



Creating a Privacy Culture in Health - Implications for the Practical Professional

Note: This paper was presented in an abbreviated version as part of the Ethics @ Ryerson Speaker Series 2006/2007: Privacy and Access Issues Across the Professions on March 1, 2007. The Ethics at Ryerson Speaker Series is part of Ryerson University's Ethics Network, which seeks to provide a venue for faculty, scholars, students, professionals, and community members to meet and explore mutual issues and interest in practical and professional ethics.

I want to thank Ryerson University for giving us the opportunity to talk to you today about the very important topic of privacy within the health professions. Consistent with the title of this Speaker Series, “Privacy and Access Issues Across the Professions”, we believe that it is very important to address this issue.

I propose to focus on three key precepts – or principles - that in my view constitute the essence of health privacy and what they mean for health practitioners. These three principles of health privacy – and in fact any modern privacy regime – are *consent*, *access* and *security*. I will show how these principles evolved from their antecedents under the laws prior to PHIPA and what these principles mean for the practical practitioner today.

The Background

When one looks at the historical experience, we know that privacy – or confidentiality – has long been a recognized precept within the practice of medicine and the providing of health care. And for good and valid reasons: there is probably no category of personal information which individuals view as more sensitive and private than that relating to their personal health. Information about one’s personal health not only reflects a person’s inherent well-being but may affect their self-esteem and perception of their ability to interact with and be part of their community – whether it be their family, work or the

broader society. In the workplace, for example, personal health information can be relevant to a person's job function or qualification for benefits such as insurance. Unintended or unauthorized disclosure of such information may have significant injurious impact on the individual's place within these contexts.

However, we know that while the privacy ethic has always underlain the practice of health care, it was a disparately recognized precept, only imperfectly stated or applied until the advent of the modern privacy laws.

Ontario's new privacy statute, the *Personal Health Information Protection Act*, 2004 - or "PHIPA" – is an embodiment of these new laws. It is the product of a decade of collaboration among a wide cross-section of stakeholders within the health sector including some very dedicated public policy-makers both within government and outside of it. The focus of these efforts has been to ensure that the law embodied as effectively as possible the dictates of good privacy practices in health, taking into account not only the key ethical principles but also the practical realities of professional practice and institutional environments.

PHIPA also reflects the widely recognized "Fair Information Practices" that are embodied in our national privacy law, the *Personal Information Protection and Electronic Documents Act*, usually known by its acronym "PIPEDA". PIPEDA represents the culmination of a separate but parallel track of development; one that ultimately merged with PHIPA when it was recognized to be "substantially similar" to PIPEDA. As a result, PHIPA supplants PIPEDA within the health sector in Ontario.

Interestingly, the original motivation to develop the general privacy laws – of which PIPEDA is the main Canadian product – came from the recognition at an international level of the tremendous potential for amassing and exploiting personal information through electronic means. By contrast, this consideration did not figure prominently in much of the original policy development for health privacy laws. However, as those laws were in their final stages of development, the impact of technology came to be recognized as a key motivator. So, significantly, we see that Roy Romanow's 2002

report on the future of health care in Canada addressed privacy almost exclusively in the context of the development of electronic health records.

In fact, some of the most critical challenges facing the integrity of a privacy culture within the health sector involve those posed by the adoption of technology – not only as the means for recording and maintaining information – but also as the medium of communication within care groupings and other health networks.

Recall that we are talking about health information that is in any way identified with an individual. So it may include a diagnosis, the daily record of care, prescription information and care or service orders. Personal information includes even the fact that a person is receiving care or is a client of a care-giving institution.

The Consent Principle

Firstly, the consent principle. Most importantly, privacy means the right and the ability of an individual to *control* the collection, use and disclosure of his or her personal information. In privacy law, this control right is reflected in the *consent principle* that underlies all aspects of the legislation. This principle says that personal information may only be collected, used or disclosed for purposes to which the individual has *knowledgeably* consented – unless the law makes an exception and permits collection, use or disclosure for specific purposes that do not require consent, such as for funding purposes, disclosure to law enforcement authorities, or research.

Consent may be given expressly or implicitly. Significantly, in PHIPA and other health privacy laws in Canada, *implied* consent is recognized for a broad category circumstances in which the individual receives health care – essentially it is implied for the collection of personal information and the use or disclosure of that information for purposes of delivering health care to the individual. The individual’s “circle of care” – a term that is not defined in the Act – means those health practitioners and institutions that are or may be providing that health care.

Implied consent is therefore important. However, it is also important to recognize that *express* consent must be obtained in circumstances where information is being used or communicated for purposes not directly involved in the health care of the individual, or is being disclosed to someone who is not a health practitioner, even if for purposes related to health care. An example of the first case might be the disclosure of a patient's contact information by a hospital to another institution for fund-raising purposes. An example of the second case would be disclosure of medical information by a doctor to the patient's employer or insurance company. In each of these circumstances, express consent is required.

Looking back to the precursors of the modern health privacy laws – specifically the various statutes and professional rules that embodied certain, albeit incomplete, privacy protection – we note recognition of the concept of *consent to disclosure*. However, the governing rule was not stated as “privacy” but *confidentiality* of the medical record: an obligation that derived from the physician's Hippocratic Oath. Essentially, medical records were to be kept confidential and not disclosed to third parties unless consented to by the patient. The modern privacy-based concept of a patient's *control* over the record or the information contained in that record was largely absent and exceptions to the consent to disclosure rule, such as for research purposes, were not clearly defined. Furthermore, without the *control* precept, the old laws had no concept of the individual's *ownership* of the record – which it may be argued is implied in the modern laws.

While implied consent is clearly available, a prudent, more preferable, approach is for the health care provider to obtain express, written consent. Such express consent has several advantages. Firstly, it sets out clearly the purposes for which information is collected – thereby addressing the *knowledge* requirement of any consent. Secondly, it ensures that any uses or disclosures for which implied consent does not suffice, are addressed. Furthermore, with a documented form of consent, health care providers have a ready reference to guide them over the future course of care for the individual.

The Right of Access

The second key precept of privacy embodied in the new laws is the *right of access* to one's personal health record. Access is a key element of privacy and an adjunct of the control right: if it is accepted that an individual has *control* over his or her personal information, then it goes without saying that the individual should be able to review that information and, if inaccurate, or documented for uses that the individual has not authorized, then to correct or update this information.

While this nexus seems self-evident today, prior to the modern era of privacy it was not clearly recognized and faced much resistance in being embraced as a clear statutory right. Notwithstanding the recommendation of then Mr. Justice Horace Krever in his 1980 *Report of the Commission of Inquiry into the Confidentiality of Health Information* – that the right of an individual to access his or her health information be legislated – it was not until a 1992 Supreme Court of Canada case that the right was unequivocally recognized.

The *access principle*, now universally recognized as a basic privacy concept, was probably the most difficult to establish within the health sector. It is interesting to note that while access is now clearly recognized as a privacy right, the Supreme Court, speaking only fifteen years ago, was not able to point to any legislation, including the *Charter of Rights and Freedoms*, that clearly established the right. Instead, it found that the right existed within the *fiduciary nature* of the patient/health care provider relationship. A fiduciary is a trustee in the law's eyes and in the Supreme Court's view an individual's personal health information is maintained by a health care provider as trustee – in other words, it is information belonging to the individual that is simply being held in trust for and on behalf of that individual.

Subsequent to the Supreme Court's decision, in 1994, Ontario enacted the *Long Term Care Act* which for the first time recognized a clear and unequivocal right of access for all health care clients. However, it was only with PHIPA's becoming law that the right was clearly enunciated and with the general application that Mr. Justice Krever had recommended.

Reticence in embracing the right of access was often framed in the context that having the information might cause psychological – or possibly physical – harm to the client. Other concerns cited over the years included providing potentially unfounded grounds for litigation.

One can understand that as a general precept, medical practitioners were not anxious to embrace the access concept. To a certain extent they may view the records they keep about their clients as their own personal files. By their nature, such records contain observations and notes made by the health care practitioner and such information as recorded may be of a sensitive nature. It may contain observations that the practitioner intends for internal administrative purposes which, while relating to the provision of care to a particular individual, is primarily intended to be used for purposes not directly related to direct care. An example would be information reflecting difficult communications between a practitioner and the client. The practitioner may want to record circumstances in which the client has expressed dissatisfaction with the care, but not want that information to be accessible to the individual.

Another, understandable, reason for health care practitioners to wish to limit the information accessible to their clients is potential liability. This is not to say that they want to hide possible errors but more that they want to avoid possible misunderstandings regarding events occurring within the course of care or decisions taken within that context.

However, the reality is that under the modern privacy laws, an individual's access to the health record is a basic tenet which not only must be recognized but must be actively embraced by health care practitioners and institutions.

In embracing the access principle, health care practitioners must be cognizant that the records which they create contain information that is accessible to and, as I have posited, under the control of the individual client. In this vein, they should be aware that the limitations on access set out in the legislation are quite narrow. Essentially, these limitations permit a practitioner to refuse to grant access *only* in circumstances in which

the information was collected in the context of legal proceedings or an investigation, or was provided by an individual who did so on the basis that his or her identity would remain confidential, or if the disclosure of the information could result in serious physical or serious harm to either the individual or another person.

What this framework of access to the personal health record means is two-fold.

Firstly, practitioners must record information related to the health care that they are providing in a manner that is presentable to the individual and, potentially, others outside of the health sector. If there are difficult circumstances that occur within the relationship, care should be taken to record these in a neutral, objective form without personal comments or epithets. A practitioner should understand that while the health record is private information, the individual might choose to make some or all of it public – including to the media.

Secondly, the information contained in the personal health record should be limited to that directly related to providing care. Administrative issues including those related to management of the health care should be documented separately. PHIPA is very clear that any information contained within an individual's record will be considered personal health information and therefore subject to disclosure under the access right.

Security

The third key precept of the modern privacy laws is *security* – the obligation of the data collector to protect the personal information that it holds and to ensure that it is secure. This is the *security principle* of the fair information practices.

While the security precept was implied under much of the pre-PHIPA law and the professional practice rules, it was only with the enactment of the modern privacy legislation that this obligation has been explicitly set out.

As I have noted, the approach to privacy prior to the modern laws focused on the concept of *confidentiality*. Confidentiality as a rule does imply security, however without

expressly stating the security requirement – which the old laws did not do – it failed to provide any guidance as to the standard of care expected, or the nature of the procedures that should be adopted.

The significance of this requirement is important: not only does it set a regulatory standard but it also creates a *civil standard of care*, which means that if practitioners or institutions fail to meet this standard, they may be liable in damages to the individuals whose information has been compromised.

The new laws not only articulate a required standard of security but contain, in varying degrees, guidance for data collectors as to the nature of the security systems and procedures that should be adopted. PHIPA's primary security obligation is however stated in quite general terms. It requires that a custodian take steps *reasonable in the circumstances* to protect information within its custody or control against theft, loss and unauthorized use or disclosure. The Act contains certain additional specific guidance, addressing protection against unauthorized copying, modification or disposal, secure handling and disposal of records. The Act also provides for regulations prescribing more detailed procedures for records retention procedures, electronic data collection and management and electronic network service providers. To date, only regulations relating to network service providers have been enacted. I believe that the lack of regulations respecting records management and electronic data procedures, clearly contemplated by the legislation, is a deficiency that must be rectified. This is particularly relevant to the burgeoning development of electronic health records and electronic health networks.

PHIPA's lack of detailed guidance respecting security procedures contrasts with the federal law, PIPEDA, which through its adoption of the CSA Model Code provides an outline of the nature of the protections that should be adopted. The PIPEDA rule makes clear that such protections should include physical, organizational and technological measures and provides examples of each of these categories. The PIPEDA rule also stipulates that organizations must ensure that their employees are trained in security procedures.

While this specificity of required procedures is not currently found in PHIPA, it is clear that, in order to comply with the legislation, custodians are *expected* to adopt detailed procedures. The only difficulty with this approach is that the law itself does not provide the required guidance. Instead, practitioners and institutions must pay expensive consultants and lawyers to tell them what they need to do!

Why is security such a critical element of a privacy regime?

Firstly, as I have noted, the elemental concept of privacy implies an individual's control over and in effect ownership of his or her personal information. Recognition of this concept dictates that if that information is entrusted to another person, that person must take appropriate precautions to prevent the information from being misused, lost or stolen. Furthermore, implicitly, a privacy regime recognizes that if personal information is misused, an individual may suffer injury - whether it be financial, psychological or physical. The security rule seeks to prevent such injury.

Within the health sector, these and other additional reasons underscore why the security rule and effective compliance measures are important. As already noted, the unauthorized disclosure of an individual's personal health information can have significant injurious impact – whether it be to the individual's dignity and self-esteem, the perception of his or her place in their family and community, or their workplace status. Clearly, this is the most important reason why personal health information must be protected with secure measures.

However, the nature of potential risks go beyond direct psychological and social impact upon the individual. As you know, *identity theft* has become a major concern today and it is a real concern within the health sector. Furthermore, beyond the specific issue of identity theft, there are concerns for protection of the integrity of the health record itself.

How can health information be used to commit identity theft?

If personal health information – whether it be an individual health card or information about a client's care - is stolen or falls into the wrong hands, it can be used to harm the

individual as well as the health care system. Let's look at an example. A client's health card number and other personal information may be used by fraud artists to steal an identity. The individual whose identity is stolen may suffer direct and immediate financial harm – such as through fraudulent credit card use. Other direct financial injury could involve mortgage or loan fraud. In addition, serious long-term harm may result to an individual's credit record and the various other important personal and financial indicia that we all take for granted.

Similar harm may result from identity theft within the health sector. An individual's health card enables the holder to obtain medical care free of charge. If a card bearing a stolen identity is fraudulently presented by someone seeking healthcare, not only is bogus information added to the innocent victim's health record but that information may compromise the very accuracy and integrity of health system databases.

Security means not only having the physical and technological systems to achieve a required level of protection but also the administrative procedures to ensure that such systems achieve that goal and where breach incidents occur, to respond and ensure that any breach is contained and steps are taken to remedy the circumstances that led to it.

A recent case involving the Ottawa Hospital points up the need for such procedures. The case is also instructive in highlighting the need for standards in electronic record keeping systems.

The case, which was the subject of only the second order issued by the Ontario Privacy Commissioner under PHIPA, involved illegal and unauthorized access to a patient's record by a nurse working in the hospital. The motivation for the breach was a rancorous custody dispute involving the patient's children and her estranged husband, who also worked at the hospital. The nurse was the girlfriend of the husband. The individual had been admitted to the hospital for treatment of a chronic heart condition. She did not want her husband to know about the condition for fear that he might use it against her in the custody proceedings. When she was admitted, the individual specifically requested that measures be taken to ensure that her husband, against whom she had a restraining order,

not learn of her admission and that her privacy be protected. The hospital responded by changing the husband's work location and noting the woman's request on her chart.

However, steps were not taken to prevent access to her electronic record or to notify the hospital's Privacy Office, both of which were required in such a situation under the hospital's established procedures.

Notwithstanding her specific request for privacy, the woman's electronic record was accessed – on numerous occasions – by the nurse. What is more distressing is that even after the woman complained to the hospital about the illegal access – which she learned about when her husband confronted her with information about her condition, subsequent to her discharge – no failsafe measures were taken by the hospital for several weeks during which period the record was accessed again by the nurse on multiple occasions. What *was* done at that time was an audit of the record by the Privacy Officer – which confirmed the unauthorized access – and placement of a “VIP Flag” on the record. This VIP Flag is a warning that appears on the computer screen when the record is accessed. The warning notifies the user that the file contains highly sensitive information and that any access will be monitored closely. The user is then asked to confirm that they wish to proceed. This procedure was followed, but it did not stop the nurse from again accessing the file. Furthermore, no monitoring of her access actually took place, [until several weeks after the individual's complaint to the hospital].

Two significant lessons can be drawn from this case.

Firstly, there was a failure to follow the hospital's established procedures. These procedures required, among other steps, that where a patient specifically has requested privacy, the hospital's Chief Privacy Officer was to be notified. Once this notification has been made, a VIP flag is to be placed on the record and the Chief Privacy Officer is to request a report of all access to the patient's record on a daily basis. If the Chief Privacy Officer determines that unauthorized access has occurred, then the hospital's Privacy Breach Process is to be followed.

Here, none of these steps were taken. Clearly, there was an inadequate response by the hospital to protect the individual's privacy and the Information and Privacy Commissioner so found, concluding that the hospital had failed to meet the standard required of it under PHIPA. The lesson that we can learn from this aspect of the case is that, for one reason or other, the privacy of the patient did not receive the high degree of priority that it should have been given. In commenting on this aspect of the case, the Commissioner emphasized that institutions must ensure that privacy is an *accepted part of their culture* in their day-to-day operations. Otherwise, even the most rigorous privacy policy will be ineffective.

The second and in my view more fundamental lesson that may be drawn from the case is that a re-evaluation needs to be made of access systems and procedures for electronic health records. I understand that the procedures in place at the Ottawa Hospital reflect those standards currently in place in the health sector in Ontario and probably Canada. Essentially, these procedures involved placing a notice on the electronic record – which may be by-passed by anyone determined to access it - and performing a daily audit of all instances of access to the file.

As the Commissioner noted in her report on the case, these procedures do not incorporate sophisticated technical features for restricting access. She made mention however of the reality of most clinical information systems which in fact contemplate a progression of more restricted access to records, based on either the role of the health practitioner or the particular condition or sensitivities of the patient. So for example, an attending nurse might have general access to the daily record but would not have access to psychiatric assessments which would be restricted. Technologies enabling such progressive access restrictions and security controls are available and are being planned for use, I understand, in some settings, including within the community care system.

It seems to me self-evident that with the advance of technology into the health sector, security for electronic records and electronic networks should reflect the best available procedures and systems.

The breach at the Ottawa Hospital, while distressing and unnecessary, did not involve a sophisticated intrusion by a fraudster or other criminal element bent on using information for identity theft or fraudulent payment purposes. However, these types of breaches pose a real risk within the health sector.

In the Ottawa Hospital case, the Commissioner concluded that the VIP flag system, properly employed, reflected current accepted standards within the health sector. In my view, those standards must be raised. I believe that all stakeholders – including government, health care practitioners, institutions and technology suppliers – have a role to play in advancing these standards. The standards should reflect both the increased potentials of exposure to wrongful access presented by the centralization of information in a single electronic record, as well as security issues inherent in and the expansion of network systems within the health sector, including mobile technologies.

Delineating community standards for legal purposes is always a challenge. For this reason and, more importantly, in order to provide clear guidance to the sector, the government should adopt the standards that I am recommending by utilizing the regulatory power clearly contemplated under PHIPA. To be clear, these standards should reflect not only best practice procedures for use of electronic systems, but also the nature of the technology devices required to be used.

Summary and Conclusions

To summarize, I have sought to highlight certain key implications for professionals, both ethical and procedural, in ensuring that a privacy culture becomes ingrained in their practices. Consent and access are key elements in establishing this culture. However, I expect that it will be under the security principle that the rubber will hit the road. It will be the responsibility of all stakeholders within the sector, including the professions and the institutions where they work, to embrace and make effective procedures and systems that ensure that the privacy of their clients is recognized as paramount. The government also has an important role in achieving this objective and, as I have recommended, its regulation-making power under PHIPA is the tool that it should use.

In conclusion, therefore I want to underscore the important ethical and procedural implications of privacy for health professionals. Practical and effective approaches to the three principles that I have identified are key to ensuring that a privacy culture becomes ingrained in the practice of health care.

I have emphasized particularly the security issue. As the Ottawa Hospital case makes abundantly clear, wrongful access to health records is too easy – particularly when the record is electronic. In addressing the issues posed by technology, all stakeholders within this sector have an obligation to work towards a higher standard. Government particularly should play a leadership role.

David M.W. Young is partner and co-chair in the Privacy Law Group in Toronto. Contact him directly at 416-307-4118 or dyoung@langmichener.ca.

Presented to the Ethics at Ryerson Speaker Series, “Privacy and Access Issues Across the Professions” Toronto, March 1, 2007.

Privacy Law Group

© 2007 Lang Michener LLP. May be reproduced with acknowledgement.

Toronto
BCE Place
181 Bay Street, Suite 2500
P.O. Box 747
Toronto, ON M5J 2T7
Tel.: 416-360-8600
Fax.: 416-365-1719

Vancouver
1500 Royal Centre
1055 West Georgia Street
P.O. Box 11117
Vancouver, BC V6E 4N7
Tel.: 604-689-9111
Fax.: 604-685-7084

Ottawa
Suite 300
50 O'Connor Street
Ottawa, ON K1P 6L2
Tel.: 613-232-7171
Fax.: 613-231-3191

Lang Michener LLP
Lawyers – Patent & Trade Mark Agents