

Submission to:

The New Brunswick, Personal Health Information Task Force

Submitted by:

Professor David A. Townsend, Faculty of Law, University of New Brunswick

and

Kevin R. Motley, Student-at-Law, University of New Brunswick

Dated: 6 July 2007

Introduction:

This submission is tendered to the Personal Health Information Task Force to assist with the committee's examination of the need for and policy particulars of a dedicated legal framework to safeguard personal health information (PHI) in New Brunswick. Part A of this submission offers general principles related to the creation of legislative policy in the area of personal health information. Where appropriate, emphasis has been placed upon the New Brunswick context. Part B addresses many of the policy questions posed within the *Consultation Guide*¹ and the *Background Paper*,² circulated on behalf of the Task Force, in order to bring focus to the public consultations on PHI policy reform.

While the phrases personal health information (PHI) and personal health data (PHD) will be used interchangeably throughout this submission, we begin by endorsing the use of the word 'data' when referring to health-related information. We note that the committee's background document uses the phrase "data custodian" for an authorized holder of personal health information. Our views about the importance of this use of terminology will be discussed within Part A below.

PART A:

The times they are a changin'...

The Province's *Consultation Guide* commences with the sentence, "The practice of health care is changing."³ This is an understatement. The delivery and management of health care services in Canada and in New Brunswick have been undergoing profound changes over the past 10 to 15 years -- and recently the pace of change has been accelerating. A number of these changes have

¹ New Brunswick, Personal Health Information Task Force, *Personal Health Information Access and Privacy: Consultation Guide*, (Province of New Brunswick, May 2007).

² New Brunswick, Personal Health Information Task Force, *Personal Health Information Access and Privacy: Background Paper*, (Province of New Brunswick, May 2007).

³ *Supra* note 1 at 1.

direct impact upon the policy directions for personal health data legislation for New Brunswick. A few of the most important changes for PHD policy reform are outlined immediately below:

- Increasingly, teams or networks of primary health care providers collect and exchange large quantities of health data about the patients they treat. Very soon, exchanges of PHD will be a prominent feature of health services delivery and management in Canada.
- More sub-acute care delivery is moving from primary care facilities like hospitals into community clinics and nursing homes.
- Home-based care has transitioned from convalescent activities to active health care treatments. These may require the administration of prescribed drugs, therapies and medical devices that may be dispensed from public health care facilities or from medical device and therapy providers operating in the private sector.
- Almost all medical devices have become, in part, computing apparatus producing vast quantities of personal health data that must be networked with other medical devices, with other health data about the patient and with various health care team members.
- Health care delivery and management is becoming increasingly ‘smarter’ with the introduction of smart (digital) technologies to authenticate and track patients (e.g. smart cards) and to analyze and rationalize multiple aspects of health care decision-making. Most provinces and territories in Canada are moving toward some type of Electronic Health Record system (EHR).
- Advancements in health sciences research are driving increased requirements for personal health data (and more varied information, such as genetic coding). Much of the compilation and analysis of this data is being performed externally to the health care facilities and care provider(s) that originally collected the information.
- Many health care facilities are introducing wireless technologies in order to network health related personnel, data banks and medical devices. The successful deployment of wireless technologies and services offers the potential for health care professions to be able to enter, access, analyze and exchange personal health information at the point-of-care, regardless of where that point is located.
- The recent appearance of certain private health care facilities in Canada is a trend that is certain to continue. Additionally, the Supreme Court of Canada’s 2005 decision of *Chaoulli v. Quebec*⁴ may stimulate the establishment of even more private sector health care facilities in Quebec and, possibly, in the rest of Canada. Our Supreme Court ruled that the sections of Quebec’s *Health Insurance Act* and *Hospital Insurance Act* that prohibited private health insurance were contrary to the Quebec *Charter of Human Rights and Freedoms* due to the inordinate delay in accessing the publicly funded health care system.

⁴ [2005] 1 S.C.R. 791, 2005 SCC 35.

- With each passing year, health care providers are being required by law to perform more public policy objectives involving the collection and reporting of PHI that are not directly related to the delivery or management of primary health care. For example, health care professionals are required to report suspected child abuse, gunshot wounds, ingestion of particular illegal drugs and the contraction of certain infectious diseases.⁵

Key policy objectives of Privacy, Security and Trust...

Yes, the practice of health care in Canada and New Brunswick is changing, and the changes noted above will profoundly impact upon the privacy, security and trust elements of dedicated personal health data legislation. We submit that privacy, security and trust are the key policy underpinnings for the challenges facing the members of the Personal Health Information Task Force. We offer the following definitions⁶ of these terms and a brief explanation of their significance to changes within the health care sector and the relevance for PHD policy reform.

Privacy concerns the operational policies, procedures and regulations implemented within an information system to prevent unauthorized use of, access to, or release of, personal information held in any format. Within a health care context, privacy relates to legislative and organizational norms that permit individuals to have control over the collection, use, disclosure, retention and accuracy of their own health data.

We submit that providing a policy framework that will give New Brunswickers explicit legal controls over the collection, use, disclosure, retention and accuracy of their own health data is the *raison d'être* of the Task Force itself. We are concerned that many of the changes in the health care sector discussed above have the potential to accentuate the importance of operational efficiencies and specialization and to minimize the dignity and personhood interests of the patient.

We need a patient-focused statute with strong presumptions that knowledgeable consent will be required from our citizens before identifying PHD can be collected, used, disclosed and exchanged. Implied consent should be explicitly and restrictively defined within the statute. It should not become the operational norm for the provision of modern health care. It is important to recall that the Supreme Court of Canada⁷ has decreed that personal health information is the property of the patient and not the health care provider or manager. Consent forms must provide real controls over PHD and be written in plain language so as to inform and assuage New Brunswickers about how their privacy is safeguarded under the legislation.⁸

⁵ The *Consultation Guide* noted the desire in New Brunswick to tie personal health data systems to a provincial prescription drug-monitoring program. (*Supra* note 1 at 1.)

⁶ For the past four years, Professor David Townsend has been a member of the Privacy, Security and Trust (PST) research collective associated with the University of New Brunswick (UNB) at Fredericton and the National Research Council IT Institute (NRC-IIT e-Business) located on the UNB Fredericton Campus. These definitions of Privacy, Security and Trust were developed by Professor Townsend and reflect collaborations with members of the PST research collective.

⁷ *McInerney v. MacDonald*, [1992] 2 S.C.R. 138.

⁸ This challenge is accentuated by the fact that the average New Brunswicker reads at a Grade 6 level.

Security addresses the various components of an information system that safeguard the data and associated infrastructure from unauthorized activity. Within a health care context, security relates to organizational control over network information and resources so as to ensure the confidentiality, integrity and availability of the personal health data being collected, accessed, reported or exchanged.

Most personal health information is now in data form and, as such, it is subject to many computer and network security challenges. For these reasons, we endorse the term “data custodian” used within the public consultation documents for the principal holders of personal health information. While data formatting greatly facilitates the collection, storage, access, analysis, sharing and exchange of personal health information, it also significantly increases its exposure to various security breaches.

The recent changes that have been happening in the health care sector have the potential to significantly increase the risks of security breaches involving personal health data. The following two examples are instructive. First, viewed from a health data perspective, we see the emergence of regional, provincial and national health data exchange (HDE) architectures where PHI is created, collected, used, exchanged and analyzed by multiple and varied health care professionals and facilities, and agents thereof, operating in both the public and private sectors.

The exchange of health data between disparately located care providers requires unique user authorization, authentication, and access control and audit requirements. Also, legal obligations for the privacy and security of PHD must apply to the requestor of personal health information as well to the data custodian. Thus, new PHI legislation must provide a framework for the implementation of specific rules, protocols and technical standards applicable to HDE infrastructures. Second, the increasing deployment of wireless technologies and services within health care contexts presents superadded security challenges.⁹

Under the general subject category of ‘health informatics,’ various committees and working groups of the International Standards Organization (ISO)¹⁰ are in the process of drafting over thirty¹¹ unique technical requirements (guidelines, protocols and standards) to ensure the privacy, security and availability of personal health data. The subject matter of these technical requirements address issues such as electronic health record communication,¹² exchange of information between health care information systems,¹³ electronic reporting of adverse drug

⁹ For a very recent incident involving privacy breaches through the use of wireless surveillance cameras at a medical clinic, see: Joaquim P. Menzes, “Bizarre Incident at Sudbury Clinic Sparks Privacy Commissioner Order” *IT World Canada* (June 8, 2007), online: <<http://www.itworldcanada.com/a/Wireless-and-Mobile-Computing/b9cf3606-e1c4-49dc-98a4-6013bb7531e7.html>>.

¹⁰ Technical Committee ISO TC 215 is undertaking most of the health informatics project work.

¹¹ Many of these technical requirements have unique subparts to them, so the actual number of ISO health informatics standards recently developed or under development is closer to sixty.

¹² For example, see ISO project reference ISO/CD 13606-1 Health Informatics – Electronic Health Record Communication, Part 1.

¹³ See, for example, the work of ISO/DIS 17113.2 Health Informatics – Exchange of Information between Healthcare Information Systems, Method for the Development of Messages.

reactions,¹⁴ privilege and management controls for health information systems¹⁵ and the interoperability of telehealth systems and networks.¹⁶

At the ISO, Technical Committee ISO TC 215 is undertaking most of the health informatics project work. Canada has representation on many of the subcommittees associated with TC 215. Once these technical standards projects are sufficiently complete, the Canadian Standards Association (CSA) may approve them for accreditation as a national standard of Canada. Within the CSA, Health Informatics Technical Committee Z295 (CSA/TC Z295) is responsible for the accreditation of standards in the health informatics domain.

Due to the inherently high sensitivity of personal health information and the potential for multiple simultaneous health file breaches, the legislative framework for PHD must create, promulgate and enforce legal and technical requirements intended to safeguard the confidentiality, integrity and availability of the data. Thus, it is fundamental to our submission that the new regulatory framework for the protection of PHI should do far more than merely specify that each ‘data custodian must employ security safeguards that are reasonable given the sensitivity of the health data at issue.’ In the near future, specific technical rules, protocols and standards for PHD security will need to be enabled, authorized and enforced within the regulatory framework provided by the PHI legislation. We ask that the Task Force members take this development into consideration.¹⁷

Trust represents a subjective measure of confidence in the reliability and integrity of an information service provider in terms of the provider's commitment and ability to complete an interaction in accordance with the expectations of those who use or otherwise rely upon that service. Trust involves a willingness to be vulnerable, and within a health care context, patients and the users of health information systems are more likely to trust an information service and its provider if individual privacy and security interests are adequately safeguarded and the service is delivered in a manner that is reasonably transparent.

Trust is a fundamental precondition to successful patient care outcomes. Patients will provide sensitive, and perhaps embarrassing, health related information only if they perceive that the privacy and security of their data will be assured. It is interesting to note that the *Hippocratic Oath* for physicians contains a solemn undertaking that doctors will maintain the privacy of patient information.¹⁸ A patient-focused PHD statute will help to give patients the confidence

¹⁴ ISO/NP TS 2224 Health Informatics – Electronic Reporting of Adverse Drug Reactions.

¹⁵ See, for example, standards project ISO/PRF TS 22600-2 Health Informatics – Privilege Management and Access Control, Part 2, Formal Models.

¹⁶ ISO/TR 16056-1:2004 Health Informatics – Interoperability of Telehealth Systems and Networks, Part 2: Real-time Systems is an example of a published (completed) standard.

¹⁷ For some legislative examples of enabling authority to create technical rules and standards for health informatics purposes see sections 505(24) and the detailed provisions in subsections 520.1 to 520.4 of Quebec's *Health Services and Social Services Act*, RSQ c. S-4.2. For detailed privacy requirements regarding patient records see sections 17 to 28 of the same statute.

¹⁸ A popular translation of the *Hippocratic Oath* written in 1964 by Louis Lasagna, then Dean of Medicine at Tufts University, casts the privacy obligations in the following terms, "I will respect the privacy of my patients, for their problems are not disclosed to me that the world may know." See the oath on line at:

they require to reveal and discuss sensitive health information. In this regard, we urge Task Force members to recommend that perambulatory text be added to our PHD legislation that contains rights-affirming statements for patients such as those found in the preamble to Manitoba's, *Personal Health Information Act*.¹⁹ Also, New Brunswickers need to know that meaningful sanctions are available for those who, without lawful excuse, enable or permit privacy or security breaches to occur. It is instructive that Ontario has added a 'private right of action' within its PHI legislation to permit those who suffer from security or privacy breaches to bring a civil law suit against the responsible parties.²⁰

Health data custodians also need to know that meaningful sanctions may be imposed if the custodians and affiliated agents with whom they share and exchange personal health data do not adhere to current security and privacy requirements. Trust is important for health information custodians too.

The New Brunswick Situation...

Clearly, the time has come for New Brunswick to join many other provinces and pass dedicated personal health information legislation. With no provincial statute dealing directly with this issue, New Brunswickers must rely on an inadequate combination offered by a blending of the provincial *Protection of Personal Information Act* (PoPIA) and the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA). Unfortunately, PoPIA is overly vague and is presently under review for its general failings, and PIPEDA takes control out of the hands of local authorities while also failing to address certain issues specific to health information. Other provinces, including Manitoba, Saskatchewan, Alberta and Ontario have separate legislation dealing specifically with personal health information, and others such as Quebec²¹ and British Columbia have incorporated specific health-related provisions into their general access to information and privacy legislation.²² In order to enhance health privacy and keep pace with developments in these jurisdictions, New Brunswick should enact its own specific health information protection legislation.

There are several reasons why New Brunswick should not rely on the federal PIPEDA to safeguard health information in the Province. PIPEDA was drafted without focusing upon its application to health information, and as such does not include the detailed health-specific provisions that purpose-built legislation would contain. It must also be noted that because PIPEDA is based on the federal regulation of commercial activity, it applies to doctors in private practice, but not to publicly-funded hospitals.²³

<http://www.pbs.org/wgbh/nova/doctors/oath_modern.html>. Since 1998, the Canadian Medical Association (CMA) has produced a health information privacy code for its members.

¹⁹ C.C.S.M., c. P-33.5.

²⁰ *Personal Health Information Protection Act*, S.O. 2004, c. 3, s. 65.

²¹ The bulk of Quebec's health privacy and security regime can be found in its *Health Services and Social Services Act*, see *Supra* note 17.

²² A good glossary of health information legislation across various Canadian jurisdictions can be found online at: Canadian Institute for Health Research, "Compendium of Canadian Legislation Respecting the Protection of Personal Information in Health Research - Updated June 2005" <<http://www.cihr-irsc.gc.ca/e/31433.html>>

²³ Canada, Office of the Privacy Commissioner, *Fact Sheet: Municipalities, Universities, Schools and Hospitals*, (Government of Canada, 2006), online: <http://www.privcom.gc.ca/fs-fi/02_05_d_25_e.asp>.

New Brunswick's present reliance on PIPEDA leaves a gaping hole in meaningful privacy and security protections when it comes to employee health information held by employers in the private sector. The provincial PoPIA only applies to public entities subject to the *Right to Information Act*, and not to private businesses. PIPEDA is of little help to those seeking a remedy against their private-sector employer, unless that employer is a federally-regulated entity, such as an airport. PIPEDA is on uncertain constitutional grounds and is presently subject to a constitutional challenge in Quebec, alleging that it interferes with provincial authority over property and civil rights.²⁴ While the federal Privacy Commissioner has been willing to invoke the federal 'trade and commerce' power to apply PIPEDA to private sector dealings with citizens, she is unwilling to risk further conflict challenges by using it to regulate labour relations.²⁵ Since the federal government is unwilling to offer assistance, provincial law is non-existent on the matter, and the Ombudsman's office lacks the resources and authority to take on these types of cases. Over half of privacy complaints to the New Brunswick Ombudsman's office originate from employees' concerns with their employer's activities, but under the present legislative scheme, there is often no remedy available in these cases.²⁶ Employees with privacy concerns working within provincial jurisdiction are left with an undesirable choice of either dropping the matter or hiring a lawyer on their own. This is often prohibitively expensive, and present law tends to favor employers, so the outcome is uncertain even if the case has serious merit.

Replacing PIPEDA with provincial legislation would allow greater local control over health information regulation, as problems could be resolved through the local supervisory body rather than the federal Privacy Office. Orders issued by a body with sensitivity to local conditions and concerns would better encourage compliance by the institutions covered by health data legislation. As compliance is the end goal of this sort of legislative scheme, local laws backed by local enforcement makes the most sense. Furthermore, there is room for significant local differences in implementation of provincial health privacy and security legislation while still meeting requirements to qualify as "substantially similar" to PIPEDA and therefore substitute for it, as demonstrated in Quebec's *Access to Documents Held by Public Bodies and the Protection of Personal Information* legislation. By enacting separate health privacy legislation in the near future, New Brunswick can address local concerns while incorporating and improving upon developments in other jurisdictions.

²⁴ Nikki Swartz, "Canada's Privacy Law Faces Legal Challenge", *Information Management Journal* (Mar/Apr 2004), online: <http://findarticles.com/p/articles/mi_qa3937/is_200403/ai_n9358220>. See Quebec Court of Appeal, Order No. 1368-2003 (17 December 2003), allowing Quebec to proceed with a constitutional challenge to PIPEDA, as referred to in Lisa M. Austin, "Is Consent the Foundation of Fair Information Practices? Canada's Experience under Pipedata", (Spring 2006) 56 :181 U. Toronto L.J.

²⁵ Interview with Christian Whalen, Legal Counsel for NB Ombudsman's Office, Friday, June 8, 2007.

²⁶ *Ibid.*

PART B:

1) Scope of Legislation:

- *What custodians of personal health information do you think should be covered by health information privacy legislation for New Brunswick?*

At page five of the Personal Health Information Task Force's *Background Paper*,²⁷ the following suggested list of data custodians is provided:

- Physicians, pharmacists and the staff working in their private offices or places of business, practicing members of all registered New Brunswick health professions
- Agencies such as the Canadian Institute for Health Information, the Canadian Institutes of Health Research and Statistics Canada with a mandate to do health research
- Regional Health Authorities and the facilities they operate (e.g., hospitals, community health centres)
- The Department of Health and other government departments
- Nursing homes
- Employers who hold personal health information about their employees
- Non-profit agencies that provide health care (e.g., Victorian Order of Nurses)
- Private health care facilities (e.g., private medical laboratories)
- Agents or affiliates of a data custodian

With the inclusion of the bodies discussed below, we submit that this is an appropriate initial list of bodies that should be included under the definition of health data custodians in any future health privacy and security legislation that New Brunswick might adopt. We would like to add the following additions:

Private health service providers and health insurance companies:

It is particularly important that new health privacy and security legislation include all private health care providers. It appears that private health delivery is assuming a much larger role in Canada's health care landscape. One need only look under the "Home Care" listing in the Fredericton phone book to find multiple for-profit companies that offer health care. The ruling in *Chaoulli v. Quebec*²⁸, as discussed in Part A of this submission, could encourage challenges to legislation prohibiting private health insurance in Ontario, Manitoba, British Columbia, Alberta, and Prince Edward Island. In 2005, the Canadian Medical Association gave a stern rebuke to the single-payer system by voting heavily in favour of permitting private health insurance and private-sector health services.²⁹ Considering these developments, it stands to reason that private health care providers will be handling a greater share of New Brunswick's personal health information in the near future, and therefore private entities – including private health insurance providers – should be expressly included in the province's health information legislation.

²⁷ *Supra* note 2 at 5.

²⁸ *Supra* note 4.

²⁹ "CMA Supports Private Health Insurance", 173:6 *Canadian Medical Association Journal* (September 13, 2005), online: <<http://www.cmaj.ca/cgi/rapidpdf/cmaj.051035v1.pdf>>.

Employers who hold personal health information about their employees:

As discussed above, New Brunswick currently suffers a serious deficiency in general privacy protection for employees. Considering the inherent sensitivity of health information and the reality that employers are often privy to their employees' health data, the need for legislation to address this issue is particularly dire.

Agents, affiliates and third-party contractors of data custodians:

Agents and affiliates of a data custodian should *not* be included under the definition of data custodians in any new health privacy legislation. As dealt with below, there should instead be statutory means of framing and managing the relationship between HDC's and third-party contractors that the custodian hires. The requirements for maintenance of security and privacy should be clearly spelled out, but the onus should be on the data custodian to ensure its contractors adhere to these requirements. Responsibility for health data should remain with its primary custodian, rather than shifted onto subordinate agents who often fill a short-term role. These contractors cannot be expected to have their own dedicated internal health privacy policies, health information officers, or even full awareness of their obligations independent of the primary custodian's instructions. Allowing custodians to delegate accountability to independent contractors, thereby making those contractors data custodians in their own right, may undermine health privacy and security objectives.

- What type of personal health information do you think should be covered by new health information privacy legislation?

New health privacy legislation should cover a broad range of health-related information. This should definitely include a person's medical record in their physician's office, personal health care history, and information relating to all laboratory tests ordered or conducted for the individual.

Legislation should specifically protect personal Medicare numbers, as Manitoba and Alberta have done. Non-custodians should be barred from ever demanding to know a person's health number except under very specific circumstances authorized by statute (for example Manitoba makes an exception to this general rule for regulated medical research purposes).³⁰ Measures specifically aimed at protecting personal health identification numbers will assist in curbing fraud and health care abuse. Therefore, prohibitions on the collection and use of Medicare numbers without lawful excuse should be added to any new provincial health privacy and security legislation.

Personal health information should also be defined to include samples of a person's genetic material, body parts or bodily fluids. With recent scientific advances, identification and medical examination of an individual through tests of their tissues has become a practical reality. These samples can also contain highly sensitive information about many existing and potential health conditions the patient may have. Information about genetic and tissue samples should therefore be given statutory protection in the same manner as other kinds of personal health data.

³⁰ *Supra* note 4, ss. 26(1)-(2).

Manitoba and Alberta have expressly included genetic material under the scope of their health information protection legislation,³¹ and New Brunswick should do the same.

Recorded and Unrecorded Information:

A recent incident in Ontario underlines the need to include and safeguard certain personal health information that may not be captured through technical means of recordation. In what was characterized as a “gross breach of privacy,” wireless cameras at a methadone clinic in Sudbury broadcast images of urine sample collection that were received by a passing motorist on their rear-view camera display.³² There was some uncertainty over whether the images, which were part of a closed-circuit television system and not recorded in any permanent sense, qualified as a “record” as defined by Ontario’s *Personal Health Information Protection Act*. PHIPA applies only to a “record” of personal health information, but it defines “record” in a flexible manner.³³ The Ontario Privacy Commissioner found that the incident came under her department’s statutory authority because the images could be deemed to be “recorded” as soon as they were encoded for processing and transmission within the camera.³⁴ However, this finding could be disputed due to the PHIPA definition’s emphasis on permanent recording media.³⁵ This incident demonstrates the blurred boundary between recorded and unrecorded personal health information, and demonstrates the need to expressly include both types of information under the scope of any health privacy legislation that New Brunswick might enact. Many medical devices transmit their data to other computing equipment wirelessly. The information should not require recordation to initiate security and privacy safeguards. As Ontario has done in PHIPA, oral information such as conversations with health professionals should also be included in the definition of personal health information³⁶.

2) Consent:

- Should implied knowledgeable consent be the “standard,” and should express consent be required in other situations? What would these situations be?

The Personal Health Information Task Force’s *Consultation Guide*³⁷ defines “implied knowledgeable consent” as existing when it is reasonable to believe that an individual knows:

- why their personal health information is being collected, used or disclosed, and
- that they can in fact provide or withhold consent

We submit that all consent must be knowledgeable. Implied knowledgeable consent should be an explicit exception to a legislative presumption for expressed knowledgeable consent. It

³¹ *Supra* note 4, s. 1(1)(a), *Freedom of Information and Protection of Privacy Act*, R.S.A. 2000, c. F-25 s. 1(1)(n)(v).

³² *Supra* note 9.

³³ *Supra* Note 20, s. 2. “a record of information in any form or in any medium, whether written, printed, photographic or electronic form or otherwise, but does not include [...] [a] mechanism that can produce a record”.

³⁴ Ontario, Office of the Information and Privacy Commissioner, *Order HO-005* (June 2007), online: <http://www.ipc.on.ca/images/Findings/up-ho_005.pdf> at 5, 7.

³⁵ *Supra* Note 20, s. 2.

³⁶ *Supra* Note 20, s. 4(1).

³⁷ *Supra* note 1 at 4.

should not be “the standard” legislative position. All exceptions to expressed consent should be explicit, comprehensible and limited.

Without referring specifically to health information, PIPEDA does allow “organizations” to collect, use and disclose personal information without individual consent in emergency situations “clearly in the interest of the individual” where their “life, health or security” are threatened.³⁸ However, health care also requires many routine disclosures between related providers - the so-called “circle of care” - for the patient’s sole benefit but in a non-emergency context. PIPEDA does not provide for these situations, which creates ambiguity as to when express consent is required, and what safeguards are in place when it is not. In these situations, health-specific legislation such as Ontario’s PHIPA have “more workable consent procedures for the collection, use and disclosure of personal health information [...] providing more options for using and disclosing personal health information without the client’s [express] consent.”³⁹

Under PIPEDA, it has been generally regarded as acceptable to “imply” consent within the “circle of care,” where disclosures are necessary to provide care and treatment. A widely-circulated memo issued in 2003 by Interim Commissioner Marleau stated that patients need not know what the information is to be used for so long as it is within this “circle of care.”⁴⁰ More recently, however, there is the growing view this interpretation would not survive a federal court challenge.⁴¹ This is because the principles in PIPEDA state that implied consent is appropriate for “less sensitive” information, when medical information by its nature is highly sensitive.⁴²

Furthermore, PIPEDA does even less to address the issue of implied consent for necessary and routine disclosures outside the immediate treatment circle, but within the larger “therapeutic nexus” to a particular condition or treatment. Medical information is routinely used outside the “circle of care,” for purposes such as “peer review, chart reviews, [and] risk mitigation consultations with the physician’s insurer.”⁴³ For this reason, it is often appropriate to rely on implied consent in cases dealing with health information. The risks associated with reliance on implied consent can be mitigated by clearly informing patients of how their information is going to be used, and obtaining advance consent for most purposes.⁴⁴

However, obtaining express consent is not the same as overwhelming the patient with a multitude of Byzantine legal forms covering every type of use and disclosure, like those that were used when PIPEDA was first implemented. Any scheme to gain advance consent must turn on accessible and understandable documents where the patient is precisely aware of the uses to which he or she is assenting. We must resist the legalistic temptation to solve this problem by resorting to complicated forms, or we risk de-valuing the consent that we do obtain. Readable

³⁸ *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, ss. 7(1)(a), s. 7(2)(b), 7(3)(e).

³⁹ “Getting Ready for Ontario’s Privacy Legislation: Guide: Privacy Requirements and Policies for Health Practitioners” College of Medical Laboratory Technologists of Ontario, Toronto, September 2003 at 5.

⁴⁰ Letter from Robert Marleau to Mr. John A. Laplume (November 21, 2003), online: <<http://www.cma.ca/staticContent/HTML/N0/I2/HIT/pdf/MMA-Marleau%20letter-PIPEDA.pdf>>.

⁴¹ David T.S. Fraser, “The Application of PIPEDA to Personal Health Information”, (2004) 1 Can. Privacy L.R. 6 at 3.

⁴² *Supra* note 38, Sched 1, 4.3.4.

⁴³ *Supra* note 41 at 5.

⁴⁴ *Ibid.* at 5.

and concise forms can be used to educate the patient about how health data is safeguarded, and thereby gain patient trust.

3) Collection, use, and disclosure:

- Are there any circumstances where collecting, using or disclosing an individual's personal health information without the individual's consent should be allowed?

The *Consultation Guide*⁴⁵ provides the following preliminary list of circumstances where an individual's health information could be collected, used or disclosed without their consent:

- minimizing or averting a risk to public health or safety
- on a court order, or assisting in a criminal investigation
- determining an individual's eligibility to receive health services
- complying with a law of New Brunswick or Canada
- planning, monitoring and evaluating the health system – including practices to uncover waste, fraud or criminality
- in the course of health service provider education
- disclosing personal health information to an individual's legal guardian

We submit that such exceptions are usual and necessary, but we do have some concerns about collecting and processing prescription drug data in order to implement a drug monitoring program in New Brunswick.

Prescription drug monitoring program:

While a proposed prescription drug monitoring program makes for good health policy, it raises serious privacy concerns if it is not carefully implemented. A provincial electronic pharmaceutical record database would be required, and prescription records are highly sensitive. Drugs are often tied to specific illnesses and can be used to infer a patient's current and historical medical circumstances. For example, a prescription for paroxetine would indicate a history of depression, while a prescription for methadone would indicate a past substance abuse problem. As such, the framework for a prescription drug monitoring program should be provided within new PHI legislation.

New Brunswick should look to British Columbia's experience regarding a provincial drug database. In 1995 B.C. established PharmaNet, a province-wide electronic prescription drug information system. PharmaNet tracks all prescriptions dispensed in the province, and contains detailed information about patient drug profiles, including what drugs are dispensed, patient drug allergies, demographic and billing information, and other information exchanged by pharmacists.⁴⁶ This information can be accessed by pharmacists and physicians (including emergency physicians and physicians in private practice) when medication is dispensed or medication information is required, and by the pharmacists' and physicians' respective Colleges for the purposes of professional regulation.

⁴⁵ *Supra* note 1 at 3.

⁴⁶ David Loukidelis, Letter to B.C. Health Minister George Abbott, May 2, 2007 online: <[www.oipcbc.org/news/Letters/F07-31479AbbottLetter\(2May07\).pdf](http://www.oipcbc.org/news/Letters/F07-31479AbbottLetter(2May07).pdf)>.

The British Columbia Privacy Commissioner, David Loukidelis, believes that when implementing electronic databases of these sorts, it is imperative that no more information be collected than is necessary, and that the uses and disclosures of such information be tightly defined and controlled.⁴⁷ These databases should remain accessible only to a clearly-defined group of individuals involved in the provision of medical care, and should not be shared with other data custodians except where absolutely necessary. From this viewpoint, allowing access to agencies concerned with drug enforcement should be permitted only as a very narrow and carefully-worded public-policy-based exception. Such agencies should only have access to the relevant parts of, or patterns in, a patient's file, and the rest should be automatically severed. Mr. Loukidelis also suggests that electronic databases lend themselves well to "proactive" privacy audits through software that monitor access requests for personal information.⁴⁸ In B.C., for example, an access request must be linked to a drug-dispensing or other specific medical transaction.⁴⁹ This could be implemented alongside a provincial drug monitoring program, in order to improve oversight and accountability alongside more traditional "reactive" privacy auditing.

Since health care information will likely move toward a unified electronic patient record in the near future, the precedents set in how privacy in electronic prescription databases are implemented are highly important. They will help determine how these wider records will balance the protection of patient information with the need for medical professionals to access this data to better provide services.

4) Access to Information:

- Under what circumstances can a person be denied access to their own information? If it would reveal private information about another person? If it would be dangerous to someone's physical or mental health?

The *Background Paper*⁵⁰ included the following list of circumstances where a person might be denied access to their own health information:

- where knowledge of the information could reasonably be expected to endanger the mental or physical health or safety of the individual or another person
- where providing access would reveal personal health information about another individual who has not given their consent
- where providing access could identify a third party, other than another custodian, who provided the information in confidence
- where the information was compiled for a civil, criminal or quasi-judicial proceeding

⁴⁷ *Ibid.*

⁴⁸ *Ibid.*

⁴⁹ British Columbia, Office of the Information and Privacy Commissioner, "Health Information Privacy - the British Columbia Experience", Transcript of speech by David Loukidelis at Canadian Institute Conference - Toronto: June 19, 2001, online: <http://www.oipcbc.org/publications/speeches_presentations/speech_04.html>

⁵⁰ *Supra* note 2 at 6.

We submit that this listing of circumstances where it may be justified to deny a person access to his or her own personal health data is compatible with the lists contained within other PHI schemes in Canada, but we have a few words of caution.

Considering the Supreme Court of Canada's decision in *McInerney v. MacDonald*,⁵¹ it stands to reason that access to one's own information should be treated as a presumptive right. Reflecting this, Ontario's PHIPA legislation creates a general presumption that a patient should have full access to information contained in their medical records.⁵² These include correspondence with consultants, even if such documents are marked as confidential.⁵³ The exceptions to this rule are relatively narrow. In order for a patient to be denied access to his or her records under PHIPA, it must be reasonably demonstrated that access would cause serious harm to the patient's treatment, serious physical harm to any person, or disclose another person's sensitive personal information.⁵⁴ Even in these cases (and particularly applicable to the latter) there are provisions to sever the offending information rather than deny disclosure outright.⁵⁵ Manitoba's *Personal Health Information Act* is worded with even greater clarity to impose a positive obligation on the health data custodian to sever such information and disclose.⁵⁶ Any new health legislation should similarly establish that the HDC "shall, to the extent possible, sever the personal health information that cannot be examined [...] and permit the individual to examine [...] the remainder."⁵⁷ Another concept that New Brunswick would do well to borrow from other provinces' general privacy and access legislation is the requirement to attempt to obtain the consent of third parties whose privacy would be violated by another's access-to-information request.⁵⁸

- Should individuals be responsible for some or all of the costs associated with accessing their health information?

As a general principle, an individual should not be deterred from accessing their own health information by the costs involved. The policy objective of ensuring that personal health information is accurate and complete is one of the principal goals of PHI legislation. We submit that Alberta has a reasonable schedule of fees set out in its health information regulations. In Alberta, the base fee for any health information request is \$25, with the possibility of additional fees if the request requires special means of preparation such as severance of unauthorized information or records retrieval from another location.⁵⁹ The health data custodian must provide an estimate of such additional fees, and the applicant must assent to them in a specified period before the request will be processed. Most importantly, there is a provision in Alberta's regulations for the fees to be waived in full or in part if the custodian believes "it is fair to excuse payment."⁶⁰

⁵¹ *Supra* note 7.

⁵² *Supra* note 20, s. 52(1).

⁵³ Erin Elizabeth Fitzpatrick, "Introduction", (March 2006) 26:3 *Health Law in Canada* at 32.

⁵⁴ *Supra* note 20, s. 52(1)(e)(i)-(iii).

⁵⁵ *Ibid.*, s. 52(2)-(3).

⁵⁶ *Supra* note 19, s. 11(2).

⁵⁷ *Ibid.*, s. 11(2).

⁵⁸ *Access to Information and Protection of Privacy Act*, S.N. 2002, c. A-1.1, s. 16(1).

⁵⁹ Alta. Reg. 70/2001, Schedules 1-2, ss. 10(1), 11(1)(a)(i)-(ii).

⁶⁰ *Ibid.*, s. 13.

It is a relatively common theme in other related pieces of legislation, including Ontario's PHIPA, that there is some provision for waiver of access fees if it is deemed "fair and equitable."⁶¹ Another notable aspect common in other jurisdictions' legislation on this matter is an express prohibition against data custodians charging additional fees to those prescribed by statute.⁶² It should be noted that Manitoba does not charge a fee for correction of an error in a person's health information.⁶³ New health privacy legislation should build on this fair practice by waiving or minimizing fees for notation of a disagreement in the event that a request for correction is not accepted. In these ways, the financial deterrent to information access can be lessened where appropriate. It is recommended that regulations take a sympathetic view toward waiver of fees for basic access to one's own medical information, while looking at the legislation and regulations in the above-mentioned jurisdictions for guidance in creating a fees structure.

5) Security and Oversight

- What duties and obligations should be placed on data custodians to ensure privacy and confidentiality of personal health information is maintained?

Specificity of legislative provisions:

We submit that new PHI legislation be as explicit as possible when specifying privacy and security safeguards. This is particularly so with the increasing trend toward private health care facilities and other providers. Generally, compliance is more challenging within the private sector.

Most dedicated provincial health privacy legislation, such as Ontario's PHIPA and Manitoba's PHIA are specific in spelling out the safeguards a health data custodian must take when handling personal health information. In Ontario, which has a dedicated "accountability and openness" segment in its legislation, the custodian must obtain consent before collecting PHI, and collect no more information than necessary for a stated and specific purpose.⁶⁴ The custodian must secure the PHI it retains against loss, theft, unauthorized disclosure, modification, copying or disposal, and must inform the affected individuals in the event of any such privacy breaches.⁶⁵ It is instructive that Manitoba refers to the holder of PHD as a "trustee."

In addition to these broad and common-sense obligations, Ontario assigns the custodian a specific duty to ensure proper disposal of PHI, plus secure storage and transfer.⁶⁶ Following a disturbing incident in 2005 where medical records misplaced by a disposal agency were scattered on the streets of Toronto as part of a movie shoot, the Ontario Privacy Commissioner established detailed rules for health information disposal in a Fact Sheet entitled "Secure Destruction of

⁶¹ *Supra* note 20, s. 54(12).

⁶² *Supra* note 20, s. 35(1), *Supra* note 19, s. 10.

⁶³ *Supra* note 19, s. 12(6).

⁶⁴ *Supra* note 20, ss. 15, 18, 30(2). See also the specific privacy and security provisions set out within Quebec's *Health Services and Social Services Act* as referenced in *Supra* note 17.

⁶⁵ *Ibid.*, ss. 12(1), 12(2), 16(2).

⁶⁶ *Ibid.*, ss. 12-13.

Personal Information.”⁶⁷ These included general principles, such as stipulating the destruction of paper records by irreversible means, and that electronic records must be disposed of by destroying storage media or using wiping software. Additionally, the publication discusses how the HDC should deal with third parties to ensure that no unauthorized personnel come into contact with PHI during the disposal process.⁶⁸ If using an information disposal service, it is recommended that the HDC enter into a detailed contract specifying how the disposal is to be done, by whom, and assigning responsibility if anything goes wrong.⁶⁹ The Commissioner’s fact sheet included sample clauses for a proper information disposal contract, illustrating the extent of the IPC’s active involvement in ensuring compliance.⁷⁰

As noted above, when framing health privacy legislation, New Brunswick would do well to consider the vital role that third-party providers now play at all stages of the information handling process. From computer consultants and security services to document shredding operators, there are many ways and circumstances in which third party contractors can come into contact with sensitive health information kept by HDCs. Following the above-mentioned privacy breach incident at a Sudbury methadone clinic, Ontario’s Privacy Commissioner discussed the need for health information custodians to clearly specify their privacy and security requirements when dealing with external service providers. Due to their statutory responsibilities under PHIPA, Ontario custodians are held to a higher standard than individuals in maintaining information security when contracting with other parties.⁷¹ In the Privacy Commissioner’s example (relating to contracting an outside party to install a wireless surveillance camera), she stated that health information custodians “should be capable of expressing their requirements for any technology dealing with personal health information, and should understand the necessity to inquire as to whether the system being recommended meets those requirements.”⁷² HDCs should inform outside providers of their statutory obligation to protect personal health information, and take appropriate measures to ensure that those third parties are not exposing that information to risk. The HDC should have a process in place to oversee the outside contractors in the course of their work, bind them to non-disclosure agreements where applicable, and set out detailed contractual obligations (as discussed in the case of disposal contractors) to ensure compliance. The ultimate onus should fall on the HDC to maintain security, and custodians should always keep this responsibility in mind: “Custodians must understand that while they can outsource services, they cannot outsource accountability.”⁷³

Obligation of HDC to destroy records:

The advent of electronic databases created the potential for almost unlimited capture and storage of health information. Since information in electronic format does not occupy significant physical space, and various storage media have become relatively inexpensive, it raises the problem that records will be retained permanently, and therefore be available for use, misuse, and potential unauthorized disclosure long after their original purpose is satisfied. Manitoba’s

⁶⁷ Ontario, Office of the Information and Privacy Commissioner “Fact Sheet: Secure Destruction of Personal Information”, December 2005, online: <www.ipc.on.ca/images/Resources/up-fact_10_e.pdf> at 1-2.

⁶⁸ *Ibid.* at 2.

⁶⁹ *Ibid.* at 2, 4.

⁷⁰ *Ibid.* at 4.

⁷¹ *Supra* note 34 at 10.

⁷² *Ibid.* at 14.

⁷³ *Ibid.* at 15. Comment by Commissioner Ann Cavoukian.

PHI statute provides some possibility for regulating mandatory records destruction, an issue that has otherwise largely escaped legislative notice in other jurisdictions. Section 66(1) allows the Lieutenant Governor in Council to make regulations “governing policies of trustees concerning retention periods for personal health information and respecting the destruction of that information.”⁷⁴ While this is a good starting point, the time is overdue for more specific legislation on this most important facet of a modern health privacy scheme. Health data custodians should be required to keep information only as long as it is reasonably needed for a specific purpose. Unless required or allowed by other legislation such as Archives statutes, or specifically authorized by the individuals concerned, health information should be destroyed following a reasonable period after the authorized health objectives have been fulfilled.

Compliance:

New Brunswick’s new health privacy legislation should place the onus on the health data custodian to prove its compliance with applicable privacy and security standards and other requirements. Each HDC should be required to conduct self-audits and produce annual compliance reports. Such formal attestations of compliance would create a potential for legal liability for a negligent or untruthful attestation. This would reduce monitoring and compliance costs for the oversight body. In the event of a security or privacy breach, there should also be a disclosure obligation by the HDC to the person or persons whose PHI was or may be compromised. There should be stiff penalties for attempting to obstruct investigation or conceal wrongdoing. For example, Ontario’s PHIPA provides fines of up to \$50,000 for an individual, and \$250,000 for an institution, which apply to a wide assortment of health privacy malfeasance including interference with investigation.⁷⁵ We submit that the imposition of a self-auditing duty on and the provision of a strict disclosure and penalty scheme would result in a very effective compliance system for HDCs with minimal costs to the regulator. Similarly, we support the creation of a statutory ‘private right of action’ so that individuals may enforce their privacy rights against negligent or malfeasant health data custodians independent of the regulator’s intervention.

Another important aspect of Ontario’s legislation is its acknowledgment of the need for public accessibility as well as education within departments about the rights and responsibilities contained within the legislation. To that effect, PHIPA requires that each HDC appoint a contact person within their organization to respond to inquiries, educate colleagues about obligations and facilitate overall compliance.⁷⁶ Further promoting accessibility, HDCs must prepare written statements to the public about their PHI rights.⁷⁷

Ontario’s *Freedom of Information and Protection of Personal Privacy Act* and equivalent municipal legislation both provide for the Privacy Commissioner to authorize mediation as an alternative to formal adjudication. A 2005 report by the Ontario Privacy Commissioner cites a 55% success rate in fully resolving mediated appeals regarding access to information, which

⁷⁴ *Supra* note 19, s. 66(1)(f)

⁷⁵ *Supra* note 20, s. 72(1)(a), (g)-(h), 72(2).

⁷⁶ *Ibid.*, s. 15.

⁷⁷ *Ibid.*, s. 16.

saves the time and cost associated with court.⁷⁸ This option would be particularly appropriate in a health information context in cases where there is a dispute over a patient's access to his or her own record, or relates to a correction thereof. Mediation also puts a human face on government - by agreeing to meet and negotiate with an aggrieved party, public institutions can show that they take the public's concerns about personal privacy seriously.⁷⁹ The inclusion of a mediation option, at the Ombudsman/Privacy Commissioner's discretion, should be considered for inclusion in New Brunswick's personal health information legislation.

- What form of independent oversight should be used?

New Brunswick's needs to enforce its personal health data legislation through an independent body which reports directly to the legislature. That body must have significant enumerated powers, including the ability to issue binding orders, particularly orders to release or sever PHD or to compel data custodians to improve security. In Ontario, the Privacy Commissioner has the power to make legally binding orders, while New Brunswick's present equivalent, the Ombudsman's office, may only make recommendations.⁸⁰

An effective enforcement body would require a sufficiently wide mandate to conduct proactive audits and initiate investigations as well as follow complaints. One of the key weaknesses in New Brunswick's current model of enforcing privacy abuses is that it is entirely complaint-based, relying on the individual to come forward to the Ombudsman or courts after an alleged violation has taken place. In some other provinces, and particularly in the field of personal health information, a more pro-active approach is taken. Under an auditing and reporting model, the appropriate agency not only takes complaints from individuals, but also actively examines the agencies under its purview for problematic incidents and trends. In Ontario, for example, the Privacy Commissioner is empowered to audit public service providers to ensure private information is being properly safeguarded.⁸¹ New Brunswick should seriously consider the possibility of introducing such a scheme. There should, however, also be provision to allow general access to the Court of Queen's Bench if any of the parties involved wish to appeal the outcome of the regulator's ruling, or if the regulating body wishes to refer a matter to the courts.

In addition to its oversight and enforcement function, this agency should also play an education role. For the data custodians that it oversees, it should issue fact sheets and guidelines spelling out preferred practices for compliance, such as the information disposal advice distributed by the Ontario IPC's office. It should also play a role in informing the public of their privacy and access rights, and what to do if they encounter difficulties accessing their patient information or are concerned about threats to their health privacy. This can be delivered through advertising campaigns as well as more unconventional methods such as public workshops. An informed populace is vital for a functioning democracy, and making the people aware of their health

⁷⁸ Ontario, Office of the Information and Privacy Commissioner, *Annual Report 2005*, (Province of Ontario, 2005) at 44.

⁷⁹ Ontario, Office of the Information and Privacy Commissioner, *It's Your Information: Information and Privacy Commissioner / Ontario Annual Report 2001*, (Province of Ontario, 2001) at 6.

⁸⁰ *Right to Information Act*, S.N.B. 1978, c. R-10.3, s. 10(3).

⁸¹ *Freedom of Information and Protection of Privacy Act* R.S.O. 1990 c. F.31, s. 65.1(8).

privacy rights would go far toward building public trust of the institutions that care for their sensitive information.

It is also important that an oversight body have sufficient resources, both financial and human, to carry out its mandate. Currently, New Brunswick's Ombudsman's office ranks as one of the most poorly funded in the nation, particularly with regard to its information and privacy function, on which the province spends \$0.14 *per capita*. This is least among all the provinces, and is far behind the likes of Manitoba, at \$0.88, Ontario, at \$0.93, and Alberta, which spends \$1.36 *per capita*.⁸² New Brunswick is second-last to PEI in raw expenditure on its Information and Privacy Office. This severely limits the attention that the Ombudsman's office can give to privacy cases, and certain types of complaints, such as employer-employee privacy disputes, are too complex for that office to handle at all due to scarcity of current resources.

Part of the problem is the wide portfolio assigned to this office: in addition to the usual functions of an Ombudsman, the New Brunswick office also operates as Youth Advocate and *de facto* Information and Privacy Commissioner. Most provinces, by contrast, have a separate office dealing specifically with information and privacy. We submit that the province should create a separate office dealing only with information and privacy issues, as other jurisdictions have. We urge the Task Force members to specifically address these funding issues should they recommend that oversight of New Brunswick's PHD scheme be assigned to our Ombudsman.

Conclusion:

We hope that the recommendations arising from the deliberations of the Personal Health Information Task Force will lead to significant changes to how personal health data is regulated and handled within our province. We hope also that the Task Force members find this submission of assistance to them.

⁸² New Brunswick, Office of the Ombudsman, *Annual Report 2005/2006* (Province of New Brunswick, 2006). All figures estimates for 2006/2007.