

New Federal and Provincial Personal Information Protection Legislation and its Impact on Physicians and Public Hospitals

Evguenia Prokopieva†

Introduction

Protection of personal information has become one of the most debatable issues in legal literature. Rapidly developing technologies make it increasingly easy to combine publicly available personal data from various sources and use that information equally for beneficial or detrimental purposes. Along with technological changes, the enactment of the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA)¹ and provincial personal data protection legislation² has also contributed to these debates.

Maintaining control over one's personal health information in particular has been hotly disputed, due to the inherent sensitivity of our medical records.³ Many would argue that because of the nature of personal health information, its protection is fundamental to the health care system and should be the default option as opposed to public disclosure or disclosure to those who are not the subject.⁴

The focus of this article is to examine the implications of the new federal and Ontario personal data protection legislation for physicians and public hospitals. This article also inquires into whether the new legislation will contribute to the protection of patient privacy. By "physician" I mean a doctor in a broad sense – i.e., "a person who has been educated, trained, and licensed to practice the art and science of medicine".⁵ This will include family doctors, pediatricians, psychiatrists, surgeons, and other medical doctors covered by the *Regulated Health Professions Act*.⁶ By the term "public hospitals" I will refer to not-for-profit hospitals as they are defined by the *Public Hospitals Act*.⁷

The first part of the article will examine the interrelationship between the personal data protection legislation and existing standards for physicians. The second part will analyze PIPEDA and its implications for doctors and public hospitals. Lastly, I will analyze the new Ontario legislation designed to protect personal information in the context of health care and treatment.

Interaction between Federal and Provincial Personal Information Protection Legislation and Standards Existing in Other Sources

PIPEDA was enacted in 2000. Since January 1, 2004, it has been in full force and effect. A number of provinces have enacted their own personal data protection legislation, whether general or sectoral. Ontario is one of the provinces that has concentrated on protection of personal health information. The new Ontario *Personal Health Information Protection Act* (PHIPA)⁸ came into force on November 1, 2004.

Before embarking on a discussion about implications of PIPEDA and PHIPA for doctors and public hospitals, I will explore a more basic issue. Is there even a need for new legislation protecting personal health information? What is the relationship between the federal and provincial personal information protection legislation, on one hand, and standards for health care professionals set out by common law and specialized provincial statutes such as the *Health Care Consent Act*,⁹ and professional codes such as the *Canadian Medical Association's Code of Ethics*,¹⁰ on the other hand?

One may argue that standards set by common law, provincial statutes, and professional codes for physicians are so high that the adherence to those standards will automatically lead to compliance with the requirements of the new personal information protection legislation, and both PIPEDA and PHIPA represent an attempt to impose on public hospitals and physicians redundant obligations amounting to an unnecessary paperwork. Indeed, some health care representatives take the view that

... the application of PIPEDA in the medical system will introduce significant impediments to the delivery of health care services, while providing virtually no substantive improvements to patient confidentiality over existing laws. ... [T]he medical profession in Ontario is bound by a clear and concise set of rules with respect to patient confidentiality, as found in the *Medicine Act*, the *Health Care Consent Act*, and augmented by the *CMA Code of Ethics*.¹¹

†© CCH Canadian Limited. The author wishes to express her gratitude to the Centre of Innovation Law and Policy of the University of Toronto for its support of this article. The author also wishes to thank Professor Margaret Ann Wilkinson of the Faculty of Law of the University of Western Ontario for her invaluable support and comments.

The argument, however, does not stand. First, the existing common-law standards of care and rules of professional conduct for medical practitioners are not designed to protect personal health information. Rather, they play the role of ensuring a relationship of trust between doctors and their patients and set rules of professional conduct. The confidentiality of information disclosed in the course of diagnoses and treatment is certainly a significant part of both trust relationships between doctors and their patients and rules of professional conduct. Protection of individuals' confidentiality and privacy is also a purpose of the new legislation. The new legislation, however, has other objectives which cannot be achieved by the existing standards. For example, PHIPA purports not only to protect the confidentiality of personal health information and the privacy of individuals with respect to that information, but also to provide individuals with a right of access to their personal health information and a right to require the correction or amendment of that information.¹² Thus, not only is the new personal data protection legislation designed to guard personal health information, but it also provides for protection of a broader spectrum of interests.

Second, the existing common-law standards of care and rules of professional conduct apply only to immediate health care providers (i.e., to physicians in the course of treatment of their patients). PHIPA, by contrast, applies to a wide range of entities, called health information custodians, which include not only physicians and other health care providers, but also all kinds of health care facilities, medical officers, pharmacies, and laboratories. In certain situations, the new Act applies to persons other than health information custodians. This ensures that personal health information is protected during "secondary uses" as well. In other words, the individual's privacy is protected not only within the trust relationship between him and his doctor, but also outside this relationship. This is true in relation to PIPEDA as well.

Technological advances and the specificities of the health care system make it necessary that dozens of people other than physicians (receptionists, lab technicians, etc.) have access to personal health information. The nature and extent of these persons' duties are not clear. Further, due to computerization of records, it is not always obvious who "holds" information and is, therefore, responsible for its protection.¹³ The new legislation tries to eliminate these difficulties. Both PHIPA and PIPEDA are broader than the existing standards of protection in their application. They not only codify rules found in common law and codes of professional conduct for physicians, but introduce new concepts and extend the requirements to supporting staff and other persons handling records of personal health information. In this respect, both pieces of legislation are a product of the evolving Canadian law accommodating the interests of individuals in today's technological environment. Both acts are designed to respond "to concerns raised by

the incomplete protection provided by the common law and intensified by technological developments".¹⁴ It is believed, therefore, that the new legislation will prevent situations such as where a patient's records forwarded to her treating physician by a laboratory show up on the back of flyers distributed in Toronto for a real estate company.¹⁵

Third, even if certain obligations under the new legislation appear to reiterate corresponding obligations under provincial health care-related statutes, common law, and rules of professional conduct, this appearance is in fact deceptive. Take, for example, the obligation to obtain consent. It is true that, under the existing standards, consent is central to the whole system of treatment. The right to decide whether a medical intervention will be accepted is an extension of one's fundamental right to bodily integrity and the concept of individual autonomy in general.¹⁶ In Ontario, the common-law rules on consent to treatment were codified by the *Health Care Consent Act*.¹⁷ However, consent to treatment by itself is by no means sufficient for the purposes of protecting personal health information. Under both PIPEDA and the new Ontario Act, the requirements of consent are broader. They cover not only consent to treatment itself but also consent to collect, use and disclose information provided by the patient for the purposes of treatment. This, again, demonstrates that the new legislation accords broader protection to individuals' privacy.¹⁸

It may well be, nevertheless, that physicians and public hospitals will use a single consent form to obtain consent to treatment and consent to the collection, use and/or disclosure of personal health information for the purposes of that treatment. The wording of such a form should be precise so that the patient is not confused. Theoretically, it is possible that the patient will give consent to treatment but refuses to give consent with respect to personal health information. In practice, however, this may mean that treatment will be impossible, for adequate treatment is premised on a full and free exchange of information between doctors and patients.

Fourth, the new personal data protection legislation equips patients with more ways of enforcing their rights. Failure to obtain a valid consent to treatment will result in a health care professional's liability for administering treatment without consent¹⁹ and may lead to an action in battery.²⁰ If consent was obtained but the requirement of adequate information is not met (i.e., consent was not informed), the patient may commence an action in negligence.²¹ The common-law actions may not always be effective because they are expensive and lengthy, or simply because the patient cannot satisfy all required elements of actions. Failure to obtain consent may also lead to a finding of professional misconduct on the part of a physician. Thus, "[p]erforming a professional service for which consent is required by law without consent" and "[g]iving information concerning the condition of a

patient or any services rendered to a patient to a person other than the patient or his or her authorized representative except with the consent of the patient or his or her authorized representative or as required by law” constitute acts of professional misconduct²² for the purposes of the *Health Professions Procedural Code*²³ and may result in disciplinary actions against the physician.²⁴ However, these provisions do not capture situations of unauthorized collection, use, or disclosure of personal health information as they arise in the context of personal data protection in the era of new technological developments. Rather, they are intended to cover cases of administering treatment without consent and divulging information about a patient’s condition and treatment to persons other than the patient (e.g., spouses, children, etc.).

On the other hand, under PIPEDA or PHIPA, failure to obtain a valid consent to collect, use or disclose one’s personal health information will lead to a health information custodian’s liability for the collection, use or disclosure of an individual’s information without consent. Certainly, neither PIPEDA nor PHIPA protects patients from physicians’ professional malpractice. Both Acts, however, broaden remedies available to the patients in situations of misuse of their personal health information. In cases where the common law or disciplinary actions are ineffective, the patients may well rely on provisions of the new legislation. Moreover, according to PHIPA, if the Ontario Information and Privacy Commissioner makes an order under this Act, or if a person is convicted of an offence under this Act, an individual affected by the order or conduct that gave rise to the offence may commence a proceeding in the Superior Court of Justice for damages for actual harm that this individual has suffered as a result of a contravention of the requirements of PHIPA.²⁵

Finally, PHIPA contains various provisions specifying changes and amendments that should be made to other provincial statutes. It is further provided that in the event of a conflict between a provision of PHIPA or its regulations and a provision of any other Act or its regulations, PHIPA and its regulations will prevail.²⁶ The new Act will not take priority only if it is specifically provided for. This suggests that it is the intention of the drafters that the new Ontario Act and other relevant statutes be consistent with each other and operate together, regulating different aspects of the health care practitioners’ and hospitals’ activities with respect to the collection, use and disclosure of personal health information so as to ensure a better protection of patient privacy.

Therefore, it is submitted that the new legislative regime is not redundant. Rather, it is designed to both further and enhance protection of patient privacy in the modern technological environment. In the next section, I will describe how physicians and public hospitals are influenced by PIPEDA and PHIPA.

PIPEDA and its Potential Impact on Physicians and Public Hospitals

Applicability of PIPEDA in General

It is more than a year since PIPEDA has been in its full force and effect. This means that the federal regime for the protection of personal information in the private sector now applies to all works, undertakings and businesses, whether federal or provincial, with respect to collection, use, and disclosure of personal information in the course of commercial activities.²⁷

The application of PIPEDA to organizations engaged in commercial activities depends on whether the latter involve inter- or intra-provincial dealings. In case of inter-provincial dealings, the Act applies irrespective of the presence or absence of an analogous provincial scheme, whereas in case of intra-provincial dealings, the Act applies unless the existing counterpart provincial personal data protection law (whether general or sectoral) meets the “substantially similar” test.²⁸

“Substantially Similar” Test

A provincial personal data protection law is deemed to be “substantially similar” to PIPEDA if it is “equal or superior to” the latter in the degree of quality of personal information protection offered.²⁹ If such is the case, the Governor in Council will issue an Order in Council exempting an organization, an activity or a class of organizations or activities from compliance with the requirements of PIPEDA to the extent that the latter applies within the provincial boundaries.³⁰

The criteria established by the Minister of Industry, through which the federal government will determine if the “substantially similar” test is met, set out certain requirements for provincial legislation. “Substantially similar” provincial/territorial legislation will be expected to:

- incorporate the ten principles in Schedule 1 (*Section 5*) of the PIPEDA, Principles set out in the National Standard of Canada entitled *Model Code for the Protection of Personal Information* ... The principles are accountability, identifying purposes, consent, limiting collection, limiting use, disclosure, and retention, accuracy, safeguards, openness, individual access, challenging compliance. These principles represent a well-established consensus on what is necessary to protect privacy in the contemporary social and technological environment. The ten principles are interrelated, make reference to one another and should be read together. They do not have to be enumerated distinctly and separately in substantially similar legislation – what is important is that they all be represented. Special

emphasis will be placed on the principles of consent, access and correction rights.

- provide for an independent and effective oversight and redress mechanism with powers to investigate . . .
- restrict the collection, use and disclosure of personal information to purposes that are appropriate or legitimate. The *Personal Information Protection and Electronic Documents Act* restricts organizations to the collection, use or disclosure of personal information only for purposes that a reasonable person would consider appropriate in the circumstances. . . . Such a provision is meant to ensure that an individual can challenge illegitimate, unreasonable or inappropriate collections, uses, disclosures of their information. Substantially similar legislation will include some reference to the reasonableness and appropriateness of the purposes for which it authorizes the collection, use or disclosure of personal information.³¹

PIPEDA applies at present in Ontario by default. As was noted above, on November 1, 2004, the new Ontario Act – PHIPA – came into force. However, until this Act is deemed to be substantially similar to PIPEDA, the latter will apply to all sectors of commercial activities including those in the health sector. An announcement that the new Ontario Act will be declared substantially similar to PIPEDA has already been made.³² Nevertheless, even after the *Proposed Order* becomes effective, PIPEDA will continue to apply to commercial activities in sectors other than health care and, as far as the health care sector is concerned, to all commercial activities relating to the exchange of personal health information between provinces and territories and to information transfers outside of Canada.³³

Before going on to discuss the interrelationship between PIPEDA and PHIPA, I will briefly review the development of personal information protection legislation in Canada and possible questions about the constitutional validity of PIPEDA.

Historically, Quebec was the first province to enact a law covering issues of the protection of personal information in the private sector.³⁴ In November 2003, Quebec's private sector personal data protection law was deemed substantially similar to PIPEDA by the federal government and the whole province was exempted from the application of the federal Act.³⁵ More recently, in January 2004, general laws on personal data protection in British Columbia³⁶ and Alberta³⁷ came into force. On April 10, 2004, the federal government found the B.C. and Alberta statutes to be substantially similar to the federal statute.³⁸ In addition to developing general personal data protection legislation, provinces have been also engaged in preparing sectoral laws. Thus, Manitoba, Saskatchewan, and Alberta have developed specific legislation for personal health information.³⁹

As PIPEDA in general, and its application to the health care sector⁴⁰ in particular, "raises questions about the division of powers between the federal and provincial governments in this field",⁴¹ it was foreseeable that the constitutional validity of the Act would be challenged.⁴² PIPEDA is indeed being challenged now. On December 17, 2003 (i.e., a month after the *Exemption Order*⁴³ was issued), the Government of Quebec obtained an order from the Quebec Court of Appeal allowing it to proceed with a constitutional challenge to PIPEDA.⁴⁴ The Quebec Court of Appeal will be asked to answer the question whether PIPEDA is *ultra vires* the federal government.

Quebec takes the position that "the very fact that PIPEDA requires a provincial law to be excluded from the purview of PIPEDA (if PIPEDA is not to apply within a province) implies that the federal government has the right to oversee the content of provincial legislation" on the protection of personal information which is "incompatible with the foundations of Canadian federalism".⁴⁵ It is anticipated that other provinces may join Quebec in this constitutional battle, and that, if the Quebec Court of Appeal answers the question posed in the affirmative, an appeal to the Supreme Court of Canada will follow. Hence, the constitutionality of PIPEDA may be an uncertain issue for several years.⁴⁶

Leaving a further detailed examination of the constitutionality of PIPEDA outside the scope of this article, I will now turn back to Ontario's PHIPA and its interrelationship with the federal Act. When the *Proposed Order*⁴⁷ becomes effective, PIPEDA will not apply to Ontario physicians' and public hospitals' intra-provincial commercial dealings.

When the criteria set out by the federal government for determining substantial similarity are applied to the new Ontario piece of legislation, the latter clearly meets the test to be exempted from PIPEDA. All of the 10 principles⁴⁸ are reflected in PHIPA: there are provisions on consent,⁴⁹ accountability,⁵⁰ openness,⁵¹ security,⁵² and accuracy,⁵³ as well as restrictions on the collection, use and disclosure of personal health information.⁵⁴ The requirement for the independent and effective mechanism of review, investigation and redress is also met, for PHIPA contains detailed provisions on administration and enforcement.⁵⁵ Further, "[i]t is not required that provincial laws are modeled precisely upon PIPEDA in order to be considered substantially similar".⁵⁶ The federal Act "... affords provinces/territories the flexibility to adopt and tailor their own private sector legislation to the specific needs and conditions of their jurisdiction while meeting the intent of [PIPEDA] ..."⁵⁷ The Act is "not trying to prescribe in detail what provinces need to do ..."; rather, it sets "the general standard, and the provinces can legislate around it".⁵⁸ Finally, it is possible that even sectoral provincial legislation may meet the "substantially similar" test.⁵⁹ All these considerations must have been taken into account when the federal

government declared its intention to deem PHIPA substantially similar to PIPEDA. In addition, because of the pending constitutional challenge, the federal government may have been more willing to find a compromise with the province.

It should be noted, however, that there are some differences between PHIPA and PIPEDA. In particular, the provincial Act takes a more expansive approach to cases of permitted disclosure of personal health information. Thus, according to section 46, a health information custodian⁶⁰ shall, upon request of the Minister of Health and Long-Term Care, disclose to the latter personal health information about an individual for the purpose of monitoring or verifying claims for payment for health care funded wholly or in part by the Ministry. This information may, however, be disclosed by the Minister to “any person for a purpose set out” in subsection (1) only “if the disclosure is *reasonably necessary* for that purpose”.⁶¹

As well, under section 47, the Minister is entitled to approve a health data institute and to request the custodian to disclose personal health information to that institute for analysis with respect to the management, evaluation or monitoring of the resources, their allocation or planning for the health system. The rights of the Minister under this provision are not, however, overreaching. First, the Minister is required to submit the proposal to the Ontario Information and Privacy Commissioner before requesting the disclosure so that the Commissioner can review and comment on the proposal.⁶² In reviewing the proposal the Commissioner must take into consideration the public interest in conducting the analysis and the privacy interests of the concerned individuals.⁶³ Any comments made by the Commissioner must be considered by the Minister.⁶⁴ Second, a health data institute, to be approved by the Minister for the purposes of the disclosure, must possess certain qualities. In particular, it must have in place practices and procedures approved by the Commissioner to protect the privacy of the individuals whose personal health information it receives.⁶⁵ Third, the institute that receives personal health information must follow certain steps in dealing with this information. For example, the institute must de-identify⁶⁶ the information in question; it can disclose the information to the Minister or those approved by the Minister only in a de-identified form; it cannot disclose the information to persons other than the Minister or those approved by the Minister even in a de-identified form.⁶⁷

To conclude on PHIPA’s provisions related to disclosure of personal health information, even though the provincial Act provides for more situations when the information can be disclosed, as was shown above, it puts reasonable restrictions on disclosure. Hence, there is no surprise that the expectations that the federal government exempt provincial health care providers from also having to comply with PIPEDA⁶⁸ will soon be satisfied. In the meantime, however, PIPEDA remains in effect,

and it is important to point out some of its implications for physicians and public hospitals.⁶⁹

What is “Commercial Activity”?

The next question to be explored is what “commercial activity” in PIPEDA is. “Commercial activity” has a broad statutory definition under subsection 2(1) of the federal Act:

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.

Thus, the inquiry is not only about the nature of the organization in question but also about the nature of the one particular transaction. As a result, any not-for-profit organizations, including public hospitals, may be caught by this definition with respect to a certain transaction. Accordingly, public hospitals ought to be cognizant of whether any of their activities are likely to be considered commercial within the meaning of the federal statute. Depending on that, they may have to comply with the requirements under PIPEDA.

It has been suggested that PIPEDA does not extend to core activities of public hospitals.⁷⁰ As to what constitute “core activities”, it has been commented that an institution’s “core activities” are the activities defined either in a provincial statute regulating that particular industry or in the legal entity’s corporate constitution.⁷¹ It follows then that core activities of public hospitals include care and treatment.⁷² In order to determine what is covered by “care” and “treatment” as core public hospital activities, provincial health care-related legislation and specialized medical dictionaries are of some assistance. “Health care” means “any observation, examination, assessment, care, service or procedure that is done for a health-related purpose” and that is carried out or provided to diagnose, treat or maintain an individual’s physical or mental condition, to prevent disease or injury or to promote health, or as part of palliative care.⁷³ “Care” may include “not only the traditional care of the acutely or chronically ill patient, but also the prevention and early detection of disease and the rehabilitation of the disabled”.⁷⁴ On the other hand, “treatment” means “anything that is done for a therapeutic, preventive, palliative, diagnostic, cosmetic or other health-related purpose”.⁷⁵ It includes “the maintenance, observation, medical care and supervision and skilled nursing care of a patient”.⁷⁶ Generally “treatment” can be defined as medical or surgical management of a patient.⁷⁷

The federal government takes the position that “[t]he funding source (public health insurance, private payer, third party payer, etc.) is not relevant in determining the existence of a commercial activity”.⁷⁸ On this view, the Act does not apply to the core activities of public hospitals, not because they are provincially funded but because they are “beyond the constitutional scope of the Act as their core activities are not commer-

cial in nature”.⁷⁹ Therefore, charging for a private room, for instance, would not make a public hospital subject to PIPEDA, for such a transaction is part of the hospital’s core activities (i.e., providing accommodation for care and treatment).⁸⁰ On the other hand, certain limited public hospital activities may be covered by PIPEDA. For instance, while PIPEDA does not apply to public hospital fundraising activities, such dealings as sales of donor lists may be caught by the Act.⁸¹

It can be argued that the conclusion that at least core activities of public hospitals do not fall within the scope of “commercial activities” under PIPEDA is supported by the rules of statutory interpretation. The rules mandate courts to consider not only the ordinary meaning of words, but also the context and the purpose of the statute in question.⁸² In particular, when PIPEDA is read with a view to its context and purpose, the courts should take into account the legislative history of the Act and the original intent of its drafters. It is a fact of the legislative history that the health care sector did not participate in the drafting of the *Model Code for the Protection of Personal Information*⁸³ containing the ten principles now deemed by the Act as essential for the protection of personal information and, thus, incorporated directly into the Act.⁸⁴ As a result, the Act was prepared without specific consultation with the health care sector.⁸⁵ Furthermore, developed in connection with the federal government’s interest in trade and commerce, PIPEDA was not originally intended to be applicable to the health care sector.⁸⁶ The application to the health care system appears to be an “incidental” or “ancillary” result of the legislative drafting.⁸⁷

Turning back to the definition of the term “commercial activity”, it should be emphasized that its scope in the context of PIPEDA will remain unclear until the courts provide guidance through their decisions on the application of PIPEDA. So far, there has not been any case law directly relevant to the issue of the meaning of the term in the context of PIPEDA. Given, however, the courts’ willingness to read down the broad language in PIPEDA,⁸⁸ it is reasonable to expect that the judiciary will take a restrictive view on the interpretation of “commercial activity” as well. In *Ferency v. MCI Medical Clinics*,⁸⁹ for instance, the Court held that although a private investigator’s videotape contained personal information about the plaintiff collected without her consent and thus, arguably, obtained and disclosed contrary to PIPEDA, it was still admissible evidence at trial, for its probative value outweighed its possible prejudicial effects. The Court even went on to suggest that the obtaining and the proposed use of the videotape at trial did not breach PIPEDA at all. The Court employed the concept of agency to find that the private investigator was acting as an agent of the defendant physician and, therefore, the Act did not apply in this situation because the defendant was collecting the said personal information not in the course of commercial activities but for the purpose of defending himself in a legal proceeding.

This decision demonstrates that the courts may use various interpretative techniques to restrict the application of PIPEDA to “the traditional areas of commerce, focusing on direct contact between businesses and their customers and potential customers”.⁹⁰ It also suggests that the courts will look at the purpose of the collection, use or disclosure of personal information to determine whether the information in question was collected, used or disclosed in the course of commercial activities.

Further, the term “commercial activity” has been interpreted by courts in the context of other legislation (e.g., in the context of income tax and state immunity laws).⁹¹ Accordingly, it has been proposed to interpret the term “commercial activity” in the context of PIPEDA with the assistance of tests developed by case law, albeit in a different setting. For example, health care sector representatives have recommended the application of the so-called “primary aim” or “preponderant purpose” test, which means that an organization’s activity is considered to be commercial so long as its primary purpose is “making a pecuniary gain for the personal benefit of its members, as opposed to recovering its costs or promoting its philanthropic, charitable, scientific, health or other like object”.⁹² In *Re Regional Assessment Commissioner and Caisse Populaire de Hearst Ltee.*,⁹³ the Supreme Court of Canada adopted the “preponderant purpose” test to determine whether an entity was carrying on a business and, thus, subject to a business tax. The test is essentially based

... upon a consideration of whether the activity concerned is carried on for the purpose of earning a profit or for some other preponderant purpose. If the preponderant purpose was other than to make a profit, then even if there were other characteristics of the organization, including an intent in some cases to make a profit . . . , it would not be classed as a business.⁹⁴

Since “carrying on a business” and “being engaged in a ‘commercial activity’” have a very close meaning, I would argue that the “preponderant purpose” and “primary aim” tests are based on analogous considerations and, thus, can be employed by the courts while interpreting the definition of “commercial activity” in PIPEDA. The Court’s “purposeful” analysis in *Ferency v. MCI Medical Clinics* seems to support this argument.

There is little doubt that PIPEDA covers private labs,⁹⁵ private pharmacies,⁹⁶ and other for-profit private health care facilities,⁹⁷ as their activities are clearly “commercial”⁹⁸ in nature.⁹⁹ It is not certain, however, to what extent the Act applies to physicians. Due to the specificity of the structure of the Canadian health care system, which is generally described as “publicly funded yet privately delivered,”¹⁰⁰ Canadian physicians are private for-profit contractors.¹⁰¹ They enter into contracts “with provincial governments through their provincial medical associations to supply publicly funded health services to Canadians”.¹⁰²

As was already noted above, the fact that the services are publicly funded is not relevant in determining

whether they can be treated as non-commercial. Indeed, the same physician can deliver services both covered and not covered by provincial health plans. For instance, a dermatologist can perform on the same patient and at the same time two operations: the removal of a carcinoma which is publicly funded and a cosmetic surgery which is not publicly funded.¹⁰³ It is absurd in this situation to require a treatment record be in compliance with two different regimes just because the operations involved have different funding sources. It has been suggested, therefore, by commentators,¹⁰⁴ as well as by health care sector representatives¹⁰⁵ that most physicians fall under the jurisdiction of PIPEDA. Only physicians “employed by a government body or a non-profit agency (e.g., a public hospital) that does not sell goods or services”¹⁰⁶ are thought to be exempt from the Act. The majority of physicians – i.e., those who have private offices and/or enjoy privileges at public hospitals and other health care facilities¹⁰⁷ – would be expected to comply with the personal information protection rules set out in PIPEDA.

To conclude the discussion on the applicability of PIPEDA, it appears the best view is that the Act does not apply to the core activities of public hospitals and services delivered by physicians employed by the latter, whereas physicians having private offices or privileges at hospitals are engaged in commercial dealings that will be subject to the Act. Recent case law lends support to expectations that PIPEDA will be interpreted narrowly. If provincial personal data protection legislation is deemed to pass the “substantially similar” threshold, or PIPEDA is declared inoperative due to its constitutional invalidity, all public hospital activities and all types of physicians (along with private health care facilities, labs, etc.) will in consequence be free from application of this federal Act. Unless PIPEDA becomes inapplicable, physicians (with the exception of those employed by public hospitals)¹⁰⁸ will need to comply with it. A discussion of the requirements for compliance follows below.

Procedures Required under PIPEDA

First of all, physicians must have free and informed consent from individuals to collect, use, and disclose their personal health information.¹⁰⁹ “Personal health information” is a defined term which means

information concerning the physical or mental health of the individual; information concerning any health service provided to the individual; 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; 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.¹¹⁰

For the purposes of the following discussion, personal health information will be treated as a subset of personal information.

Under section 7 of the Act, no personal information can be collected, used or disclosed to third parties without the knowledge or consent of the individual. There are, however, some exceptions to this general principle. One of them, relates to use and disclosure without knowledge or consent for the purposes of statistical, or scholarly study or research, provided that: *first*, these purposes cannot be achieved without using or disclosing the information; *second*, the information is used or disclosed in a manner that will ensure its confidentiality; *third*, it is impracticable to obtain consent; and *fourth*, the organization informs the Commissioner of the use or disclosure beforehand.

This exception may be relevant to physicians conducting health research in the course of their patients’ treatment. The scope of this exemption has yet to be clarified. Nevertheless, it can be argued that if the court agrees that “[a]ny *bona fide* health research, undertaken by legitimate organizations¹¹¹ under appropriate safeguards, will . . . constitute ‘statistical or scholarly study or research’ even if there is an element of pecuniary interest involved”,¹¹² physicians will not need patients’ consent in order to use and disclose personal health information for the purposes of health research. Consent will still be necessary though for the collection of such information. It should also be stressed that to be able to rely on the scholarly research exception, physicians will have to follow the conditions set out above.

Further on the issue of consent, the requirements in Principle 4.3 of Schedule 1 to the Act must be met. Patients must be advised of the purposes of collection, use and disclosure of the information, taking into account the patients’ reasonable expectations.

In addition to the procedures related to the issue of consent, doctors, as organizations¹¹³ responsible for personal information under their control, must put in place other procedures so that the rest of the principles in Schedule 1, such as accountability, identified purposes, limited collection, use, disclosure, and retention, accuracy, security, and openness, are complied with.

Doctors must also ensure that patients have access to their personal health information. Access can be denied in limited circumstances: if doing so would likely reveal personal information about a third party, if the information is protected by the solicitor–client privilege, if to give access would reveal confidential commercial information or could reasonably give rise to threatening the life or security of other individuals.¹¹⁴ If however, the information can be severed, access must be given after severing.

To help physicians cope with the new situation, the College of Physicians and Surgeons of Ontario has provided health practitioners with some guidance as to what practical measures must be implemented in order to safeguard personal health information in the manner

prescribed by the federal law. For example, it has been suggested that doctors implement

physical measures (e.g., restricted access areas, locked filing cabinets), organizational measures (e.g., need-to-know and other employee policies, security clearances), and technological measures (e.g., passwords, encryption, virus protection, firewalls).¹¹⁵

There are also recommendations with regard to the location and transfer of paper and electronic information, education of staff, review of agreements with consultants and contractors, and so forth.¹¹⁶

If the provisions of PIPEDA imposing obligations to protect personal information are contravened, an affected individual may file a complaint with the office of the federal Privacy Commissioner.¹¹⁷ If there are reasonable grounds to investigate the matter, the complaint may be initiated by the Commissioner.¹¹⁸ In respect of all complaints, whether filed by individuals or initiated by the Commissioner, proper investigations must be conducted.¹¹⁹ Unless the Commissioner is satisfied that it is more reasonable or appropriate that the complaint is dealt with by other means, she must issue a report containing findings, recommendations or requests to the organization whose practices have been under investigation.¹²⁰ After receiving the Commissioner's report, the complainant, if not satisfied with the result, may further apply to the court¹²¹ which, in addition to any other remedies available in law generally, may order the organization to correct its practices, as well as award damages to the complainant, including damages for any humiliation suffered.¹²²

Having outlined the main obligations imposed on physicians by PIPEDA, I will continue my analysis by looking at the new Ontario legislation and its possible effects.

Impact of PHIPA

PHIPA is an example of sectoral provincial personal data protection legislation. As was noted above, apart from Ontario, there are three other provinces – Alberta, Manitoba, and Saskatchewan – which have enacted statutes related to the protection of personal health information. None of these Acts has been declared to be substantially similar to PIPEDA. However, all three statutes – Alberta's *Health Information Act*,¹²³ Manitoba's *Personal Health Information Act*,¹²⁴ and Saskatchewan's *Health Information Protection Act*¹²⁵ – “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”.¹²⁶ PHIPA, on the other hand, is clearly an Act designed to enhance protection of patient privacy and due to this the federal government has already announced that the new Ontario law will be deemed to be substantially similar to PIPEDA in the nearest future.¹²⁷

Application

According to section 7 of PHIPA, the statute applies to:

- (1) the collection of personal health information by a health information custodian;
- (2) the use or disclosure of personal health information by a health information custodian or any other person, to whom the information has been disclosed by the custodian;
- (3) the collection, use or disclosure of a health number by any person.

Thus, as far as personal health information is concerned, PHIPA is intended to apply primarily to health information custodians in the course of collection, use and disclosure of such information. PHIPA also has a very limited application to non-custodians when the latter use or disclose personal health information disclosed to them by health information custodians. The new legislation applies to the use and disclosure of the personal health information even if collected before enactment.¹²⁸ Further, the new Act applies to any personal health information collected, used or disclosed by a health information custodian, or used or disclosed by any other person, regardless of whether the custodian or the person in question is engaged in commercial activities.

The term “health information custodians” refers to persons who have custody or control of personal health information as a result of or in connection with their work, powers or duties, and includes a variety of individuals and organizations from health care practitioners to all types of hospitals.¹²⁹ Clearly, physicians and public hospitals, which have been the focus of this article, are covered by the definition of health information custodians.

A full and free exchange of information between health care practitioners, particularly physicians, and patients is a prerequisite for the provision of adequate care and treatment. It will be impossible to either diagnose or treat “if the physician does not have all the necessary information” about the patient.¹³⁰ Most of this information is personal. Every time the patient goes to see her doctor, the doctor collects patient's personal health information (e.g., symptoms, family predispositions to certain illness, habits, etc.). The information collected invariably needs to be used and disclosed in order to provide the patient with adequate therapeutic relief (e.g., referrals to specialists or specific procedures such as blood tests, ultrasound, X-rays, etc.). Hence, virtually all health care-related activities are covered by PHIPA, and it is critically important for all physicians and public hospitals to be aware of the new Ontario Act's implications.

Procedures Established by PHIPA

Administrative Obligations

Part II of the Act¹³¹ imposes certain duties on health information custodians. First, there are a number of administrative requirements. Each health information custodian must have in place information practices, i.e., policies in relation to the collection, use and disclosure of personal health information, which include the administrative, technical, and physical safeguards.¹³² There are special rules on the handling of records.¹³³ Health information custodians must appoint an information officer, called “contact person”, who is required to act as the custodian’s agent to facilitate compliance with PHIPA and communicate with the public.¹³⁴ The custodians must also describe their information practices in a publicly available statement.¹³⁵ This statement must outline how to reach contact persons, obtain access to or request corrections of individual’s records, and make complaints. Each health information custodian must take steps to ensure accuracy¹³⁶ and security¹³⁷ of personal health information. Generally, if personal health information is stolen, lost, or accessed by unauthorized persons, a health information custodian must notify an affected individual at the first reasonable opportunity.¹³⁸

Consent Provisions

Further, PHIPA contains detailed provisions on consent and capacity to give consent to the collection, use or disclosure of personal health information.¹³⁹ Echoing PIPEDA, PHIPA provides that consent must be voluntary and knowledgeable. However, unlike PIPEDA, PHIPA establishes “more workable consent procedures for the collection, use and disclosure of personal health information”.¹⁴⁰ For instance, consent under PHIPA is “knowledgeable” if it is reasonable to believe that a person giving consent knows the purposes of the collection, use or disclosure of personal health information and that consent may be given and withheld.¹⁴¹ Unless it is not reasonable in the circumstances, it is presumed that the person knows the purposes of the collection, use or disclosure of personal health information if the custodian posts or makes readily available a notice describing the purposes where it is likely to come to the person’s attention or provides the person with such a notice.¹⁴²

Consent to the collection, use or disclosure of personal health information about an individual may be express or implied.¹⁴³ Consent to disclosure must be express in only two situations: first, when a health information custodian makes a disclosure to a person who is not a health information custodian and, second, when one health information custodian makes a disclosure to another health information custodian for purposes other than providing health care.¹⁴⁴ It follows then that in general terms, implied consent will be sufficient. To demonstrate implied consent, public hospitals and physicians can use “[a] poster or brochure readily available and likely to be seen by a patient”.¹⁴⁵

The legislation has been praised for the fact that not only can physicians assume implied consent for disclosure of personal health information to other health care

practitioners treating the patient, but they can also assume that a signed consent form relating to personal health information is valid.¹⁴⁶ However, consent can no longer be assumed to be “implied” if the custodian receiving the information is aware that the individual has expressly withheld or withdrawn the consent.¹⁴⁷ The fact that “the rules for substituted consent for information handling are very similar to those for substituted consent for treatment”¹⁴⁸ has been noted as being among the positive effects of PHIPA as well.

Permitted Disclosure

The new Ontario Act sets out special rules for situations when health information custodians are permitted to collect, use or disclose personal health information without individuals’ consent. These rules mainly correspond with analogous provisions in PIPEDA. As far as permitted disclosure is concerned, both PIPEDA and PHIPA provide, for instance, that information can be disclosed without knowledge or consent of the individual if it is prescribed, permitted or required by law.¹⁴⁹ Another example is the disclosure of personal health information to a researcher for the purpose of research, provided that certain conditions are met.¹⁵⁰ Generally, the imposed conditions are considered to be met if a Research Ethics Board has approved the researcher’s research plan and the custodian and researcher have entered into an agreement before the disclosure of personal health information in which the researcher agrees to comply with the statutory requirements on the use, security and disposal of the information in question.¹⁵¹ “Research” is defined in PHIPA as “a systematic investigation designed to develop or establish principles, facts or generalizable knowledge, or any combination of them, and includes the development, testing and evaluation of research”.¹⁵² This exception appears to be similar to the scholarly research exception under PIPEDA.

However, the provincial Act goes beyond the federal Act in that PHIPA, as was mentioned under the “‘Substantially Similar’ Test” section of this article, provides for more situations when personal health information is permitted to be disclosed without the patient’s consent. Thus, health information custodians are permitted to disclose the information to prescribed persons for purposes related to providing health care¹⁵³ and to eliminating or reducing risks of serious bodily harm;¹⁵⁴ for health or other programs¹⁵⁵ and for proceedings in which custodians or their agents are parties or witnesses;¹⁵⁶ for monitoring health care payments¹⁵⁷ and allowing potential successors to evaluate operations of custodians,¹⁵⁸ and for the analysis¹⁵⁹, planning and management of the health care system.¹⁶⁰ In all of these situations, the Act appears to put reasonable restrictions on disclosure so as to ensure that personal health information is not disclosed for inappropriate, unreasonable or illegitimate purposes.

Access

PHIPA gives patients a general right of access to records containing their personal health information in the custody and control of a health information custo-

dian.¹⁶¹ In certain cases, access can be denied. One such case is when granting of the access can reasonably be expected to result in a risk of serious harm to the patient's treatment or recovery.¹⁶² Such an exception to the general right of access to one's personal information is not provided for in PIPEDA.

Generally, health information custodians have thirty days to process a request.¹⁶³ In certain situations, this time period may be extended¹⁶⁴ or reduced.¹⁶⁵ If a health information custodian refuses or is deemed to refuse access, the individual has a right to make a complaint to the Commissioner.¹⁶⁶ Finally, custodians may charge individuals fees for access.¹⁶⁷ The amount of the fee is, however, limited to the prescribed amount or the amount of reasonable cost recovery, if no amount is prescribed.¹⁶⁸

Enforcement and Remedies

Part VI of the new Act outlines consequences of non-compliance with the requirements. They include complaints to the Commissioner,¹⁶⁹ reviews,¹⁷⁰ and inspections.¹⁷¹ The Commissioner under PHIPA is the Information and Privacy Commissioner of Ontario appointed in accordance with the *Freedom of Information and Protection of Privacy Act*.¹⁷² PHIPA enumerates powers of the Commissioner in relation to the protection of personal health information.¹⁷³ Generally, the Commissioner has powers to review complaints about contravention of PHIPA or initiate her own reviews and to make orders as a result of such reviews. Upon receiving the Commissioner's order, an affected individual may appeal the order to the Divisional Court on a question of law.¹⁷⁴ When the order becomes final as a result of there being no further right of appeal, the affected individual may commence a proceeding in the Superior Court of Justice for damages for breach of privacy and mental anguish.¹⁷⁵

Lastly, PHIPA provides for fines imposed on health information custodians and non-custodians, when the latter are within the reach of PHIPA, for contraventions of the Act.¹⁷⁶ Natural persons are liable, on conviction, to a fine of up to \$50,000, and organizations and corporations are liable, on conviction, to a fine of up to \$250,000.¹⁷⁷

To conclude on procedures under PHIPA, the obligations imposed by the new Ontario Act largely resemble those imposed by PIPEDA. Consequently, "most physicians who have developed privacy policies to comply with PIPEDA will only have to make minor adjustments to them as a result of PHIPA".¹⁷⁸ A close

examination of PHIPA reveals, however, that the discharge of the obligations under the new Ontario law aligns more with the needs and traditions of the medical profession than under PIPEDA. Most significantly, PHIPA provides for more workable provisions on consent. Thus, it can be argued that the new Ontario Act suits interests of the health care sector better and, therefore, should supercede the federal Act.

Conclusions

Obligations created under PIPEDA and PHIPA not only codify rules found in common law, but also go beyond that and introduce new concepts instigated by new technological developments.

Until the new Ontario Act is deemed to be substantially similar to PIPEDA, and as long as PIPEDA is not found to be constitutionally invalid, this federal Act applies in the provincial health care sector. While core activities of public hospitals are not covered by the definition of "commercial activity" in PIPEDA, activities performed by physicians in their private offices or in hospitals where they have privileges are commercial in nature and, thus, subject to PIPEDA. Physicians, with the exception of those employed by public hospitals, and, in extremely rare situations, public hospitals when engaged in other than core activities such as care and treatment, must comply with the obligations under PIPEDA.

As PHIPA applies to the whole health care sector, all health care practitioners, including physicians, and health care facilities and public hospitals need to follow rules established by the new Ontario Act. Due to the fact that the new Ontario Act meets all the criteria set out by Industry Canada, the federal government have already declared that PHIPA will be deemed substantially similar to PIPEDA. When the *Proposed Order* becomes effective, physicians and public hospitals in Ontario will be exempt from the reach of PIPEDA and, thus, will need to comply only with the requirements established by the provincial Act. In the meantime, compliance with both pieces of legislation is required.

Generally, obligations under PHIPA are similar to those under PIPEDA. The difference between the two Acts, in the author's opinion, is that PHIPA better meets the needs of the health care sector in Ontario, as it is tailored specifically for that purpose. The most significant advantage of PHIPA is that it provides for more workable provisions on consent.

Notes:

¹ Canada, S.C. 2000, c. 5 [PIPEDA].

² See e.g. British Columbia *Personal Information Protection Act*, S.B.C. 2003, c. 63; Alberta *Personal Information Protection Act*, S.A. 2003, c. P-6.5.

It appears to be a proper place here to draw a line between "privacy protection", on the one hand, and "personal information" or "personal data protection", on the other hand. Although they are closely interconnected, these phrases can be distinguished. Privacy "... may be defined as the right of the individual to determine for himself when, how, and to what extent he will release personal information about himself...": *R. v.*

Sanelli (sub nom. R. v. Duarte), [1990] 1 S.C.R. 30 at para. 27. Thus, "personal information" or "personal data protection" seems to be broader than "privacy protection". Personal information protection involves not only safeguards related to the right of an individual to decide whether "to release personal information about himself" and, if so, when, how, and to what extent to do that, but also rules on how this information can be collected, kept, used, and/or disclosed once the individual has decided to release it. While privacy protection concentrates on the subject's rights,

personal information/data protection adds to this by stipulating the procedures to follow for those who deal with the subject's personal information.

Therefore, "personal information" or "personal data protection" will be used in this article in relation to PIPEDA and analogous provincial legislation.

- ³ See, e.g., Brian Foran, "Privacy on the Information Highway: Myth or Reality?" Government Information in Canada, Vol. 2, No. 2.4 (1995), online: <http://www.usask.ca/library/gic/v2n2/foran/foran.html>; Barbara von Tigerstrom, "The 'Hidden Story' of Bill C-54: The Personal Information Protection and Electronic Documents Act and Health Information" (1999) 8 Health L. Rev. No. 2 13; Stephanie Perrin & Heather H. Black, *The Personal Information Protection and Electronic Documents Act: An Annotated Guide* (Concord, Ont.: Irwin Law, 2001) ch. 5, online: (QL).
- ⁴ See Jocelyn Downie & Thomas Caulfield, *Canadian Health Law and Policy*, 2nd ed. (Butterworths, 2002) at 157-158; Peter D. Jacobson, "Medical Records and HIPAA: Is It Too Late to Protect Privacy?" [2002] Minn. L. Rev. 1497 at 1499.
- ⁵ See the definition of "physician" in *Stedman's Medical Dictionary*, 27th ed. (Lippincott, Williams & Wilkins, 2000), online: (Westlaw).
- ⁶ S.O. 1991, c. 18.
- ⁷ R.S.O. 1990, c. P.40.
- ⁸ S.O. 2004, c. 3, Sch. A [PHIPA].
- ⁹ S.O. 1996, c. 2, Sch. A [*Health Care Consent Act*].
- ¹⁰ Online: CMA http://www.cma.ca/index.cfm/ci_id/2419/la_id/1.htm [CMA Code of Ethics].
- ¹¹ CPSO, "Concerns about Privacy Legislation: College Lobbies Government to Exempt Physicians" *Members' Dialogue* (September–October 2003), online: The College of Physicians & Surgeons of Ontario <http://www.cpso.on.ca/publications/dialogue/0903/registrar.htm>.
- ¹² PHIPA, *supra* note 8 s. 1.
- ¹³ See, e.g., Barbara von Tigerstrom, "Protection of Health Information Privacy: The Challenges and Possibilities of Technology" (1998) 4 Appeal 44 (QL) at para. 15.
- ¹⁴ *Ibid.* at para. 16.
- ¹⁵ Richard Steinecke, "Get Ready for Privacy Legislation in 2004" *Grey Areas* 60 (February 2003), online: Steinecke Maciura LaBlanc, Barrister & Solicitors <http://www.sml-law.com/pageDisplay.asp?webDocID=3403>.
- ¹⁶ See, e.g., *Ciarlariello v. Schacter*, [1993] 2 S.C.R. 119; *Starson v. Swayze*, [2003] 1 S.C.R. 722.
- ¹⁷ Downie & Caulfield, *supra* note 4 at 111, n. 1.
- ¹⁸ Some would argue, however, that this broader protection may come at the expense of the ability of researchers to access or use patient data.
- ¹⁹ *Health Care Consent Act*, *supra* note 9 s. 29.
- ²⁰ Downie & Caulfield, *supra* note 4 at 127.
- ²¹ Downie & Caulfield, *supra* note 4 at 127. See also *Reibl v. Hughes*, [1980] 2 S.C.R. 880, *Arndt v. Smith*, [1997] 2 S.C.R. 539; *Hollis v. Dow Corning Corp.*, [1995] 4 S.C.R. 634.
- ²² *Professional Misconduct*, O. Reg. 856/93, ss. 9-10. This regulation is enabled under the *Medicine Act*, S.O. 1991, c. 30.
- ²³ *Regulated Health Professions Act*, *supra* note 6, Sch. 2. The *Health Professions Procedural Code* is also deemed to be part of the *Medicine Act*, *ibid.* s. 2(1).
- ²⁴ *Health Professions Procedural Code*, *ibid.*, cl. 51.
- ²⁵ PHIPA, *supra* note 8, ss. 65(1) and (2).
- ²⁶ *Ibid.*, s. 7(2).
- ²⁷ PIPEDA, *supra* note 1, ss. 4.1(a) and (b).
- ²⁸ Canada, Department of Industry, *PIPEDA Awareness Raising Tools (PARTs) Initiative for the Health Sector: Questions & Answers – First Series*, question 2, online: <http://strategis.ic.gc.ca/epic/internet/inccic-ceac.nsf/vwGeneratedInterE/gv00211e.html> [PIPEDA Awareness Raising Tools].
See also PIPEDA, *supra* note 1, ss. 4(1) and 26(2)(b).
- ²⁹ See Canada, Privacy Commission, *Report to Parliament Concerning Substantially Similar Provincial Legislation* (May 2002), online: Privacy Commissioner of Canada http://www.privcom.gc.ca/legislation/leg-rp_e.asp [Report to Parliament].
- ³⁰ PIPEDA, *supra* note 1, s. 26(2)(b).
- ³¹ Canada, Department of Industry, *Personal Information Protection and Electronic Documents Act: Process for the Determination of "Substantially Similar" Provincial Legislation by the Governor in Council*, C. Gaz. Vol. 136 No. 31 2003.L2385 at 2388, online: *Canada Gazette* <http://canadagazette.gc.ca/part1/2002/20020803/pdf/g1-13631.pdf> [Process for the Determination of "Substantially Similar" Provincial Legislation]; see also Report to Parliament, *supra* note 29.
- ³² See the proposed order at *Health Information Custodians in the Province of Ontario Exemption Order* (5 February 2005), C. Gaz. Vol. 139, No. 6 2005.I.331, online: *Canada Gazette* <http://canadagazette.gc.ca/part1/2005/20050205/html/regle4-e.html#REFa> [Proposed Order].
- ³³ Ontario, Information and Privacy Commissioner, *Frequently Asked Questions: Health Information Protection Act* (28 October 2004), online: Ontario Information and Privacy Commissioner http://www.ipc.on.ca/scripts/index.asp?action=31&P_ID=15607&N_ID=1&PT_ID=11351&U_ID=0 [Frequently Asked Questions: PHIPA].
- ³⁴ *An Act Respecting the Protection of Personal Information in the Private Sector*, R.S.Q. 1994, c. P-39.1.
- ³⁵ *Organizations in the Province of Quebec Exemption Order*, P.C. 2003-1842 (19 November 2003), C. Gaz. Vol. 137, No. 25 2003.II.2830 at 2917, online: *Canada Gazette* <http://canadagazette.gc.ca/part1/2003/20031203/html/sor374-e.html> [Exemption Order].
- ³⁶ *Supra* note 2.
- ³⁷ *Ibid.*
- ³⁸ *Organizations in the Province of British Columbia Exemption Order* (10 April 2004), C. Gaz. Vol. 138, No. 15 2004.I.1125 at 1178, online: *Canada Gazette* <http://canadagazette.gc.ca/part1/2004/20040410/html/regle4-e.html>; *Organizations in the Province of Alberta Exemption Order* (10 April, 2004), C. Gaz. Vol. 138, No. 15 2004.I.1125 at 1174, online: *Canada Gazette* <http://canadagazette.gc.ca/part1/2004/20040410/html/regle3-e.html>.
See also Canada, Privacy Commission, *News Release: Federal, British Columbia and Alberta Commissioners Working Together to Ensure Seamless Privacy Protection in the Private Sector* (26 January 2004), online: Privacy Commissioner of Canada http://www.privcom.gc.ca/media/nr-c/2004/nr-c_040126_e.asp.
- ³⁹ *Personal Health Information Act*, S.M. 1997, c. 51; *Health Information Protection Act*, S.S. 1999, c. H-0.021; *Health Information Act*, R.S.A. 2000, c. H-5.
Note that since Alberta's *Personal Information Protection Act* has been deemed equivalent to PIPEDA, all organizations in this province including those in the health care sector other than federal works, undertakings or businesses are exempt from the application of Part I of the federal Act, regardless of whether or not Alberta's *Health Information Act* is considered substantially similar to PIPEDA.
- ⁴⁰ With respect to the regulation of the health care sector, it should be noted that the general parameters for funding of the Canadian health care system are established by the *Canada Health Act*, R.S. 1985, c. C-6 [Canada Health Act]. However, the administration of the system in general is within the provincial powers: *Constitution Act, 1867* (U.K.), 30 & 31 Vict., c. 3, s. 92, reprinted in R.S.C. 1985, App. II, No. 5.
See also Mark Weitz & Neil Drummond, "In Whose Interest? Current Issues in Communicating Personal Health Information: A Canadian Perspective" (2003) 31 J.L. Med. & Ethics 292.
- ⁴¹ Downie & Caulfield, *supra* note 4 at 173.
- ⁴² *Ibid.*
- ⁴³ *Supra* note 35.
- ⁴⁴ *Release: Reference to the Court of Appeal Relating to the Personal Information and Electronic Documents Act*, S.C. 2000, c. 5, online: Quebec Court of Appeal http://www.tribunaux.qc.ca/mjq_en/c-appel/order_in_council_release_19_february_20004.htm.
See also Quebec *Preparing Constitutional Challenge to PIPEDA* (24 January 2004), e-Alert 21, online: Stikeman Elliot <http://www.stikeman.com/newslett/EAlertIssue21b.htm> [Quebec Preparing Constitutional Challenge to PIPEDA].
- ⁴⁵ *Quebec Preparing Constitutional Challenge to PIPEDA*, *ibid.*
- ⁴⁶ *Ibid.* See also Rick Shields, "Health Privacy in Canada – Shedding Light on Murky Waters" (2004) 4:10 Privacy & Info. L. Rep. 8, online: (WESTLAW).
- ⁴⁷ *Supra* note 32.

- ⁴⁸ The 10 principles cover: 1. Accountability; 2. Identifying purposes; 3. Consent; 4. Limiting collection; 5. Limiting use, disclosure, and retention; 6. Accuracy; 7. Safeguards; 8. Openness; 9. Individual access; 10. Challenging compliance.
- ⁴⁹ PHIPA, *supra* note 8, ss. 18–28.
- ⁵⁰ *Ibid.*, ss. 15–17.
- ⁵¹ *Ibid.*
- ⁵² *Ibid.*, s. 12.
- ⁵³ *Ibid.*, s. 11.
- ⁵⁴ *Ibid.*, ss. 29–50.
- ⁵⁵ *Ibid.*, ss. 56–69.
- ⁵⁶ Rick Shields, *supra* note 47.
- ⁵⁷ *Process for the Determination of “Substantially Similar” Provincial Legislation*, *supra* note 31 at 2388.
- ⁵⁸ *Ibid.*
- ⁵⁹ As noted by Industry Canada, the Governor in Council’s Order under s. 26(2)(b) of PIPEDA “can exempt organizations or activities governed by sector specific provincial/territorial legislation that is deemed substantially similar” to PIPEDA: *ibid.*, at 2387–88.
- According to s. 26(2)(b) of PIPEDA, “the Governor in Council may, by order, . . . if satisfied that legislation of a province that is substantially similar to this Part applies to an organization, a class of organizations, an activity or a class of activities, exempt the organization, activity or class from the application of this Part in respect of the collection, use or disclosure of personal information that occurs within that province”.
- ⁶⁰ Under section 3 of PHIPA *supra* note 8, the term “health information custodian” means a person described in one of the paragraphs of this provision who has custody or control of personal health information as a result of or in connection with performing the person’s powers or duties or the work. For more on health information custodians, see “Application” under the “Impact of PHIPA”.
- ⁶¹ PHIPA, *supra* note 8, s. 46(2). My emphasis.
- ⁶² *Ibid.*, s. 47(4).
- ⁶³ *Ibid.*, s. 47(7).
- ⁶⁴ *Ibid.*, s. 47(8).
- ⁶⁵ *Ibid.*, s. 47(9).
- ⁶⁶ The term “de-identify” has a defined meaning under PHIPA; it means “to remove any information that identifies the individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify the individual”: *ibid.*, s. 47(1).
- ⁶⁷ PHIPA, *supra* note 8, s. 47(15).
- ⁶⁸ *Frequently Asked Questions: PHIPA*, *supra* note 33.
- ⁶⁹ As well, physicians and public hospitals should be aware of PIPEDA’s implications because even after PHIPA is deemed to be substantially similar to PIPEDA, the federal Act will continue to apply to the physicians’ and public hospitals’ inter-provincial and international commercial dealings.
- ⁷⁰ *PIPEDA Awareness Raising Tools*, *supra* note 28, questions 14–15.
- ⁷¹ See Rick Shields, *supra* note 46.
- ⁷² Pam Springer, “Ontario Hospital Association: Executive Report”, Vol. 15 No. 15 (17 December 2003), online: OHA <http://www.oha.com/oha/execrep.nsf/0/3719e0e207cc3bf585256dff0072f997?OpenDocument>.
- ⁷³ PHIPA, *supra* note 8, s. 2.
- ⁷⁴ *Stedman’s Medical Dictionary*, *supra* note 5.
- ⁷⁵ *Health Care Consent Act*, *supra* note 9, s. 2.
- ⁷⁶ *Public Hospitals Act*, *supra* note 7, s. 1.
- ⁷⁷ *Stedman’s Medical Dictionary*, *supra* note 5.
- ⁷⁸ *PIPEDA Awareness Raising Tools*, *supra* note 28, question 7.
- ⁷⁹ *Ibid.*, question 15. See also Megan E. Evans, “Healthcare Sector Impact” in Julie Thorburn & Megan Evans, *Canada Personal Information Protection and Electronic Documents Act: Quick Reference* (Toronto: Carswell, 2004) at 20.
- ⁸⁰ Megan E. Evans, *ibid.*, at 20.
- ⁸¹ Pam Springer, *supra* note 72. See also Anita D. Fineberg, “Personal Health Information: The ‘Scope’ Issues” [2003] C.H.L. LEXIS 3 at 10–11, online: (LEXIS).
- ⁸² *Stuart Investments Ltd. v. The Queen*, [1984] 1 S.C.R. 536; *R. v. Sharpe*, [2001] 1 S.C.R. 45.
- ⁸³ Canadian Standards Association, Standard CAN/CSA-Q830-96, online: CSA <http://www.csa.ca/standards/privacy/code/Default.asp?language=English>.
- ⁸⁴ The health care sector was not represented on the Technical Committee responsible for the Canada Standards Association’s *Model Code for the Protection of Personal Information*: Gilbert Sharpe, “Regulating Health Information: The Ontario Approach” [2000] C.J.L. LEXIS 6 at 15, online: (LEXIS).
- ⁸⁵ Gilbert Sharpe, *ibid.* See also Erika King & John H. Fuson, “An Overview of Canadian Privacy Law for Pharmaceutical and Device Manufacturers Operating in Canada” [2002] Food & Drug L.J. 205 at 209.
- ⁸⁶ Gilbert Sharpe, *supra* note 84.
- ⁸⁷ *Ibid.*
- ⁸⁸ See e.g. *Ferency v. MCI Medical Clinics et al.* (2004), 70 O.R. (3d) 277 (S.C.J.) [*Ferency v. MCI Medical Clinics*].
- ⁸⁹ *Ferency v. MCI Medical Clinics*, *ibid.*
- ⁹⁰ Richard Steinecke, “Chipping Away at Privacy Rights?” *Grey Areas* 75 (May 2004), online: Steinecke Maciura LaBlanc, Barrister & Solicitors <http://www.sml-law.com/publications/newsletters-detail.asp?DocID=4751>.
- ⁹¹ See e.g. *London Life Insurance Co. v. Canada*, [2000] G.S.T.C. 111 (Fed. C.A.) considering “commercial activity” as it relates to the operation of the *Excise Tax Act*, R.S.C. 1985, c. E-15 and *Income Tax Act*, R.S.C. 1985, c.1 (5th Supp.), and *Re Canada Labour Code*, [1992] 2 S.C.R. 50 interpreting the term “commercial activity” in relation to the *State Immunity Act*, R.S.C. 1985, c. S-18.
- ⁹² Canadian Institutes of Health Research, *Recommendations for the Interpretation and Application of the Personal Information Protection and Electronic Documents Act* (S.C. 2000, c. 5) in the Health Research Context (30 November 2001), online: http://www.cihr-irsc.gc.ca/e/documents/recommendations_e.pdf.
- ⁹³ [1983] 1 S.C.R. 57.
- ⁹⁴ *Ibid.*, at para. 22.
- ⁹⁵ “Private labs” here refers to “laboratories” within the meaning of the *Laboratory and Specimen Collection Centre Licensing Act*, R.S.O. 1990, c. L.1 s. 5: “laboratory” means a place equipped for the performance of microbiological, serological, hematological, biophysical, etc. tests for the purposes of diagnosis, prophylaxis or treatment.
- ⁹⁶ “Private pharmacies” refers to “pharmacies” within the meaning of the *Drug and Pharmacies Regulation Act*, R.S.O. 1990, c. H.4.
- ⁹⁷ Such as, for instance, private hospitals within the meaning of the *Private Hospitals Act*, R.S.O. 1990, c. P. 24; homes for the aged within the meaning of the *Homes for the Aged and Rest Homes Act*, R.S.O. 1990, c. H.13; nursing homes within the meaning of *Nursing Homes Act*, R.S.O. 1990, c. N.7.
- ⁹⁸ “Commercial” here means “viewed with regard to profit”: see Merriam-Webster Online Dictionary; online: <http://www.m-w.com/cgi-bin/dictionary?book=Dictionary&va=commercial>
- ⁹⁹ See, e.g. Downie & Caulfield, *supra* note 4 at 172.
- ¹⁰⁰ *Ibid.* at 34.
- ¹⁰¹ There is nothing in the *Canada Health Act*, *supra* note 40, preventing private for-profit organizations from supplying health services, and physicians managed through provincial medical associations and Colleges of Physicians and Surgeons “to ensure protection of their clinical autonomy and a measure of control over their incomes by entrenching a fee-for-service payment system”: Downie & Caulfield, *supra* note 4 at 34–35.
- ¹⁰² Downie & Caulfield, *ibid.*, at 35.
- ¹⁰³ See Anita D. Fineberg, *supra* note 81 at 12.
- ¹⁰⁴ See, e.g. *ibid.* at 13; Downie & Caulfield, *supra* note 4 at 172.
- ¹⁰⁵ See, e.g. CPSO, “Ontario Introduces Its Own Health Privacy Legislation” *Members’ Dialogue* (January–February 2004), online: The College of Physicians & Surgeons of Ontario <http://www.cpso.on.ca/publications/dialogue/0104/privacy.htm>.
- ¹⁰⁶ CPSO, “Protecting Patient’s Personal Information: Federal Privacy Legislation Sets out the Ground Rules” *Members’ Dialogue* (November–December 2003), online: The College of Physicians & Surgeons of Ontario <http://www.cpso.on.ca/publications/dialogue/1103/cover.htm>.

- ¹⁰⁷ Such as, for instance, psychiatric facilities within the meaning of the *Mental Health Act*, R.S.O. 1990, c. M.7; institutions within the meaning of the *Mental Hospitals Act*, R.S.O. 1990, c. M.8. See also health care facilities in *supra* note 99.
- ¹⁰⁸ Having concluded that PIPEDA applies to public hospitals only in extremely rare situations such as sales of donor lists, whereas core activities of the public hospitals are not subject to the federal Act, in “Procedures Required under PIPEDA”, I will concentrate on physicians not employed by public hospitals and their obligations under PIPEDA.
- ¹⁰⁹ PIPEDA, *supra* note 1, s. 7.
- ¹¹⁰ *Ibid.*, s. 2.
- ¹¹¹ Under s. 2 of PIPEDA, “organization” includes an association, a partnership, a person and a trade union. Thus, privately practicing physicians can also be considered “organizations” within the meaning of PIPEDA.
- ¹¹² George Radwanski, [former] Privacy Commissioner of Canada, “Privacy in Health Research: Sharing Perspectives and Paving the Way Forward”, Speech to the Canadian Institute of Health Research (14 November 2002), online: Privacy Commissioner of Canada http://www.privcom.gc.ca/speech/02_05_a_021114_e.asp
- ¹¹³ Again, “organizations” here means both physicians, with the exceptions of those employed by public hospitals, and public hospitals only in situations when the latter are engaged in dealings other than their core activities.
- ¹¹⁴ PIPEDA, *supra* note 1, s. 9.
- ¹¹⁵ Richard Steinecke, “Privacy Act: An Opportunity to Review Practice Policies” *Members’ Dialogue* (November-December 2003), online: The College of Physicians & Surgeons of Ontario <http://www.cpso.on.ca/publications/dialogue/1103/cover2.htm>.
- ¹¹⁶ *Ibid.*
- ¹¹⁷ PIPEDA, *supra* note 1, s. 11(1).
- ¹¹⁸ *Ibid.*, s. 11(2).
- ¹¹⁹ *Ibid.*, s. 12.
- ¹²⁰ *Ibid.*, s. 13.
- ¹²¹ *Ibid.*, s. 14.
- ¹²² *Ibid.*, s. 16.
- ¹²³ *Supra* note 39.
- ¹²⁴ *Ibid.*
- ¹²⁵ *Ibid.*
- ¹²⁶ David T.S. Fraser, *The Application of PIPEDA to Personal Health Information*, online: McInnes Cooper: Privacy Law http://www.privacylawyer.ca/privacy/pipeda_and_personal_health_information.pdf.
- ¹²⁷ See *Proposed Order*, *supra* note 32.
- ¹²⁸ PHIPA, *supra* note 8, ss. 7(1)(b)(i) and (ii).
- ¹²⁹ *Ibid.*, s. 3.
Note that neither Manitoba’s *Personal Health Information Act* nor Saskatchewan’s *Health Information Protection Act* contains the term “health information custodian”. Alberta’s *Health Information Act* uses the term “custodian” which is somewhat analogous, but not equivalent, to the term “health information custodian” employed in the new Ontario piece of legislation.
- ¹³⁰ Downie & Caulfield, *supra* note 4 at 158.
- ¹³¹ PHIPA, *supra* note 8, ss. 10–17.
- ¹³² *Ibid.*, s. 10.
- ¹³³ *Ibid.*, ss. 13–14.
- ¹³⁴ *Ibid.*, s. 15.
- ¹³⁵ *Ibid.*, s. 16.
- ¹³⁶ *Ibid.*, s. 11.
- ¹³⁷ *Ibid.*, s. 12.
- ¹³⁸ *Ibid.*, s. 12(2).
- ¹³⁹ *Ibid.*, ss. 18–28.
- ¹⁴⁰ Richard Steinecke, “More Workable Consent Procedures Under New Privacy Legislation” *Members’ Dialogue* (September-October 2004), online: The College of Physicians & Surgeons of Ontario <http://www.cpso.on.ca/publications/dialogue/0904/privacy.htm> [*More Workable Consent Procedures under New Privacy Legislation*].
- ¹⁴¹ PHIPA, *supra* note 8, s. 18(5).
- ¹⁴² *Ibid.*, s. 18(6).
- ¹⁴³ *Ibid.*, s. 18(2).
- ¹⁴⁴ *Ibid.*, ss. 18(3)(a) and (b).
- ¹⁴⁵ *More Workable Consent Procedures under New Privacy Legislation*, *supra* note 140.
- ¹⁴⁶ *Ibid.* See also PHIPA, *supra* note 8, ss. 20(1) and (2).
- ¹⁴⁷ PHIPA, *ibid.*, s. 20(2).
- ¹⁴⁸ *More Workable Consent Procedures under New Privacy Legislation*, *supra* note 140.
- ¹⁴⁹ PIPEDA, *supra* note 1, s. 7(3)(i); PHIPA, *supra* note 8, s. 43(1)(h) with respect to health information custodians and s. 49(3)(a)(ii) with respect to persons other than health information custodians.
- ¹⁵⁰ PHIPA, *supra* note 8, s. 44.
- ¹⁵¹ *Ibid.*
- ¹⁵² *Ibid.*, s. 2.
- ¹⁵³ *Ibid.*, s. 38.
- ¹⁵⁴ *Ibid.*, s. 40.
- ¹⁵⁵ *Ibid.*, s. 39.
- ¹⁵⁶ *Ibid.*, s. 41.
- ¹⁵⁷ *Ibid.*, s. 46.
- ¹⁵⁸ *Ibid.*, s. 42.
- ¹⁶⁰ *Ibid.*, s. 45.
- ¹⁶⁰ *Ibid.*, s. 45.
- ¹⁶¹ *Ibid.*, s. 52.
- ¹⁶² *Ibid.*, s. 52(1)(e)(i).
- ¹⁶³ *Ibid.*, s. 54(2).
- ¹⁶⁴ *Ibid.*, s. 54(3).
- ¹⁶⁵ *Ibid.*, s. 54(5).
- ¹⁶⁶ *Ibid.*, s. 54(8).
- ¹⁶⁷ *Ibid.*, s. 54(10).
- ¹⁶⁸ *Ibid.*, s. 54(11).
- ¹⁶⁹ *Ibid.*, s. 56.
- ¹⁷⁰ *Ibid.*, ss. 58–59.
- ¹⁷¹ *Ibid.*, s. 60.
- ¹⁷² R.S.O. 1990, c. F.31.
- ¹⁷³ *Ibid.*, s. 66.
- ¹⁷⁴ *Ibid.*, s. 64(4).
- ¹⁷⁵ *Ibid.*, s. 65.
- ¹⁷⁶ *Ibid.*, s. 72.
- ¹⁷⁷ *Ibid.*, ss. 72(2)(a) and (b).
- ¹⁷⁸ *More Workable Consent Procedures under New Privacy Legislation*, *supra* note 140.