

Submission to the New Brunswick Personal Health
Information Task Force

Bernard Richard, Ombudsman and Child & Youth
Advocate
July 4, 2007

Happiness lies, first of all, in health.
George William Curtis

Grounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual. For this reason alone, it is worthy of constitutional protection, but it also has profound significance for the public order. The restraints imposed on government to pry into the lives of the citizen go to the essence of a democratic state....

...

... hospitals [are] one of the specific areas of concern in the protection of privacy. This is scarcely surprising. At one time, medical treatment generally took place in the home, or at the doctor's office, but even then, of course, the confidentiality of the doctor-patient relationship was fully accepted as an important value in our society. ... This is obviously necessary if one considers the vulnerability of the individual in such circumstances. He is forced to reveal information of a most intimate character and to permit invasions of his body if he is to protect his life or health. Recent trends in health care exacerbate the problems relating to privacy in the medical context, particularly in light of the health-team approach in an institutional setting and modern health information systems. If the health-team approach gives a patient easy access to a wide range of medical services, it inevitably results in the fragmentation of the classical doctor-patient relationship among a team of medical and para-medical personnel. The dehumanization that can result has led some hospitals in the United States to appoint an ombudsman for patients.

Gerald V. Laforest, Supreme Court Justice, *R. v. Dymont*

The doctor-patient relationship is one of the most important non-familial relationships that many of us have in our lives. Many of us share information with our physician or other health care provider that we would not share with a parent, spouse or child. If a patient believes the information he or she has entrusted to their health care provider has been breached, it could be detrimental to the relationship and perhaps even to the health of the patient. In order to have a viable health care system, we need to ensure that the special doctor-patient relationship remains intact. At the heart of this is ensuring that a patient's right to privacy is protected

As technology advances there is a growing need for legislation that specifically addresses access and privacy issues for personal health information (hereafter, PHI). Currently, the provinces of Alberta, Manitoba, Saskatchewan and Ontario have specific legislation to address this issue. British Columbia has private sector legislation that encompasses health information and Newfoundland is in the process of drafting health information privacy legislation. In Quebec the *Act Respecting Health and Social Services* provides for protection of PHI. The health information protection legislation in these jurisdictions emphasizes the obvious necessity for legislative reform in New Brunswick. Given the sensitive nature of health information, the expanding use of technology, and the unique nature of consent in the health care regime, I strongly believe that the New Brunswick government should implement PHI protection legislation.

As I outlined in my submission to the Task Force on Right to Information and Protection of Personal Information led by Donald Savoie, I believe that time has come to codify all our existing information and privacy laws into one statute, an Information and Privacy Rights Code. I envision within this Code a dedicated chapter that addresses PHI specifically. Codifying all access and privacy laws into one piece of legislation will help to ensure that health information managers, doctors, nurses, dentists, physiotherapists and all care-providers within a given health team are guided by a consistent set of rules, one which is specific to their needs, but consistent with Canadian approaches in the field elsewhere, and consistent also with the general privacy and information rights guaranteed under the Code.

New Brunswick is significantly behind other jurisdictions in PHI protection; however, we can use this to our advantage by learning from legislation in other provinces. We can use the experiences of other jurisdictions to determine what works and what does not work instead of reinventing the wheel. We should also endeavor to be consistent with other provinces in an effort to develop a uniform approach across the country for the treatment and protection of PHI, ensuring a similar standard of privacy rights for individuals across Canada.

In my submission to the New Brunswick Task Force on Right to Information and Protection of Personal Information, I emphasized the importance of access and privacy legislation. As Mr. Justice Laforest pointed out in *R. v Dymont* twenty years ago, privacy and health information privacy in particular is profoundly important to our individual well-being, but protection of this fragile freedom also goes to the essence of our democratic state. I have expanded on the need to approach reforms in this area from a rights-based framework in my submission to the Savoie Task Force and will not be revisiting those issues here but refer the Personal Health Information Task Force to that paper for my views on access and privacy legislation generally, as well as the historical context.

In the pages which follow, I will endeavour to cover the issues raised by the Personal Health Information Task Force in its consultation documents and to offer such advice as I have gleaned from my colleagues in jurisdictions that have been enforcing PHI laws for several years already.

The need for consistency

All provinces should establish PHI protection legislation to ensure consistency throughout the country. For jurisdictions that have neither specific health information privacy legislation nor private sector privacy legislation, such as New Brunswick, health information is covered by separate public and private sector legislation. In New Brunswick *The Protection of Personal Information Act*¹ (POPIA) regulates how personal information held by public bodies is treated, whereas health information held by private bodies is subject to the *Personal Information Protection and Electronic Documents Act*

¹ *The Protection of Personal Information Act*, S.N.B. 1997 C. P-19.1

(PIPEDA).² Although the fundamental and guiding principles contained in POPIA and PIPEDA are the same, the legislation is different; consequently, health information providers may be subject to different legislative rules depending on which Act applies to them.

As I recommended to the Savoie Commission, there should be an Information and Privacy Rights Code for the province. Within this Code there should be a separate chapter or part for PHI. Addressing the specific requirements of PHI in a dedicated chapter within the Code will send a strong message to health care providers to get serious about personal health information management. Although the current law does apply to public bodies within the health care sector, patients and health care workers are not clear that it applies and are even less clear on what implications the law has for PHI management. New legislation should be more detailed and capture concerns about PHI management by private health care providers, insurance companies, or employers. There would need to be training for health sector employees on precautions for handling PHI as opposed to personal information generally.

It is not enough for individual provinces and territories to adopt health information privacy legislation in each jurisdiction; they must also work together to ensure harmonization across the country so that when individuals move from one part of the country to another they can be assured that their PHI is treated consistently.³ Any legislation that the province introduces regarding PHI should be ‘substantially similar’ to PIPEDA in order to be exempted from its provisions, so that only one piece of legislation applies.

Technology

It is trite to say that technology is changing at a very rapid pace. Significant amounts of information can be readily accessible via the Internet. Prior to computers, medical records used to be locked in filing cabinets in various health care providers’ offices. With computers and technological advances, medical records may now be compiled in one location and can be threatened by internet security issues.

In 2002, the Kirby and Romanow Reports recommended the creation of national electronic health records (EHR) as they believed that EHRs could improve health care delivery⁴. Academics have predicted that EHRs will ‘enhance the effectiveness and efficiency of health care and play a key role in health system reform.’⁵ All jurisdictions have already had started e-health projects with the assistance of Canada Health Infoway. Canada Health Infoway is the independent, not-for-profit organization whose Members

² *Personal Information Protection and Electronic Documents Act*, 2000 C. 5

³ Canadian Institute for Health Information, ‘*Brief to the British Columbia Special Legislative Committee on Information Privacy in the Public Sector*’, October 2000.

⁴ Ries, Nola & Geoff Moysa ‘*Legal Protections of Electronic Health Records: Issues of Consent and Security*’ (2005) 14 Health L. Rev. No. 1, 18-25 at paragraph 1.

⁵ Ries, Nola ‘*Patient Privacy in a Wired (and Wireless) World: Approaches to Consent in the Context of Electronic Health Records*’ (2006) 43 Alta. L. Rev. 681-712 at paragraph 1.

are Canada's 14 federal, provincial and territorial Deputy Ministers of Health⁶. In conjunction with other agencies and organizations, Canada Health Infoway has over 100 projects, either completed or underway, delivering electronic health record solutions.

Electronic health records are changing the way we look at privacy from a health perspective. While EHRs have significant benefits to the health care system, they also raise serious concerns over the privacy of PHI.⁷ We are concerned regarding the security of electronic documents and information exchanged over the World Wide Web. We are also concerned that Health Departments may not be bringing privacy to the table when discussing the implementation of EHRs.

It is not enough to simply encode or encrypt information as it travels across the web. We also have to insure that only authorized users have access to PHI. In Alberta a Health clerk recently accessed, on six different occasions, the PHI of the wife of the man with whom she was having an affair. Alberta courts imposed a fine of \$10,000 upon her for this violation of the patient's privacy. We strongly believe health information privacy legislation needs to be in place to address the subject specific issues that arise because of technological advances in society.

To whom should the legislation apply?

I believe that anyone who has access to PHI should be included as a data custodian. Physicians, pharmacists, staff, regional health authorities, the Department of Health, employers, private health care facilities—everyone who uses or has access to this type of information should be included. Additionally, the Task Force should consider including regulatory bodies and employers who collect their employee's PHI. The chain of privacy protection is only as strong as its weakest link; if someone in the information-handling chain is not included in legislation, then the opportunity for a breach is enhanced.

What type of information should be covered?

In his 2001 speech to the Canadian Institute for Health Information, the then Privacy Commissioner for Canada stated, "Nothing is as personal or as private as the intimate details about the state of our own minds and bodies".⁸ Some of these intimate details are so personal that although we may share them with our physician or other health care provider in order to find a solution to an ailment, we may choose not to reveal this information to those closest to us. Arguably, the majority of people would not want their PHI disclosed in any way to the public, their employers, co-workers, or neighbors.

⁶ <http://www.infoway-inforoute.ca/en/WhoWeAre/Overview.aspx>

⁷ Supra, note 7.

⁸ Privacy Commissioner of Canada, "Condition Critical: Health Privacy in Canada Today", (Speech delivered to the Canadian Institute for Health Information, Toronto, 18 June 2001), Office of the Privacy Commissioner of Canada www.privcom.gc.ca/speech/02_05_a010618_e.asp

The Manitoba *Personal Health Information Act* emphasizes the sensitive nature of PHI in its preamble, stating that “health information is personal and sensitive and its confidentiality must be protected so that individuals are not afraid to seek health care or to disclose sensitive information to health professionals”.⁹ The preamble to Saskatchewan’s *Health Information Protection Act* further reminds us that individuals provide PHI with the expectation officials will keep the information confidential and respect their personal privacy.¹⁰ Legislation such as that found in Saskatchewan and Manitoba, in addition to providing a legal framework for the protection of PHI, educates individuals and organizations involved about the sensitivity of the information that they have access to. The sensitive nature of the information that trustees and custodians collect, or have access to, requires that the information is treated in a way that respects the principles of privacy legislation in general and health information specifically; hence, the need for legislation to address PHI per se.

The definition of PHI in legislation should be broad but include specific guidance to trustees and others in determining what needs to be protected. Any legislation need not impede the functioning of the health care system and should not prevent governments from striving constantly to improve how the system functions. Both recorded and unrecorded information should be included. I believe that health-related aspects of legislation should be limited to PHI and should not apply to anonymous or statistical health information that cannot reasonably be expected, either by itself or combined with other information, to allow the individual to be identified. A general principle that may bear mention in the Code is that protection of privacy should not compromise patient care. Similarly, over the long term patient care may be compromised if necessary medical research cannot be carried out to facilitate advances in medicine, diagnosis and treatment. Here again the choice is not between research and privacy, but research must henceforth be undertaken in a fashion that is consistent with the goals of protection of personal health information.

Data custodians

To date, New Brunswick has taken a reactive approach to privacy information in general. We now need a more proactive approach. Mr. Justice Laforest also underscored the need for this approach in *Dyment*:

One further general point must be made, and that is that if the privacy of the individual is to be protected, we cannot afford to wait to vindicate it only after it has been violated. This is inherent in the notion of being secure against unreasonable searches and seizures. Invasions of privacy must be prevented, and where privacy is outweighed by other societal claims, there must be clear rules setting forth the conditions in which it can be violated.

In other Canadian jurisdictions PHI laws have taken this advice to heart and have established detailed audit and reporting provisions as the primary compliance mechanisms for such statutes. The PHI laws also of course have complaint based

⁹ *Personal Health Information Act*, SM 1997, C.51

¹⁰ *The Health Information Protection Act*, R.S.S. 1999 Chapter H-0.021

mechanisms and offence provisions and other such enforcement tools. However audit and reporting mechanisms imposed on all data custodians has proven to be, along with significant training and educational efforts, the most successful means in bringing about a culture of personal health information protection in health care settings. It is recommended that New Brunswick opt for a similar approach.

The Code's Chapter on PHI should also detail the Commissioner's authority to conduct spot audits of his own motion and to require the preparation and filing of Privacy Impact Assessments where new health programs or data treatment or applications raise personal health information concerns. Data Custodians should be given the resources to develop the proper safeguards to protect personal information, to conduct privacy audits, to develop policies and procedures and to respond to requests. This has significant resource allocation implications for government over the short to medium term in meeting the training challenge. Consultation with the Newfoundland ATIPP office would be helpful in gaining insight into the cost of such reforms. In the Alberta example above, the privacy breach could not have occurred if there had been proper safeguards placed on PHI so that only authorized personnel could access it. We need to provide data custodians with the tools they need to have efficient and effective flow of health information without compromising a patient's right to privacy.

Consent

Consent is one of the foundations of privacy legislation. In New Brunswick, the *Protection of Personal Information Act* (POPIA) states that, "the consent of the individual is required for the collection, use, or disclosure of personal information, except where inappropriate". Similar types of consent provisions are contained in PHI privacy legislation. For example, the Saskatchewan Act preamble states that, "wherever possible, the collection, use and disclosure of personal health information shall occur with the consent of the individual to whom it relates."¹¹

This principle was affirmed by the Supreme Court of Canada in *Ciaraliello v. Schacter*¹² when the court quoted from the Ontario Court of Appeal decision in *Fleming v. Reid*¹³:

The right to determine what shall, or shall not, be done with one's own body, and to be free from non-consensual medical treatment, is a right deeply rooted in our common law. This right underlies the doctrine of informed consent...The fact that serious risks or consequences may result from a refusal of medical treatment does not vitiate the right of medical self-determination...it is the patient, not the doctor, who ultimately must decide if treatment—any treatment—is to be administered.

Consent is a major consideration for legislators drafting PHI privacy legislation and determination of the boundaries of consent is critical, in light of the above-noted challenges. It is also important to determine the standard form of consent in the health

¹¹ Supra, note 3.

¹² [1993] 2 S.C.R. 119 at page 135

¹³ (1991), 4 O.R. (3d) 74 (C.A.), at page 85

care context. Should the legislation require express (formal written or verbal) consent which may be difficult to obtain in emergencies? As indicated by the Alberta Information and Privacy Commissioner, express consent may be difficult to obtain regarding specific disclosures by electronic means.¹⁴ As noted by the Personal Health Information Task Force in their Background Paper, implied knowledgeable consent is the model used in some provinces, namely Ontario. After consulting with other Privacy Commissioners, I have determined that implied knowledgeable consent is the best option. Without provisions requiring implied knowledgeable consent the legislation would most likely not be considered “substantially similar” to PIPEDA and then both pieces of legislation would apply and paramourcy issues would result.

The Manitoba experience also indicates that legislators need to address the policy issue of whether other professionals, such as clergy and police, should have access to PHI without the express consent of the patient.¹⁵ Express consent occurs when the individual gives formal written or verbal permission to the specific request for access. Prior to PHI privacy legislation, it was not uncommon for hospitals to provide religious leaders with copies of the list of hospital patients so that they could visit members within their religious community.¹⁶ With the implementation of PHI privacy legislation, hospital administrators will need to strike a balance between privacy and proper practice of a patient’s faith.

Some PHI privacy legislation has also addressed disclosure of personal information to the police. In 2006, the Alberta government amended its *Health Information Act*¹⁷ permitting disclosure of certain PHI without consent to the police and/or the Minister of Justice and Attorney General if needed to protect the health and safety of Albertans or if necessary because the information relates to the possible commission of an offence.. Some argue that such amendments are both unwise and unconstitutional.¹⁸ A rights based framework as outlined in the proposal for an Information and Privacy Rights Code is best suited to help determine these and similar issues that will arise in the area of personal health information management. Strong privacy guarantees are required if the twin goals of patient care and democracy are to be protected from further encroachment.

To summarize, implied knowledgeable consent should be the model adopted by New Brunswick when it drafts its PHI protection legislation. The use and disclosure of PHI without consent should be limited and legislators need to insure that privacy does not take a back seat to other aims such as drug monitoring.

Fees

¹⁴ Ibid 5 at paragraph 25

¹⁵ Neufeld, Renata ‘*The Realities of Implementing Health Information Legislation: The Manitoba Experience, 1997-2004*’ (2005) 14 health L. Rev. No. 1, 47-50

¹⁶ Ibid.

¹⁷ R.S.A. 2000, C. H-5 as amended by *Health Information Amendment Act*, 2006, SA 2006, C. 18.

¹⁸ Bailey, Tracey M. & Steven Penny ‘*Healing, not Squealing: Recent Amendments to Alberta’s Health Information Act*’ Health Law Review – 15:2 (2006)

The existing fee and cost structure has served the province well over the past thirty years and is, in fact, one of the areas where our law compares favorably with the provisions in other jurisdictions. The idea of introducing a ‘money for value’ or ‘cost recovery’ system is inconsistent with the concept that access assists the general goal of having an informed citizenry in a fully functioning democracy. It is essential that fees be reasonable.

Compliance

As I recommended in my submission to the New Brunswick Task Force on Right to Information and Protection of Personal Information, new legislation should establish an independent Information and Privacy Commissioner as a distinct legislative Officer with appointment provisions and guarantees of independence modeled on the recently amended provisions of the *Ombudsman Act*. I do not believe it is necessary to establish a separate commissioner to deal specifically with health information issues; however, there should be a separate and independent Information and Privacy Commissioner overseeing all privacy and access legislation in the province.

Resourcing

If the Ombudsman’s office is to have an expanded role in privacy issues, adequate resources will be needed to carry out this role. Thus, in addition to our compliance function, we would need to be more proactive on the research, education and legislative review front. As indicated in my annual report of 2005/2006 New Brunswick is significantly behind other provinces with respect to funding for privacy and access issues.

Not all RHAs have their own privacy policy, few RHAs have dedicated Chief Information Officers or Chief Privacy Officers and these individuals do not often have the required standing within hospital administrations to drive meaningful implementation of privacy laws and policy. In the area of private clinics and professional health care providers offices, everything remains to be done, starting with a credible and representative audit of existing privacy practices and benchmarks.

In this context, the establishment and proper resourcing of an independent oversight body is just a small piece of the pie. Under a proposed Information and Privacy Rights Code I have recommended the creation of a dedicated Access to Information and Protection of Privacy Office (an ATIPP Office), housed either with the Attorney General’s Office or with Supply and Services, to direct and implement the training and policy development piece. I would recommend that the PHI Chapter of the Code task the Deputy Minister of Health with specific accountability for the implementation of this Chapter of the Code and detail reporting requirements to the ATIPP Office on implementation goals and milestones. The central ATIPP Office would therefore play a supporting and coordinating role with Department of Health Officials and Chief Privacy and Information Officers in the RHAs and other Data Custodian representatives in implementing the Code’s PHI provisions. The ATIPP trainers would advise and assist in the processing and mediation of access requests and privacy complaints, develop routine access and privacy policies, advise on how to carry out privacy audits and privacy impact assessments, and train staff on how to administer the Code.

Conclusion

Specific legislation that addresses PHI protection is needed in New Brunswick and in much of the rest of Canada. Several provinces, notably Manitoba, Saskatchewan, Alberta and Ontario, have provided the rest of the country with precedents and learning experiences to facilitate other jurisdictions' entry into this legal arena. They are examples of how the legislation works, what it needs to address and how it can be implemented.

I am recommending that New Brunswick strengthen its access and privacy legislation by establishing an Informational and Privacy Rights Code. This code should include a Part dedicated to personal health information. The province should also establish a separate Information and Privacy Commissioner to oversee compliance with this Code. Personal health information privacy rights should be balanced with patient care; however privacy needs to be part of the system and not an afterthought. This is very important as we build EHRs and increase our use of technology. The Code should have a broad array of enforcement mechanisms. Meaningful remedial order-making powers should be conferred upon the Commissioner. However, the principle enforcement mechanism for the Code's PHI provisions should be through training, and audit and reporting mechanisms. The legislation should have implied knowledge consent as its model for collection, use and disclosure of PHI. Most importantly, resources needed to be increased substantially within the health care system and to the central administrative authority and the legislative oversight body in order to ensure the Code's consistent and appropriate application.