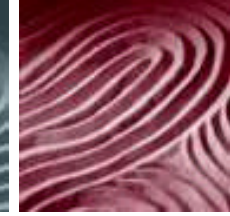
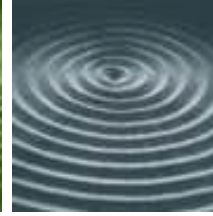


2500, 20 Queen St. West
Toronto, ON M5H 3S1
Canada
Tel. 416.595.8500
Fax.416.595.8695
www.millerthomson.com



MILLER THOMSON LLP

Barristers & Solicitors, Patent & Trade-Mark Agents

TORONTO VANCOUVER CALGARY EDMONTON WATERLOO-WELLINGTON MARKHAM WHITEHORSE WASHINGTON, D.C.

We are a medical
partnership. What do
we have to do for
patients' privacy?

Kathryn M. Frelick
April 19, 2004

We are a Medical Partnership. What do we have to do for Patients' Privacy?

Kathryn Frelick*

Introduction

Health professionals and organizations have long dealt with the concept of confidentiality in relation to health information and generally have a clear understanding of requirements in this regard. The evolving concept of privacy of personal information is a relatively recent development and the implications for patient and other types of personal information are far less understood.

Traditionally, there has been no right to privacy in Canada. With increased globalization, use of computers and the internet there has been heightened concern regarding the information collected about individuals and its use. In the health sector, there has been a proliferation of Information and Communications Technologies (ICTs), including the advent of e-Health and electronic health records. Fair information practices demand that opportunities for improving access, efficiency and the quality of health care be balanced against the right of the individual to decide what should happen with his or her personal information.

Confidentiality rights arise out of the special relationship between the patient and the health professional or provider. In contrast, privacy rights are general rights of all persons to limit access to themselves, or "informational self-determination." Confidentiality and privacy rights may exist in the same information. Health professionals must comply with the rules arising out of both confidentiality and privacy obligations.

Background – Privacy Legislation

Personal Information Protection and Electronic Documents Act (PIPEDA)

Federal privacy legislation, the *Personal Information Protection and Electronic Documents Act* (PIPEDA) was promulgated and came into force on January 1, 2001. The Act creates a right to privacy concerning 'personal information'. It is premised upon the principle that personal information should not be collected, used or disclosed without the prior knowledge and consent of the individual concerned.

PIPEDA had staged application, and in its first stage applied to federal works, undertakings and businesses (generally organizations subject to federal labour law) and to commercial activities of other organizations that do not collect, use or disclose personal information solely within a province. Commercial activities are defined as, "any particular transaction, act or conduct, or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fund-raising lists".

* Kathryn Frelick is a lawyer practicing in Miller Thomson LLP's Health Industry Practice Group. Her practice focuses on regulatory, administrative, health policy issues and privacy.

On January 1, 2002, the Act also applied to personal health information for the organizations and activities covered in the first stage. Personal health information is defined as information about an individual's mental or physical health, including information concerning health services provided and information about tests and examinations.

As of January 1, 2004, PIPEDA applied to any and all provincial entities that collect, use or disclose personal information in the course of commercial activities, unless the province enacted substantially similar privacy legislation. Such legislation has not been enacted in Ontario.

Ontario Privacy Initiatives

In order to address concerns about the appropriate collection, use, and disclosure of personal information, a number of different pieces of legislation have been considered in Ontario. With respect to personal health information, draft legislation was circulated by the Ministry of Health and Long Term Care (MOHLTC) in 1997. Following a further consultation draft in 2000, Bill 159, the proposed *Personal Health Information Privacy Act, 2000* was introduced into the Legislature. It passed first reading in December of 2000, but after vigorous opposition, died on the order paper.

Privacy responsibilities then shifted from the MOHLTC to the Ministry of Consumer and Business Services (MCBS). The MCBS released a consultation draft on a broad-based private sector privacy bill entitled the *Privacy of Personal Information Act, 2002*. Despite extensive consultations on the draft legislation, it was never introduced into the Legislature.

Bill 31, the *Health Information Protection Act, 2003* was introduced by the MOHLTC on December 17, 2003. Following public hearings, the amended bill passed second reading on April 8, 2004, and has been referred back to the Standing Committee on General Government. It is now proposed that the bill come into force on January 1, 2005, along with any associated regulations.

Obligations on Health Professionals

Confidentiality

As stated above, through the course of their duties, health professionals are entrusted with sensitive patient information, collected for a specific purpose (i.e. to provide care and treatment). There is a corresponding duty to protect the confidentiality of that information. Regulated health professionals are required to maintain confidentiality in accordance with professional, ethical and legal standards.

Confidentiality obligations as set out in common law, legislation and professional standards primarily focus on issues of disclosure and access to information. They are based on consent of the patient or the incapable patient's authorized representative, subject to a number of exceptions (i.e. sharing information with colleagues to ensure proper care or where such disclosures are required by law).

For example, with respect to physician obligations, the Supreme Court of Canada¹ has made it clear that the physician-patient relationship is fiduciary in nature. This fiduciary relationship requires the physician to act with utmost good faith and loyalty and to hold information received from or about a patient in confidence. It also gives rise to the physician's duty to make proper disclosure of information to the patient. As a general rule, the patient should have a right of access to the information and the physician should have a corresponding obligation to provide it.

Depending upon the practice setting of the health professional, legislative requirements with respect to confidentiality are currently found in a patchwork of facility-specific legislation. For example, the *Public Hospitals Act*, *Mental Health Act*, *Nursing Homes Act* and *Long Term Care Act* all have different rules in terms of confidentiality, access and disclosure, correction of information, retention and destruction of health information.

As with other regulated health professionals, physicians must comply with legislative requirements under the *Regulated Health Professions Act, 1991* and associated profession-specific legislation. Specifically, the professional misconduct regulation under the *Medicine Act, 1991*² sets out actions relating to confidentiality and record-keeping that are considered to be professional misconduct. It is professional misconduct for a physician to disclose patient information except with the patient or authorized representative's consent or as required by law.

Regulated health professionals, including physicians, are also subject to applicable professional standards, policies³ and codes of conduct. Breach of confidentiality by such health professionals may result in professional misconduct proceedings, civil action or, where applicable, employment sanctions or alteration of privileges.

Of particular note, the Canadian Medical Association adopted the *CMA Health Information Code* ("the Code") in 1998.⁴ This very detailed Code is based on the Canadian Standards Association's Model Code for the Protection of Personal Information and "articulates principles for protecting the privacy of patients, the confidentiality and security of their health information and the trust and integrity of the therapeutic relationship"⁵. In many respects, this document was ahead of its time and it was recognized by the drafters that the Code and its provisions would be more exacting than existing legislation and standards protecting health information in the Canadian health care system.

Application of PIPEDA to Private Medical Practices

PIPEDA was drafted with the goal of supporting and promoting electronic commerce. Since its inception, there has been grave concern about its applicability to the health sector and the potential implications for the provision of care. Specifically, PIPEDA has been widely viewed as a blunt instrument whose applicability to the health sector is both inappropriate and

¹ *McInerney v. MacDonald*, [1992] 2 S.C.R. 138

² Ontario Regulation 856/93 under the *Medicine Act, 1991*, s. 1(1)(10)

³ See for example, the College of Physicians and Surgeons of Ontario Policy #9-00 *Confidentiality and Access to Patient Information* and Policy #10-00 *Mandatory Reporting*

⁴ Canadian Medical Association, *CMA Health Information Privacy Code* (1998)

⁵ Section A: Scope

unworkable. It is perceived that it does not achieve the balance between protecting patient privacy and ensuring that patients receive timely, safe and effective treatment. In order to achieve this balance, these organizations sought an exemption or carve out for organizations that collect, use or disclose personal health information for health care purposes.⁶

Strong lobbying efforts by a number of physician organizations, including the Canadian Medical Association, Ontario Medical Association, College of Physicians and Surgeons of Ontario and Canadian Medical Protective Association continued up until the legislation came into force on January 1, 2004. In particular, these groups argued that ethical obligations, existing legislation, policies and the Code sufficiently protected patient privacy. In the end, such an exemption was not granted.

Although not always clear cut, the application of PIPEDA to physician practice will depend upon the practice setting. For example, given the broad definition of commercial activity and statements made by the Federal Privacy Commissioner, there appears to be consensus that a physician or other health professional in private practice is engaged in commercial activities, regardless of the funding source.⁷ This has been confirmed by Industry Canada, which has published a number of Questions and Answers on the application of PIPEDA to the health sector. These specifically cite the example of health care providers in private practice as being subject to the act.⁸ Although not binding authority, these questions are instructive in regards to the approach that the federal Privacy Commissioner may take.

The Questions and Answers also define a number of terms. For example, a commercial activity in the context of the health care sector “involves the making and provision of a product or providing a service that is commercial in nature.”⁹ In determining whether an activity is commercial, it appears that will be based on the nature of the activity (transaction), rather than the nature of the organization. For example, there appears to be consensus that PIPEDA does not apply to the core activities of a public hospital, which are not commercial in nature. In looking at an organization’s core activities, reference may be had to that organization’s stated objects and purposes, as set out in its constituting documents. If the activity appears to be intimately connected to a core activity, it similarly would not be covered by PIPEDA. As such, the activities of a physician providing care in a hospital setting would not be covered by federal privacy legislation since this is part of the hospital’s core activities (i.e. provision of care). In contrast, where a hospital undertakes revenue-generating activities, these activities are subject to PIPEDA.

⁶ See for example, letter to the Honourable Allan Rock and the Honourable Anne McLellan dated May 23, 2003 from Hilary Short and L.S. Erlick, available online at <<<http://www.oma.org>>> and R. Gerace, “Concerns about Privacy Legislation”, *Members’ Dialogue*, September/October 2003

⁷ Letter from R. Marleau (Interim Privacy Commissioner of Canada) to J. Laplume (CEO Manitoba Medical Association) dated November 21, 2003, available on-line at <<<http://cma.ca>>> ; D. Fraser, “The Application of PIPEDA to Personal Health Information” *Canadian Privacy Law Review*, 1(6), March 2004 at p. 62

⁸ Industry Canada, “PIPEDA Awareness Raising Tools (PARTs) Initiative for the Health Sector Questions and Answers” q. 9, available on-line at <<http://e-com.ic.gc.ca/English/privacy/health/pipeda_qas_first.html>>

⁹ *Ibid.* q. 7

Application of Bill 31 to Private Medical Practices

As stated above, the proposed Bill 31, the *Health Information Protection Act, 2003* is currently moving through the Ontario legislative process. Given the current state of privacy in the province and the special concerns around personal health information, there is strong impetus for this bill to become law. It is comprised of two Schedules: the *Personal Health Information Protection Act, 2003* (PHIPA) and the *Quality of Care Information Protection Act, 2003*.

Like PIPEDA, PHIPA is based on the 10 principles set out in the CSA Model Code for the Protection of Personal Information. It is a very complex piece of legislation and as indicated, will be subject to amendment. Nevertheless, following is a brief summary of some of the key elements of the draft legislation, with particular focus on some of the issues that are of primary concern to physicians in private practice.

If passed, PHIPA will apply to the collection of personal health information by Health Information Custodians (“HICs”) after the Act comes into force, and to the use and disclosure of Personal Health Information (“PHI”), regardless of when it was collected. It will also apply to non-HICs or “recipients” when they receive PHI from a HIC.

HICs are listed individuals or organizations that have custody or control of PHI as a result of or in connection with their work, powers or duties. It includes health care practitioner or a person who operates a group practice of health care practitioners.

PHI is defined as identifying information about an individual, whether living or deceased and whether in oral or recorded form, that relates to matters such as an individual’s physical or mental health, the provision of health care to the individual (including the identification of a person as provider of health care), the donation of tissue or bodily substance, or the individual’s health number.

Information Practices

PHIPA defines “Information Practices” as “the policy of the custodian for actions in relation to personal health information including:

- a) when, how and the purposes for which the custodian routinely collects, uses, modifies, discloses, retains or disposes of personal health information; and
- b) the administrative, technical and physical safeguards and practices that the custodian maintains with respect to the information”;

A HIC must have in place information practices with respect to the collection, use and disclosure of PHI and the administrative, technical and physical safeguards that it maintains with respect to that information. A HIC must make a statement available to the public that describes its information practices, how to contact its contact person, how an individual can obtain access to or request correction of a record of personal health information and how to make a complaint to the custodian. An individual may also make complaint to the Information and Privacy Commissioner.

Consent

Part III of PHIPA sets out rules concerning consent and capacity relating to the collection, use or disclosure of PHI. Consent must be knowledgeable, relate to the information and not be obtained through deception or coercion. Consent is knowledgeable if it is reasonable to believe in the circumstances that the individual knows the purposes of the collection, use or disclosure, as the case may be, and that the individual may provide or withhold the consent.

Consent may be express or implied, however the consent to the disclosure of PHI to a person who is not a HIC must be express. Similarly, consent must be express where information is disclosed by a HIC to another HIC, if this is done for a purpose other than providing health care or assisting in providing health care.

Consent has always been one of the most contentious issues facing the health industry in terms of informational privacy. Principle 3 under the CSA Model Code requires both the *knowledge* and *consent* of the individual for the collection, use and disclosure of personal information. It further provides that the form of consent sought by an organization will depend upon the type of information. "An organization should generally seek express consent when the information is likely to be considered *sensitive*". PHI is almost always considered to be sensitive in nature, which has suggested the need to obtain express consent. At face value, such a requirement would surely be an insurmountable barrier to the provision of care.

Importantly, PHIPA recognizes that a HIC that receives PHI from an individual, substitute decision maker or another HIC for the purpose of providing health care to the individual, is entitled to assume implied consent for the collection, use and disclosure of information for these purposes, unless such consent is expressly withheld. Imbedded in this provision is a construct that has developed of a "circle of care" and the recognition of implied consent within this construct.

Relative to PIPEDA, Industry Canada has also embraced the principle of implied consent within the construct of "circle of care." It clarifies that "the expression includes the individuals and activities related to the care and treatment of a patient. Thus, it covers the health care providers who deliver care and services for the primary therapeutic benefit of the patient and it covers related activities such as laboratory work and professional or case consultations with other health care providers." Again, while this is comforting to those in the health industry wishing to rely on an implied consent model, the ultimate interpreter of PIPEDA will be the Federal Court of Canada. Further, there is nothing in PIPEDA itself, or the Code that would lend tangible support to this approach.

It must be reiterated that implied consent is based upon the purposes for which the information is collected and is premised upon the knowledge of the individual and what a "reasonable person" would consider appropriate, logical and fair in the circumstances. Relying upon an implied consent model, absent an appropriate analysis of the specific purposes and uses of PHI is fraught with risk.

Interaction between PIPEDA and Provincial Privacy Legislation

At the present time, health professionals in private practice are required to comply with PIPEDA with respect to personal information collected, used and disclosed in the course of commercial activities, along with applicable provincial legislation dealing with confidentiality. If, as expected, Bill 31 becomes law, health professionals operating as HICs will be required to comply with this legislation in regard to PHI that is collected, used and disclosed in the course of providing health care services. This leaves such health professionals dealing with co-existing federal and provincial regimes, with the potential for contradictory rules.

To the extent that the health professional or organization is able to comply with both federal and provincial privacy regimes, standards and codes of practice, there is no conflict. For example, PIPEDA allows for an individual to correct a record of personal information, including modifying such records. PHIPA sets out rights of correction where the individual believes the record is inaccurate or incomplete, but recognizes current best practices and professional standards that allow for modifications, but do not allow original records to be modified. In this situation, a health professional or organization would be able to comply with both requirements by adding a notation, addendum or statement of disagreement to the record, but without altering the original record.

There are other areas where this is not the case, for example, under PHIPA and in accordance with the common law, an individual is entitled to access a record of PHI that is kept by the HIC except where granting such access could reasonably be expected to result in a risk of serious harm to the treatment or recovery of the individual or where access is prohibited by law. PIPEDA does not allow denial of access for this purpose. If access is denied on this basis, the requester can complain to the federal privacy commissioner.

In addition to the above, there are also areas to which privacy legislation does not apply, but where it may still be advisable for the health professional or health organization to meet minimum standards of privacy protection. For example, employee information is specifically excluded from PIPEDA and PHIPA, however, as employers it may be appropriate to adopt fair information practices relative to this type of information.

Finally, if PHIPA becomes law, it is still possible for the federal government to remove health information from the purview of PIPEDA or that the provincial statute will be found to be substantially similar. Having said this, a number of western provinces, namely Saskatchewan, Manitoba and Alberta, have enacted privacy legislation that deals with health information. None of these statutes have been declared to be "substantially similar" to PIPEDA, nor has an exemption been granted for health information. Very recently, based on the recommendation by the Minister of Industry that the Alberta *Personal Information Protection Act* and British Columbia *Personal Information Protection Act* are substantially similar to PIPEDA, exemption Orders have been sought from its application.¹⁰ These statutes are quite different in scope from their health counterparts.

¹⁰ Department of Industry, Alberta and British Columbia exemption orders. Notice available online at << <http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/gv00236e.html>>>. Regulatory impact analysis statements and

It should be noted that there are a number of tools available for physicians to deal with privacy compliance issues.¹¹ There are promises of additional resources to come as privacy continues to evolve, especially if PHIPA is enacted in Ontario.

It is clear that at least for some period of time, health professionals will have to contend with dual regulation. Underlying both the federal regime and the proposed provincial regime are the 10 CSA privacy principles. Current provincial confidentiality provisions are also consent-based and rely upon a number of the same principles. Regardless of the regime, there are commonalities and steps that health professionals can take towards achieving privacy compliance. By incorporating and formalizing these principles into their practices, health professionals can go a long way towards managing their risk and can reassure their patients that their privacy concerns are of foremost importance.

It is recognized that the effort and resources to develop a privacy compliance regime will vary substantially depending upon the size and type of the practice. The steps outlined below will need to be modified and may be somewhat informal for smaller practice groups.

Steps to Privacy Compliance

Step 1 Understanding privacy

This step involves an educational aspect, that is, raising awareness and understanding of privacy legislation and principles, along with reflecting upon how personal information is collected, used and disclosed in your practice.

Step 2 Appointment of Contact Individual

Both PIPEDA and the proposed PHIPA require that an individual be designated to be responsible for an organization's privacy compliance. Depending upon the size of the practice group, it may be logical to designate a "contact person", "privacy officer" or "information officer", who may be a physician or senior employee of the organization. For single practice settings, the physician will be solely responsible for his or her information practices.

The contact person will be accountable to the organization and authorized to facilitate compliance with privacy legislation. This should include the development of fair information policies, procedures and practices and ensuring that individuals within the organization are sufficiently informed of their obligations under privacy legislation. The contact person typically responds to enquiries and complaints from the public about its information practices, and responds to requests for access or correction of personal information records.

proposed regulatory texts published in the April 10, 2004 *Canada Gazette*, Part I at <<<http://canadagazette.gc.ca/partI/2004/20040410/pdf/g1-13815.pdf>>>

¹¹ See for example, Canadian Medical Association, "Privacy in Practice: A Handbook for Canadian Physicians" (2003), and the College of Family Physicians of Canada, "Privacy Legislation A Critical Review for Family Physicians", December 2003 and Ontario Medical Association, Privacy Statement, available at www.oma.org.

Step 3 Assess your privacy readiness

This step requires a comprehensive review of your data collection, use and disclosure practices and retention guidelines. Diagnostic tools or questionnaires may be employed in order to create an inventory of the information collected, how it is used and disclosed and the protections that are in place.

This also involves a review of your information policies and practices (i.e. confidentiality, security, privacy, retention/destruction of records, facsimile, email, internet, patient records). Contracts, consent forms and notices should be reviewed to ensure that privacy concerns are adequately addressed.

Step 4 Prioritize/ develop action plan

Once an inventory has been completed, you can develop a task list and action plan. This may involve policy and practice development and review, development of contractual agreement language, forms, notices and consent forms, complaint process, data sharing agreements, and a review of security safeguards. Several of these issues will be touched upon in more detail below.

Privacy Statement or Policy

Both PIPEDA and PHIPA require that certain information be made available to the public with respect to the organization's information practices. As such, health professionals and organizations should assess how to communicate its privacy practices, both internally and externally. For example, a user friendly description of your privacy practices may be provided to patients and other members of the public via a website, a brochure or through an information handout.

The statement or policy should include information about the purposes for which the health professional or organization collects, uses and discloses personal information, as well as information about how that information is safeguarded. The statement should also include information about the organization's contact person, how to obtain access to personal information or request the correction of a record, and how to make a complaint to the organization.

Notices

Under privacy legislation, consent must be "knowledgeable", that is, it must be reasonable in the circumstances that the individual knows the purposes of the collection, use or disclosure of his or her personal information, and knows that he or she may withhold or withdraw consent. One way of ensuring that the individual is knowledgeable about how his or her information is through the use of posted notices. Typically, such notices are posted in conspicuous areas, where this information is most likely to come to patients' attention, such as waiting rooms or physician offices.

To ensure that patients are knowledgeable about the health professional's information practices, notices may be effectively combined with a consent form, intake form or information handout.

Safeguards

One of the largest sources of complaint involves the protection of personal information, especially when security measures are inadequate or fail. Given the sensitivity of personal health information, health professionals must be especially cognizant of how that information is protected, and the administrative, technical and physical safeguards that must be in place. While a full discussion of necessary safeguards is beyond the scope of this paper, ensuring that there are appropriate systems in place to support record-keeping is essential.

Conclusion

Even after the implementation of fair information practices, there is an ongoing need to monitor the organization's compliance. Privacy obligations will continue to evolve as the law in this area develops and we see how privacy principles are applied in practice. Obligations in regard to health information are enormously complex, however, health professionals and organizations will be best served in adhering to the first principles of privacy.

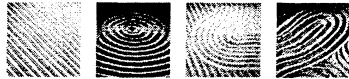
MILLER THOMSON LLP

Barristers & Solicitors, Patent & Trade-Mark Agents

**We are a Medical Partnership. What do we
have to do for Patients' Privacy?**

OBA Privacy for the Business Lawyer

April 19, 2004



Kathryn Frelick



Concepts

- What are the current obligations of physicians for protecting patient information?
- Confidentiality
- Privacy

- Confidentiality and privacy rights may exist in the same information

MILLER THOMSON LLP

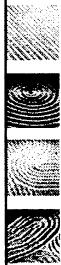
Barristers & Solicitors, Patent & Trade-Mark Agents



Confidentiality

- Confidentiality is a legal, professional and ethical obligation of every physician
- Common law - i.e. *McInerney v. MacDonald*
- Legislation - profession, facility-specific
- Professional standards, policies and codes
 - CPSO policies
 - Canadian Medical Association Health Information Privacy Code
 - CMA Code of Ethics

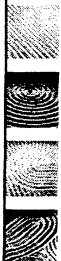
MILLER THOMSON LLP
Barristers & Solicitors, Patents & Trade-Mark Agents



Application of PIPEDA to private medical practices

- January 1, 2004 - PIPEDA applies to provincial entities that collect, use or disclose personal information in the course of commercial activities
- Strong lobbying efforts by physician groups and others for an exemption or carve out for health sector
- Viewed as inappropriate for application to personal health information

MILLER THOMSON LLP
Barristers & Solicitors, Patents & Trade-Mark Agents



Application of PIPEDA (cont'd)

- Commercial activity - “any particular transaction, act or conduct or any regular course of conduct that is of a commercial character ...”
- Health context - “involves the making and provision of a product or provision of a service that is commercial in nature”
- Consensus – physicians in private practice are engaged in commercial activity and are subject to PIPEDA
- Application depends upon practice setting and nature of activity

MILLER THOMSON LLP
Barristers & Solicitors, Patent & Trade-Mark Agents



Consent obligations

- Requires knowledge and consent
- Principle 3 – express consent generally required for “sensitive” information
- Construct of “circle of care” has developed supporting use of implied consent for activities related to the direct care and treatment of the patient and related activities such as laboratory work and consultations

MILLER THOMSON LLP
Barristers & Solicitors, Patent & Trade-Mark Agents



Bill 31 – Personal Health Information Protection Act, 2003 (PHIPA)

- If passed, PHIPA will apply to the collection, use and disclosure of Personal Health Information (PHI) by Health Information Custodians (HICs)
- HICs are individuals or organizations that have custody or control of PHI in connection with their work, powers or duties
- HICs include an individual physician or a person who operates a group medical practice

MILLER THOMSON LLP
Barristers & Solicitors, Patent & Trade-Mark Agents



PHI under PHIPA

- Broad definition of PHI
- Identifying information about an individual, living or deceased, regardless of form
- Relating to individual's physical or mental health, the provision of care, care provider, donation of tissue or bodily substance, health number, etc.

MILLER THOMSON LLP
Barristers & Solicitors, Patent & Trade-Mark Agents



PHIPA - Information Practices

- Must have in place “information practices” (i.e. policy of the HIC for actions in relation to PHI) for:
 - When, how, and the purposes for which the HIC collects, uses, modifies, discloses, retains or disposes of PHI
 - the HIC’s administrative, technical and physical safeguards and practices with respect to PHI

MILLER THOMSON LLP
Barristers & Solicitors, Patent & Trade-Mark Agents



PHIPA - Consent

- Knowledge and consent
- Reasonable person test - reasonable to believe that the individual knows the purposes of the collection, use or disclosure
- Sets out requirements for express or implied consent
- More explicit recognition of “circle of care” within PHIPA i.e. where consent may be implied for purposes of providing care

MILLER THOMSON LLP
Barristers & Solicitors, Patent & Trade-Mark Agents



Interaction - PIPEDA, PHIPA, other provincial legislation

- January 1, 2004 - PIPEDA applies to health professionals in private practice in regard to PI
- January 1, 2005 - if it becomes law, will also be subject to PHIPA in regard to PHI
- Subject to exemption, to the extent that federal and provincial privacy regimes co-exist, must comply with both schemes
- May also be required to comply with other provincial legislation (i.e. mandatory reporting), professional guidelines, etc.

MILLER THOMSON LLP
Barristers & Solicitors, Patent & Trade-Mark Agents



Application of Privacy Legislation

- Even where privacy legislation does not strictly apply, the privacy principles constitute a national standard against which organizations will be measured ... reflect best practices i.e. employee information

MILLER THOMSON LLP
Barristers & Solicitors, Patent & Trade-Mark Agents



What steps should the medical partnership take to protect patients' privacy?

- Step 1 – Understanding Privacy
 - Educational component and raising awareness within the organization
 - Understanding obligations and reflecting on how PI and PHI are collected, used and disclosed in the medical practice


MILLER THOMSON LLP
Barristers & Solicitors, Patent & Trade-Mark Agents



What steps should the medical partnership take to protect patients' privacy?

- Step 2 – Appoint a Contact Individual
 - Person responsible for organization's privacy compliance
 - Person should use all available resources in the development of fair information practices, education and training within the organization
 - Respond to enquiries and complaints
 - Respond to requests for access or correction of PI records

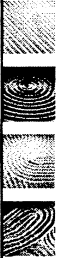
MILLER THOMSON LLP
Barristers & Solicitors, Patent & Trade-Mark Agents



What steps should the medical partnership take to protect patients' privacy?

- Step 3 – Assess Privacy Readiness
 - Comprehensive review of data collection, use, disclosure, retention and safeguards
 - Create inventory what and how information is collected, used and disclosed and protections that are in place
 - Review of contracts, consent forms, notices, policies and procedures


MILLER THOMSON LLP
Barristers & Solicitors, Patent & Trade-Mark Agents



What steps should the medical partnership take to protect patients' privacy?

- Step 4 – Prioritize / Action Plan
 - Creation of privacy statement or policy
 - Available to public upon request – website, brochure, information handout
 - Set out purposes
 - Safeguards
 - Information practices
 - Contact information for access, correction, complaints

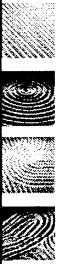
MILLER THOMSON LLP
Barristers & Solicitors, Patent & Trade-Mark Agents



What steps should the medical partnership take to protect patients' privacy?

- Step 4 – Prioritize / Action Plan
 - Notices
 - Consent must be knowledgeable
 - Posted in high traffic areas
 - May be combined with consent forms, intake form, information handouts
 - Safeguards
 - Adequate administrative, technical and physical safeguards to protect sensitive information

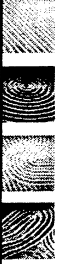
MILLER THOMSON LLP
Barristers & Solicitors, Patent & Trade-Mark Agents



What steps should the medical partnership take to protect patients' privacy?

- Step 4 – Prioritize / Action Plan
 - Confidentiality Pledges
 - Contracts, data sharing
 - Policy and procedure development (complaints, access, correction, retention and destruction, security, email, internet, etc.)

MILLER THOMSON LLP
Barristers & Solicitors, Patent & Trade-Mark Agents



What steps should the medical partnership take to protect patients' privacy?

- Step 5 – Implementation and Monitoring
 - Implement fair information practices and ongoing monitoring of efforts
 - Audit procedures
 - Monitor ongoing privacy developments

MILLER THOMSON LLP

Barristers & Solicitors, Patent & Trade-Mark Agents