuse access to personal information if:

- The information is subject to solicitor-client privilege
- The information is confidential commercial information
- Disclosure of the information could harm an individual's life or security
- The information was collected without the individual's knowledge or consent to ensure its availability and accuracy, and the collection was required to investigate a breach of an agreement or contravention of a federal or provincial law (the Federal Privacy Commissioner must be notified)
- The information was generated in the course of a formal dispute resolution process.

(10) Challenging Compliance

An organization should develop a complaint procedure and inform complainants of the avenues of recourse, including the organization's own complaint procedures, regulatory bodies and the Federal Privacy Commissioner. All complaints should be acknowledged, investigated and responded to in an appropriate fashion.

Consequences of Non-Compliance with PIPEDA

The enforcement powers of PIPEDA indicate that non-compliance could lead to serious problems for organizations involved in the collection, use and disclosure of personal information in the course of commercial activities. PIPEDA provides that an individual can file a complaint with the Privacy Commissioner against an organization for contravening a provision of PIPEDA or failing to follow a recommendation set out in Schedule 1[24]. It is also possible for the Privacy Commissioner to initiate a complaint[25]. Once a complaint is made, the Privacy Commissioner is obliged to conduct and investigation and is given broad powers to carry out such investigation.[26] The Privacy Commissioner must respond to the complainant by providing a written report of the investigation within one year of the complaint[27]. The complainant may, after receiving the Privacy Commissioner's report, apply to the Federal Court for a hearing in respect of any matter which the complaint was made, or that is referred to in the Privacy Commissioner's report[28]. The Court then has the power to:

(a) Order an organization to correct its practices in order to comply with PIPEDA;

(b) Order an organization to publish a notice of any action taken or proposed to be taken to correct its practices; and

---

[24] PIPEDA, s. 11(1)

[25] PIPEDA, s. 11(2)

[26] PIPEDA, s. 12

[27] PIPEDA, s. 13

[28] PIPEDA, s. 14

(c) Award damages to the complainant, including damages for any humiliation that the complainant suffered.[29]

There are few cases dealing with the interpretation of PIPEDA, however, in *Maheu v. IMS Health Canada*[30], the Federal Court considered the issue of who is entitled to apply to Court for a hearing. An issue in *Maheu* was whether the complainant could initiate an action when the subject of the complaint did not involve his own personal information. The Court found that PIPEDA does not require the complainant to take issue with respect to their own personal information, but rather anyone could make a complaint if they believe PIPEDA has been contravened[31].

IV. CONSENT

PIPEDA requires that, apart from a few limited exceptions, no organization can collect, use or disclose personal information about an individual without that individual's consent. PIPEDA does not contain a definition of "consent", but provides examples of ways in which consent may be obtained, including[32]:

- An application form;
- A checkoff box 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;
- Orally over the telephone; and
- At the time that individuals use a product or service.

The above noted examples of consent demonstrate that consent may be express, implied or deemed. An application is an example of written, "express" consent. The use of a checkoff box

---

[29] PIPEDA, s. 16

[30] [2003] F.C.J. No. 3 (T.D.)

[31] *Ibid* at paras. 35 & 39

[32] PIPEDA, Schedule I, Principle 4.3.7

is an example of a deemed consent, in that consent is assumed or deemed unless the individual takes some step to "opt out" and specifically deny their consent. Consent may be implied where it is clear from the facts that had consent been sought, it would have been granted as a matter of course.

In a 2002 decision[33], the Federal Privacy Commissioner stated that when determining the appropriate form of consent, an organization must take the sensitivity of the information into account. He determined that negative or "opt out" consent is not appropriate for sensitive information, which requires "opt in" consent. The Privacy Commissioner's decision echoes Principle 4.3.6 of PIPEDA which provides that an organization should generally seek express consent where the information is likely to be considered sensitive while implied consent is generally acceptable where the information is less sensitive. Additionally, the form of consent also depends on the reasonable expectations of the individual and the circumstances surrounding collection[34].

Consent is only meaningful when the individual understands the way in which their personal information will be used. As such, consent clauses should be clear, easy to find, as specific as possible about related organizations (subsidiaries) that will handle the information, and should not use blanket categories for purposes, uses or disclosures.

Given the particularly personal and sensitive nature of information generated in the healthcare context, it is likely that consent for the disclosure of medical information will need to be express, written consent.

PIPEDA does recognize circumstances where personal information may be collected, used and disclosed without consent[35]. For instance, sections 7(2)(c) and 7(3)(f) permit an organization to use or disclose personal information without the knowledge or consent of the individual to whom it pertains if the following five conditions are met:

- The disclosure or use must be strictly for statistical or scholarly study or research;

---

[33] *PIPED Act* Case Summary #42

[34] *Supra*, note 19

[35] PIPEDA, s. 7

- The purposes cannot be achieved without using or disclosing the information;
- The information must be used in a manner that safeguards its confidentiality;
- Obtaining consent must be impractical; and
- The organization seeking exemption under section 7 of PIPEDA must inform the Privacy Commissioner of the proposed use or disclosure beforehand.

The exceptions contained in sections 7(2)(c) and 7(3)(f) of PIPEDA indicate that PIPEDA is not intended to deter or impede legitimate health research that uses information in ways that does not impact the individuals to whom it pertains[36]. The Federal Privacy Commissioner has stated that he intends to give a broad interpretation to the definition of statistical or scholarly study or research[37].

Assuming that PIPEDA applies, it requires an organization involved in the management of health care within Aboriginal communities to obtain consent from individuals before collecting, using or disclosing any personal information about the individual. Failure to comply with the obligation to obtain consent could result in a complaint by an individual to the Privacy Commissioner, which may put the organization in a poor light and cause patient distrust.

V. CONCLUSION

PIPEDA, or similar provincial legislation eventually enacted, may present administrative challenges for organizations involved in the management of healthcare in Aboriginal communities. Given the breadth of obligations, such organizations are well advised to begin assessing their situation to determine if information collecting can be limited in anyway. While the administrative burden of complying with PIPEDA or provincial private sector privacy legislation may seem great, gaining public confidence in private sector privacy policies may make the effort worthwhile.

---

[36] G. Radwanski, *Privacy In Health Research: Sharing Perspectives and Paving the Way Forward*, November 14, 2002: http://www.privcom.gc.ca/speech/02_05_a_021114_e.asp

[37] *Ibid*