Hospital Law

The Implications of the New Federal Privacy Legislation for Public Hospitals

PAMELA C. SPENCER

On April 4, 2000, Parliament passed Bill C-6, now known as the Personal Information Protection and Electronic Documents Act. Bill C-6 subsequently received Royal Assent on April 13, 2000. Passage was preceded by almost two years of deliberation and sometimes acrimonious debate. Some of this debate, and related acrimony, centred on the concerns that key healthcare stakeholders expressed as to the possible implications of the Act on the health system. In this article, I outline the concerns of these stakeholders and focus on the possible implications of the Act on public hospitals in Canada. By way of caveat, given the scope of the Act and its interrelationship with the numerous statutes and regulations that apply provincially to public hospitals, it is beyond the mandate of this article to offer an in-depth analysis of the possible effects of the Act on hospitals in any particular province. This article provides a broad overview of the Act from the perspective of public hospitals and highlights some of the key areas of concern.

It is important to make two points regarding the Act's mandate. First, the Act is an initiative of Industry Canada and is rooted in the federal government's constitutional power to regulate "trade and commerce." Thus, while healthcare delivery (including the protection of personal health information) is a matter for provincial regulation, the federal government is attempting to rely on its constitutional authority over "trade and commerce" to regulate healthcare delivery in the private sector and in respect of interprovincial and national cross-border exchanges. Given Canada's constitutional framework, one might reasonably take the position that it is a stretch for the federal government to attempt to include personal health information under the Act. Certainly, many key healthcare stakeholders argued against its inclusion during the discussions held in respect of the Act. In fact, although the matter was later disputed by the Minister of Industry, it was alleged during the Senate Committee hearings on Bill C-6 that Industry Canada officials had stated on the record that health information would not be a part of the Act (see the testimony of the Ministry of Industry, Senate Standing Committee 1999, at 27 on-line). Whether or not this is true, it is important to recognize that the Act was never specifically designed as a health information protection act. As such, it is not surprising that the Act, in its present incarnation, fails in several key respects to recognize the interests of healthcare stakeholders, including public hospitals.

The Structure of the Act

It should be stated at the outset that the legislation is complex, and sometimes confusing. Hospital administrators who find themselves confused after reviewing the Act will be in good company. Several legal colleagues and commentators have expressed frustration with the Act's complicated structure, its internal inconsistencies and the vagueness of some of its key definitions.

The Act is comprised of six parts and a schedule. Part 1 of the Act, which is the focus of this article, deals with the collection, use and disclosure of personal information, including personal health information, in the private sector. The schedule restates the fair information principles and commentary

that comprise the Model Code for the Protection of Personal Information (the "Model Code") approved by the Standards Council of Canada in 1996. Organizations subject to the Act will be required to comply with the Model Code, subject to the various provisions in the Act. A summary of the ten privacy principles set out in the schedule is found at the end of this article.

What makes the Act confusing is that, unlike most legislation, the operative provisions are set out both in the body of the Act and in the schedule. The reader is thus required to engage in a fair amount of flipping back and forth between the Act and the schedule in order to make sense of the provisions. An additional source of confusion stems from the fact that while the Model Code was meant to establish a voluntary national standard for the protection of personal information, many of its provisions, as set out in the schedule, use language that suggests the creation of obligations. Certain other provisions, however, are treated as recommendations for the purposes of the Act. The result is that the operation of the schedule, which is an integral part of the Act, is unclear.

What Is the Basic Right of Privacy in the Act?

Part 1 of the Act provides individuals with a right to privacy concerning their "personal information." The basic principle at the core of this right to privacy is that personal information should not be collected, used or disclosed, without the prior knowledge and consent of the individual concerned, subject to the limited exceptions set forth in the Act.

How Is "Personal Information" Defined?

"Personal information" is broadly defined in the Act as information about an identifiable individual, with the exception of the name, title or business address or telephone number of an employee of an organization. While the Act does not itself provide any guidance as to what constitutes "information about an identifiable individual," Industry Canada advises in its website (http://ecom.ic.gc.ca/english/privacy/632d30.html) that such information includes such things as race, ethnic origin, colour, age, marital status, religion, education, medical, criminal, employment or financial history, address and telephone number, numerical identifiers such as the Social Insurance Number, fingerprints, blood type, tissue or biological sample, and views or personal opinions. In short, Industry Canada's view is that any information in any form that can be attributed to an identifiable individual is caught by this definition, regardless of its sensitivity. Time will tell how personal information comes to be defined in practice.

How Is "Personal Health Information" Defined?

On the recommendation of the Senate, and in response to submissions by several healthcare stakeholders, the Act was amended before final passage by the House of Commons to include a separate definition for "personal health information." According to this definition, "personal health information," with respect to an individual, whether living or deceased, means:

- information concerning the physical or mental health of the individual or any health service provided to the individual;
- information concerning the donation by the individual of any body part or any bodily substance (such as blood or tissue samples), or information derived from the testing or examination of a body part or bodily substance of an individual;
- information that is collected in the course of providing health services to the individual; or
- information that is collected incidentally to the provision of health services to the individual.

It should be understood that "personal health information" is a subset of "personal information," such that the restrictions on dealings with personal information contained in Part 1 of the Act and Schedule 1 should be read as being generally applicable to personal health information.

What Is Commercial Activity?

Part 1 of the Act applies to organizations subject to the Act, that collect, use or disclose personal information "in the course of commercial activities." The distinction between what is commercial activity versus non-commercial activity is therefore key to the application of Part 1 of the Act. Unfortunately, the definition of "commercial activity" provided in the Act is unlikely to assist in making this distinction. The Act broadly defines "commercial activity" to include any single 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. Given the definition's inherent tautology, its scope is rather unclear. And while well-drafted regulations might have assisted in determining what constitutes "commercial activity," the Minister of Industry has indicated that no regulations are proposed to define the distinction between commercial and non-commercial activity (see the testimony of the Minister of Industry, Senate Standing Committee 1999, at 24 on-line).

The good news is that the majority of a public hospital's activities are unlikely to be subject to the Act since they are operated on a not-for-profit basis and are generally understood not to be commercial. However, some of a hospital's activities, such as the operation of a gift shop, might be characterized as commercial when viewed separately from the rest of the hospital's operations. Moreover, information disclosures made between a hospital and a private sector organization such as a private nursing home, laboratory, pharmacy, or clinic are likely caught by the Act (Doray 2000).

The 10 Privacy Principles

There are 10 principles at the heart of the Act. These principles set out the obligations of organizations when dealing with individuals' personal information.

1. **Accountability**
   Organizations are responsible for the personal information under their control. A specific individual or position must be designated as responsible for the organization's compliance with the Act.
2. **Identifying Purposes**
   Organizations must advise individuals why they are collecting the personal information and how it will be used.
3. **Consent**
   Organizations will be required to obtain an individual's consent to collect, use or disclose personal information, unless they can satisfy one of the limited exceptions to obtaining consent. Consent may be implied or expressly given; it may be provided orally or in writing.
4. **Limiting Collection**
   Organizations will only be entitled to collect the minimum personal information necessary to fulfil their stated goals.
5. **Limiting Use, Disclosure and Retention**
   Organizations must use and disclose personal information in accordance with the reasons stated to the individual. New uses and disclosures require new consent. Also, the information should be kept only for as long as necessary to meet the original purpose.
6. **Accuracy**
   The information must be kept accurate and as current as necessary to fulfil the stated purpose.
7. **Safeguards**
   Organizations must safeguard individuals' personal information to protect against loss, theft, unauthorized disclosure, copying, use or alteration. Technological safeguards include the use of passwords and encryption of information. Organizational security measures include the use of security clearances and limiting access on a "need-to-know" basis.
8. **Openness**
   Organizations must inform individuals about the personal information they hold, the purposes for which it is used, the persons to whom it is disclosed and how an individual may access it.
9. **Individual Access**
   Individuals are entitled to be given access to their personal information retained by organizations to ensure its accuracy and completeness, and to identify to whom it was disclosed, subject to certain exceptions.
10. **Challenging Compliance**
    Individuals can challenge an organization's compliance with these principles both through the organization's required complaints process and by making a complaint to the Privacy Commissioner. When the Privacy Commissioner investigates a complaint or conducts an audit, the Commissioner has broad powers, including entering an organization's premises, interviewing people and extracting records.

It has been pointed out that, assuming public hospitals are not generally covered by the Act, a number of inconsistencies arise. For example, the activities of a hospital pharmacy or laboratory would not be subject to the Act, while the very same activities carried out by a private pharmacy or laboratory would likely be covered (McNairn and Scott 2000: 16). Complicating the situation for hospitals is the uncertainty as to whether the Act affects health professionals in the delivery of their services (McNairn and Scott 2000: 16). The statements made by the Minister of Industry on this issue suggest that while information exchanges related to patient care among health professionals within a hospital will be considered non-commercial for the purposes of the Act, information exchanges between the hospital and third party payers related to reimbursement for these same health services will likely fall under the definition of "commercial activity" (see the testimony of the Minister of Industry, Senate Standing Committee 1999, at 24 on-line.) Trying to figure out which activities carried out by a hospital are sufficiently "commercial" so as to fall under the Act is likely to be a challenge.

Consent Issues

While the interrelationship between the Act's consent provisions and the various provincial statutes dealing with consent to medical treatment is beyond the scope of this article, it can be stated that the Act's consent provisions raise concerns for health professionals. First, while the premise of the Act is a consent-based system, the Act does not identify who is to be responsible for determining capacity to consent or for obtaining consent. Moreover, the Model Code, as set out in Schedule 1, does not preclude reliance upon implied consent; instead, it notes that organizations should generally obtain express consent when the personal information at issue may be sensitive. Conversely, the Model Code states that implied consent is appropriate for less sensitive information (Schedule 1, section 4.3.6). On their face, the consent provisions in the Model Code suggest a reworking of the concept of informed consent as it has developed over the past several decades. From the hospitals' point of view, the coming into force of the Act will likely precipitate an overhaul of the hospital's existing consent forms and consent practices.

Implications of the Act on Research Activities

Starting from the premise that the Act will apply to hospitals and possibly health professionals in the context of their "commercial activities" (subject to the Act's transitional provisions discussed below), it is likely that the Act will apply to industry-sponsored research activities that involve hospital patient data. For example, clinical drug trials carried on in a hospital and sponsored by a pharmaceutical company will likely be caught by the Act.

The Act does contain a limited exception for personal information that is used for research purposes. In this regard, the Act permits an organization to use or disclose personal information, without the knowledge or consent of the individual:

- where it is used for statistical, scholarly study or research purposes that 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 federal Privacy Commissioner of the disclosure or use before the information is disclosed or used.

There are three important points to note about this exception. First, no similar exemption is made for the collection of the information. The Model Code clearly requires that the individual be told of the purposes for which the personal information is collected at or before the time the information is collected (Schedule 1, section 4.2). Therefore, "commercial" research that is based on a retrospective review of hospital charts (assuming that these charts have been "washed" of personal identifiers) will only be permitted where the patient had consented, at the time that the information was initially collected, to the subsequent use of his or her medical records for research purposes.

Second, there is no "grandfathering" provision in the Act that exempts an organization from the application of the Act with respect to the use or disclosure of information already in its possession. Therefore, a hospital will be unable to use or disclose to anyone involved in commercial research activities any personal information contained in its existing medical records that the hospital collected before the Act came into force without the prior knowledge and consent of the patients concerned, unless the hospital now obtains all of those patients' consents, or it obtains the research exemption under the Act described above.

Third, it is unclear from the wording of the exemption whether it would apply only to the initial disclosure by the hospital of the patient's health information to the researcher, thus requiring the researcher to apply separately for an exemption for subsequent disclosures. Presumably, the application by the hospital for the initial exemption could anticipate subsequent disclosures, but this is not certain.

To Whom Will the Act Apply and When?

To encourage the harmonization of provincial and federal privacy laws, the application of the Act will take place in three stages. On January 1, 2001, the Act will apply to private sector federal works and undertakings, and to businesses or organizations that disclose personal information across provincial borders for "consideration" (i.e., some type of financial payment or other form of benefit) in the course of commercial activities. Therefore, the Act will not apply to hospitals at the first stage of implementation, except for those hospitals that are engaged in the disclosure of personal information outside of their chartering province for consideration,

While it is unlikely that hospitals will be engaged in cross-border disclosures of information for consideration, it is possible that some information disclosures by hospitals to researchers participating in industry-funded research may be caught at this first phase of implementation. Any such disclosures of personal information made by the hospital without the patient's consent that cross provincial or national borders (for example, as part of a multicentre trial where the industry sponsor is outside the hospital's province of jurisdiction) may be caught at this first phase of implementation.

On January 1, 2002, the Act will apply to personal health information that federally regulated entities collect, use or disclose in the course of commercial activities. Because hospitals are not federally regulated entities, the Act will not apply to hospitals at the second stage of implementation.

Finally, on January 1, 2004, the Act will apply to all private sector entities that collect, use or disclose personal information in the course of commercial activities, if the province that has the jurisdiction to regulate the business has failed to enact legislation that is "substantially similar" to this Act. Therefore, the Act will not apply to public hospitals until January 1, 2004, and then only in respect of their commercial activities, with the exception of hospitals that are trading in personal information for consideration across provincial or national borders.

Exemption for "Substantially Similar" Legislation

Whether or not the Act will eventually be of concern to provincially regulated organizations depends upon whether the provinces act before January 1, 2004, to pass legislation similar to the Act for commercial activities within the jurisdiction. To date, only Quebec has passed substantially similar legislation. (The Minister of Industry indicated that An Act Respecting the Protection of Personal Information in the Private Sector, S.Q. 1993, c. 17, satisfies the "substantially similar" criterion; see Senate Standing Committee 1999, at 20 on-line.)

In addition to the general exemption for "substantially similar" legislation, the federal cabinet could also grant an exemption to those health service organizations subject to the Act whose information practices are governed by provincial

health information protection legislation. To date, the provinces that have comprehensive legislation of this kind are Manitoba, Saskatchewan and Alberta, although the legislation of the last two provinces has not yet been proclaimed in force (Personal Health Information Act, S.M. 1997, c. 51; Health Information Protection Act, S.S. 1999, c.H-O.021; Health Information Act, S.A. 1999, c. H-4.8). In Ontario, the Ontario Ministry of Health and Long Term Care is working on draft personal health information privacy legislation for the health sector. Whether health service organizations subject to this existing and proposed provincial health information privacy legislation will eventually be exempted from the application of the federal Act remains to be seen. It is important to note that even where such exemptions are granted, the federal Act will continue to apply to any disclosures of personal information across provincial and national borders.

How Should Hospitals Respond to the Federal Act?

With all of this provincial legislative activity underway, and with three years to ramp up for the general application of the Act to provincially regulated organizations, what steps should hospitals be taking now to deal with the Act?

- First, information officers should familiarize themselves with the general framework and application of the Act. To this end, this article should be of some assistance. Readers may also wish to consult the Industry Canada website.
- Second, hospitals that have not already done so, should now take steps to identify and record all public-private sector information and data flows that may cross provincial and national borders. Any hospital that is concerned that it may be involved in such cross-border commercial exchanges so as to be caught on the January 1, 2001 implementation should consult with legal counsel.
- Third, information officers should closely monitor the legislative initiatives underway in their province to bring in substantially similar privacy legislation. If it does not appear within the next year that your province will be moving in this direction, then a more comprehensive strategy will have to be developed to prepare for the general application of the Act on January 1, 2004.

In summary, while it is important that hospitals adopt a thoughtful strategy in order to respond to the Act, it is also important that hospitals not overreact. The framework for privacy legislation will likely change in many provinces before the January 1, 2004, general application date – in which case, hospitals in these provinces will happily be spared from having to deal with the federal Act as the primary piece in the privacy framework. HQ

References

Doray, Raymond. 2000. "The Implications of Bill C-54 on Medical Information: An Analysis of the Submission to the House of Commons Standing Committee on Industry by the Ontario Ministry of Health Concerning Bill C-54 (Personal Information and Electronic Documents Act)." Available on-line at http://ecom.ic.gc.ca/english/privacy/632d30.html.

McNairn, Colin H.H. and Alexander K. Scott. 2000. *A Guide to the Personal Information Protection and Electronic Documents Act.* Toronto: Butterworths.

Model Code for the Protection of Personal Information: A National Standard of Canada. 1996. Etobicoke: Canadian Standards Association, CAN/CSA-Q830-96.

Senate. Standing Committee on Social Affairs, Science and Technology. 1999. Issue no. 5 (December 2). Available on-line at http://www.parl.gc.ca/36/2/parlbus/commbus/senate/com-e/soci-e/05ev-e.htm.

Pamela Spencer is a corporate lawyer with the firm of Fraser Milner Casgrain specializing in hospital and health law. Pamela is currently completing her Masters of Health Sciences in Health Administration/Collaborative Program in Biomedical Ethics at the University of Toronto. You may contact her at pamela.spencer@fmc-law.com.