
April 2004

# The Application of PIPEDA to Personal Health Information

Reprinted by permission of LexisNexis Canada Inc., from
*Canadian Privacy Law Review*, March 2004, edited by Michael Geist, Copyright 2004.

**David T.S. Fraser -** david.fraser@mcinnescooper.com

Since it was a bill being debated before Parliament, one of the most contentious issues related to the *Personal Information Protection and Electronic Documents Act*[1] ("PIPEDA") has been if — and how — it applies to the practice of medicine and the handling of personal health information. The Canadian Medical Association and other similar organizations lobbied strongly against the inclusion of health information within the ambit of PIPEDA. This lobbying continued to the final hours of 2003, at which point it became clear that the federal cabinet did not support either a "carve-out" or a postponement of the law's application to medical information.

Among medical professionals, PIPEDA is widely seen as a tool that does not effectively address the nuances that separate personal information collected in the medical context from that which is ordinarily used in the course of commerce. There was also a strong strain of opinion that physicians' ethical obligations and the CMA Health Information Privacy Code are sufficient to protect patient privacy. The medical and dental professions should be exempted, it was argued. In the end, PIPEDA did not treat health information as a special class of information and did not specifically exempt physicians or dentists from its application.[2]

Leaving the statute unamended did not clarify the application of the law to health information because a myriad of questions linger, at least in the minds of many. While there are many important issues related to PIPEDA and personal health information, this article will focus on the impact of PIPEDA on medical professionals in private practice. Many medical professionals who have turned their minds to this issue are primarily concerned with whether PIPEDA applies in a particular circumstance and the impact of other laws specifically focused on personal health information.

According to s. 4 of the Act, PIPEDA applies to:

> ...every organization in respect of personal information that
>
> (*a*) the organization collects, uses or discloses in the course of *commercial activities*;... [Emphasis added.]

This raises the very important question: what part of the practice of medicine is, in fact, a commercial activity? There appears to be a consensus that a physician in private practice is engaged in commercial activities, regardless of whether services are paid for by public insurance. PIPEDA thus applies to private practice. What about physicians working at a hospital? Or, physicians employed by university health clinics? The lines can get very blurry.

In determining whether an activity is commercial, the approach of the Office of the Privacy Commissioner appears to be to (a) characterize the objectives and general activities of the organization; and (b) characterize the particular activity in question. The activity may appear to be a "commercial activity", but if it is intimately connected to an overarching non-commercial objective, it may not be caught within the Act. (An example might be the operation of a student residence at a university. Renting accommodation may appear to be commercial, but in the university context where the accommodation is provided to students, it is intimately related to the non-profit objectives of the university. However, if the university rents out the rooms to tourists during the summer, that activity crosses the line because it would no longer be connected to core non-commercial function of the university.) It has been said by representatives of the Office of the Privacy Commissioner that PIPEDA does not generally apply to public hospitals:[3]

> The Act does not, however, apply to: ... Any organization that collects, uses or discloses personal information in the course of a non-commercial activity such as a public hospital, a charity engaged in fundraising, a university in respect of information about its students, and so on.

There does not appear to be much question that a physician providing care in a hospital is carrying out a core function of the public hospital. Assuming that the courts follow the above reasoning, this group of physicians is excluded from the Act, at least when they are acting on behalf of the hospital. Unfortunately, many circumstances are not nearly as cut and dried as the above. Many physicians split their time between hospitals and their own practices, a practice that has been relatively seamless up to this point. It appears that PIPEDA would apply to only half of their practice.

Once the question of "who is in and who is out" is settled (or at least there is some sense of comfort with the shades of grey), the question to be asked is what impact PIPEDA will have on those who are bound by its provisions *and* deal with personal health information. For most medical professionals, the important question is how to implement the consent principle:

> 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.

Patients must provide consent for the collection, use and disclosure of their personal health information. Some have suggested that consent should be implied and that it is "business as usual" for those dealing with health information. In a letter to the Manitoba Medical Association, the interim Privacy Commissioner suggested that implied consent is acceptable within the "circle

of care".[4] A message that can easily be lost in Mr. Marleau's letter is that consent, from Principle 3, must be based on the identification of purposes, from Principle 2:[5]

> While consent has to be based on knowledge of why the information is being collected and how it will be used and disclosed, this does not require that doctors and other providers hold conversations with every patient to ensure they are informed — consent is acceptable, assuming it is based on a general understanding of how personal information will be used and disclosed, for those uses or disclosure that a patient would reasonably expect;…. Implied consent is acceptable within the "circle of care", i.e. for uses and disclosures required to provide care and treatment.

The letter from the Interim Commissioner has been widely circulated among the medical community and is quoted from by the President of the Canadian Medical Association in an Op-Ed article in the *Medical Post*.[6] In addition, Industry Canada's "PIPEDA Awareness Raising Tools Initiative for the Health Sector" embraces the principle of implied consent.[7] Overall, much of the medical community believes it is "business as usual" because medical professionals can rely on implied consent within the circle of care.

The ultimate interpreter of PIPEDA will be the Federal Court of Canada and there is a strong view that implied consent is insufficient in many cases for the routine collection, use and disclosure of personal health information by health care professionals. Subprinciples 4 and 5 of the consent principle elaborate on the law's requirements:

> 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....
>
> 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*. Consent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney). *[*Emphasis added.*]*

There is no debate that medical information is among the most sensitive personal information and diagnostic information is even more sensitive. This was the conclusion of the Assistant Commissioner in a recent finding. PIPEDA Case Summary #226[8] is the most recent of a small handful of findings to consider personal health information,[9] and the only one in which the complaint was well-founded. The complainant was a former employee of a telecommunications company who alleged that the employer was unnecessarily collecting

personal medical information and had not implemented appropriate security safeguards to protect that information.

The allegation that the employer did not adequately safeguard the employee's information is the most relevant for the purposes of this discussion because the safeguards principle is similar to the consent principle, in that both require a consideration of the sensitivity of the information in question:

> 4.7 Principle 7 — Safeguards
>
> Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

The employer was assisting its insurer with the administration of its long-term disability program and required employees to file claim forms and medical reports with the employer's Human Resources office instead of directly with the insurer. The complainant objected to the employer's practice of collecting medical reports by facsimile to the Human Resources office.

With respect to the complaint about safeguards, the Assistant Commissioner made some very important determinations. First of all, she concluded that medical information is considered to be "sensitive information" and information related to a "specific diagnosis is among the most sensitive of medical information". The organization was in violation of Principle 7 because it received sensitive medical information, including diagnostic information, on a facsimile machine that was in an unlocked, accessible room. In the circumstances, receiving the information by fax was not appropriate, regardless of whether it occurred at the local human resources office or at the company's head office. Allowing general human resources staff to receive and process reports containing such sensitive medical information was also not appropriate. While employers may have a legitimate need to collect certain medical information (for purposes of verifying an employee's medical absences and to meet employer obligations to accommodate employees under human rights legislation), stringent safeguards must be put in place. Specifically, the Assistant Commissioner said that medical diagnoses should only be shared among qualified medical practitioners.

The Assistant Commissioner concluded that while the purposes for the collection by the employer might have been legitimate, the practices were unacceptable "on the whole".

The highly sensitive nature of personal health information demands stringent safeguards. Likewise, under PIPEDA, any collection, use or disclosure of such sensitive information would also require robust consent, all of which must be based on communicating to the patient the purposes for which the information will be used:

> 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.

For "ordinary" personal information, one can only rely on implied consent if the individual concerned is aware of the purposes for which the information is being collected and the organization has complied with Principle 2 by making reasonable efforts to bring the

purposes to the attention of the individual concerned. In some cases, the purposes of an organization collecting personal information are blindingly obvious from the circumstances. If this is the case, consent can be very easily inferred. But, in the medical context, many patients do not know what happens to their medical records and they probably do not know that they are routinely used outside the "circle of care" for peer review, chart reviews, risk mitigation consultations with the physician's insurer, etc.

Relying on implied consent with medical information is fraught with risks. Certain disclosures outside the "circle of care" only take place when there are difficulties with the patient (such as seeking advice from the Canadian Medical Protective Association). If, for example, a physician is experiencing difficulties with a particular patient and needs medico-legal advice from his or her insurer, the state of the relationship with the patient will likely preclude obtaining informed consent. These risks can be mitigated by clearly informing patients how their information will be used and getting advance consent to all such uses. The consent form should be carefully drafted so that it does encompass virtually every ordinary use of personal information. Specific disclosures, such as sending a copy of the file to the patient's lawyer, should be documented by additional signed consent.

At least in a number of provinces, medical professionals are also left wondering about the application of other laws to personal health information. Before PIPEDA came into force for the provincially-regulated private sector, a number of western provinces had enacted legislation to deal specifically with health information: See Saskatchewan's *Health Information Protection Act*;[10] Alberta's *Health Information Act*;[11] and Manitoba's *Personal Health Information Act*.[12] In the last few months, Ontario has introduced the *Personal Health Information Protection Act, 2003*.[13] None of these statutes have been declared to be "substantially similar" to PIPEDA. In fact, they have been variously described as having very little to do with privacy and much more concerned with providing government and researcher access to confidential medical records. Physicians in those affected jurisdictions — at least those who are engaged in commercial activities — will be subject to two statutes. Many are unaware of their obligations under *one* statute, let alone both. Jurisdictional overlap may be inconvenient for individuals who are seeking recourse, but the co-existing federal and provincial regimes may leave medical and dental professionals having to contend with different — and perhaps contradictory — rules.

Unfortunately for medical professionals in such provinces, there is no easy answer. As long as PIPEDA is constitutional in its application to commercial activities, health information used in private practice is an area where both the federal Parliament and the provincial legislatures are competent to act. Many medical professionals still hope that the federal government will remove health information from the purview of PIPEDA or that these provincial statutes will be declared to be substantially similar. There is little hope that either of these two changes will occur, so health care professionals are going to have to contend with dual regulation.

Medical professionals and the lawyers who advise them, like many others, are discovering that PIPEDA is based on principles, rather than strict rules. Even though its application to particular activities is somewhat difficult to discern in areas where the private and public sectors abut, the law itself is a reality to which those who handle health information must become accustomed. This is supplemented by the complete overlap of jurisdictions in some

western provinces. Among the few areas of absolute clarity is that personal health information is among the most sensitive of personal information and the threshold for its protection is set proportionately high.

---

[1] S.C. 2000, c. 5.

[2] PIPEDA did treat health information differently from ordinary personal information during the law's first year of application in the federally-regulated private sector. Federal works, undertakings and businesses were given an additional year — until 2002 — before the law would apply to "personal health information". See PIPEDA, ss. 30(1.1) and (2.1).

[3] Speech by Heather Black (then General Counsel to the Office of the Privacy Commissioner) to the Law and Technology Institute of Dalhousie University (March 22, 2002), available on-line at: <http://www.privcom.gc.ca/speech/02_05_a_020322_2_e.asp>.

[4] Letter from Robert Marleau to Mr. John A. Laplume (November 21, 2003), available on-line at: see <http://www.cma.ca/staticContent/HTML/N0/l2/HIT/pdf/MMA-Marleau%20letter-PIPEDA.pdf>.

[5] Ibid.

[6] Dr. Sunil Patel, "Patient Privacy, 'PIPEDA' and You," Medical Post (December 16, 2003), available on-line at: <http://www.cma.ca/cma/menu/displayMenu.do?tab=422&skin=432&pMenuId=4&pageId=/staticContent/HTML/N0/l2/advocacy/news/2003/12-16.htm>.

[7] See the PART web site at: <http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/vwGeneratedInterE/gv00211e.html>. Importantly, the web site's authors emphasize that implied consent has to be based on the patient being informed of the purposes of the collection, use or disclosure of personal health information.

[8] The summary of this finding is available from the Office of the Privacy Commissioner at: <http://www.privcom.gc.ca/cf-dc/2003/cf-dc_031031_e.asp>.

[9] See also PIPED Act Case Summaries #118, 119, 120 and 135, all of which are available from the web site of the Office of the Privacy Commissioner.

[10] S.S. 1999, c. H-0.021.

[11] R.S.A. 2000, c. H-5.

[12] C.C.S.M., c. P33.5.

[13] Bill 31, An Act to enact and amend various Acts with respect to the protection of health information, 1st Session, 38th Parliament (Ontario), 2003.

## THE MCINNES COOPER PIPEDA TEAM

McInnes Cooper's Privacy Practice Group is comprised of lawyers with experience and expertise in advising businesses, non-profits and medical professionals on the application of PIPEDA to their operations. If you have any questions, please contact any of the following:


**Nova Scotia**
David T.S. Fraser
902 424 1347
david.fraser@mcinnescooper.com

**New Brunswick**
Jaime Connolly
506 458 1544
jaime.connolly@mcinnescooper.com

**Newfoundland**
Jackie Penney
709 724 8239
jackie.penney@mcinnescooper.com

**Prince Edward Island**
Clea Ward
902 629 6271
clea.ward@mcinnescooper.com