



- MICHAEL WHITT -

HEALTH INFORMATION 101 - Confidentiality & Privacy

Michael Whitt is a Partner in the Calgary office of Borden Ladner Gervais LLP. He is a lawyer, patent agent, and trade-mark agent, and provides legal advice to technology-based businesses.

Editor's Note:

This article (and the sequel planned for the next issue of this publication) is designed to be informative and accessible to informatics professionals, medical professionals, and non-specialist managers. This article was written by Michael Whitt, with the assistance of a number of lawyers from Borden Ladner Gervais' various offices experienced in healthcare informatics, outsourcing, and privacy law, as well as information technology ("IT") in commercial legal settings generally. We hope you enjoy reading it, and welcome your feedback either directly or to the firm; contact information is indicated at the end of the article.

1.1 Health Information

(a) What is Health Information ("H.I.")?

In this review, Health Information is information about the medical condition or status of a human individual (a "data subject"), or a population of human individuals, at any point in time as well as longitudinally over a period of time. Generally, IT professionals speak of an "electronic health record" or "EHR" and an "electronic medical record" or "EMR", and draw a distinction between the medical records collected and kept in a hospital or institutional setting from medical records collected and kept in a physician's practice. For most purposes, both types of records are included in our discussion of H.I.

A brief history of H.I. regulation in various jurisdictions

H.I. has likely been considered confidential since physicians first began thoughtfully recording their observations and conclusions about their patients' health. In Canada, perhaps the clearest statement about the nature of H.I. comes from our Supreme Court in the "McInerney" case (discussed below), which stands for the proposition that the information in a patient's physician's file is held by the physician for the benefit of the patient, and thus (among other things) access and control by the patient cannot generally be denied. The H.I. was compiled for the benefit of managing the patient's medical needs, and the physician thus owed a very high duty of disclosure and fair recording to the patient directly. A corollary of that concept is that the patient's H.I. must be held in the strictest of confidence by the physician, and used only for the purpose of managing the patient's healthcare. Of course, the patient (if competent) can waive that requirement for confidential treatment and often does so when, for instance, purchasing insurance coverage or making claims for insurance benefits or engaging in treatment programs involving more than one care-giver or facility.

In more recent times, governments, payors and healthcare service providers have begun to understand the benefits which may come from more fully integrated IT systems accessing and managing H.I. of larger numbers of patients. In order to manage concerns by IT providers arising from information-sharing and

new types of risks to patient confidentiality introduced by electronic record-keeping, law-makers have introduced legislation and regulations which attempt to regulate information-sharing behaviors and limit IT providers' risks arising from electronic record-keeping and sharing systems. Examples include the *Health Information Act* (Alberta) (RSA 2000, c.H-5), the use of *Freedom of Information and Protection of Privacy* (FOIPPA) legislation in British Columbia (RSBC 1996 c.165) with respect to public bodies such as hospitals, and the recently enacted (S.O.2004, c.3) Ontario *Personal Health Information Protection Act*, and the Federal *PIPEDA* (RSC 2000, c.5) for H.I. in some commercial (non-government funded) settings. These statutes are relatively new, and neither well integrated nor is there any significant body of judicial interpretation (although that is starting to come). We provide a table showing the most directly relevant statutes below.

While each of those regulatory regimes differs slightly, it is helpful to remember the purpose of their enactment, namely to afford a workable regime for the installation of wide-spread electronic systems to collect, keep, access, and share H.I., and to "rebalance" patients' legitimate confidentiality and privacy expectations and rights against the requirements of the larger healthcare IT systems, and the needs or perceived needs of administrators, care-givers and payors.

(b) What is Personal Information ("P.I.")?

Personal Information in each of the Healthcare IT regulatory regimes includes most information about the identity, health, status, and treatment of an identifiable human individual ("data subject"). Typical exemptions from requirements for overt consent imposed by usual privacy regulations (with respect to collection, disclosure, safekeeping and use of P.I.) include things like freely volunteered information, and information necessarily disclosed for purposes which society values. Information which is collected, used, disclosed and kept in safekeeping with the "knowledgeable consent" of the data subject may be collected, used, disclosed, and kept in line with that consent.

(c) What P.I. is included in Health Information ("H.I.")?

	HEALTH INFORMATION PRIVACY REGULATION (Specific to Health Information Only)
PROVINCE	
BRITISH COLUMBIA	<i>Freedom of Information and Protection of Privacy Act RSBC 1996, c. 165</i> <i>Personal Information and Privacy Act, SBC 2003, c-6</i>
ALBERTA	<i>Health Information Act RSA 2000, c. H-5</i> <i>Personal Information Protection and Electronic Documents Act RSC 2000, c. H-5</i> <i>Personal Information Protection Act SA 2003, c. P-6.5</i> <i>Freedom of Information and Protection of Privacy Act RSA 2000, c. F-25</i>
SASKATCHEWAN	<i>Health Information Protection Act S.S. 1999, c. H-0.021</i> <i>(effective September 1, 2003, except for subsections 17(1)</i> <i>as amended by the Statutes of Saskatchewan</i> <i>The Freedom of Information and Protection of Privacy Act S.S. 1990-91, c. F-22.01 as amended by</i> <i>the Statutes of Saskatchewan, 1992</i>
MANITOBA	<i>The Personal Health Information Act C.C.S.M. c. P33.5</i> <i>(Assented to June 28, 1997)</i> <i>The Freedom of Information and Protection of Privacy Act</i> <i>C.C.S.M. c. F175</i>
ONTARIO	<i>Personal Health Information Protection Act, S.O. 2004, c. 3, Schedule A</i> <i>Quality of Care Information Protection Act, S.O. 2004, c. 3, Schedule B</i> <i>Freedom of Information and Protection of Privacy Act R.S.O. 1990, c. F.31</i>
QUEBEC	<i>An Act Respecting the Protection of Personal Information in the Private Sector, R.S.Q., c. P-39.1</i> <i>An Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal</i> <i>Information R.S.Q., chapter A-2.1</i>
NEWFOUNDLAND & LABRADOR	<i>Access to Information and Protection of Privacy Act [Part IV to be Proclaimed]</i> <i>SNL 2002 Chapter A-1.1</i> <i>Centre for Health Information Act [To be Proclaimed] SNL 2004 Chapter C-5.1</i> <i>An Act to Provide the Public with Access to Information and Protection of Privacy Newfoundland</i> <i>(Assented to March 14, 2002) Amended: 02 cI-0.1 s54; 2004 c47 s2</i>
NEW BRUNSWICK	<i>Protection of Personal Information Act S.N.B. 1998, c. P-19.1 Assented to February 26, 1998</i>
NOVA SCOTIA	<i>Freedom of Information and Protection of Privacy Act S.N.S. 1993, c. 5</i>
NORTHWEST TERRITORIES	<i>Access to Information and Protection of Privacy Act S.N.W.T. 1994, c. 20</i>
NUNAVUT	<i>Access to Information and Protection of Privacy Act (Nunaut) S.N.W.T. 1994,c.20 (In force</i> <i>December 31, 1996); SI-016-96</i>
PRINCE EDWARD ISLAND	<i>Freedom of Information and Protection of Privacy Act R.S.P.E.I. 1988, c. F-15.01</i>
YUKON	<i>Access to Information and Protection of Privacy Act R.S.Y. 2002, c. 1</i> <i>Access to Information Regulations, Y.O.I.C. 1996/053</i>

[B.C. regulates H.I. at the hospital level under its FOIPPA legislation and at the physician level under its PIPA legislation. Alberta's regulation of H.I. is primarily under its HIA legislation, with some activities falling under its PIPA. Ontario's regulations of H.I. is primarily under its PHIPA legislation. Some regimes treat H.I. at the large institutional level more like "government-controlled" databanks, while others deal more specifically with healthcare-specific data handling rules]

H.I., when collected and recorded about a particular data subject, is all P.I. If the H.I. can be aggregated or otherwise stripped of any link to a data subject (or identifiable group), then it would not subsequently be Personal Information. Most H.I. regulatory schemes deal with the use of H.I. for demographic and epidemiological studies as well as for the administration of provider systems (such as hospitals) and the management of providers (such as physicians and pharmacists) and patients (such as system users and abusers). In the case of demographic or epidemiological use of H.I., proposed uses must usually be reviewed by an ethics committee or similar review board, and concerns about privacy and confidentiality of P.I. maintained.

1.2 Regulation of Health Information

(a) Who owns H.I.?

From a lawyer's perspective, we should explain that the "information" component of H.I. is different from the medium within which the information is stored. Generally, in Canada, the "information" is "owned" (to the extent that information can be owned - more exactly, "controlled") by the patient, while the "medium" is owned by whomever keeps the record. In a doctor's office, the traditional paper file (if one still exists) contains information which the patient owns and controls, while the paper file belongs to the doctor.

Things start to become more interesting when the information is collected on a system which involves a variety of different media types spread over a large geographic territory, owned by different people, and controlled and accessed by different constituents in the healthcare system. For instance, a prescription written by a physician may be delivered electronically or by fax to a pharmacy for fulfillment, and reports about the prescription, the prescribing physician, the pharmacist and the patient may be generated and delivered to an insurer, a billing and payment system, an oversight body (such as for "triplicate form" or controlled drugs like opiates), and perhaps a government department or agency (Blue Cross, or Health and Wellness for program management as well as payment or contribution). In another example, a hospital-ordered lab report may involve a specimen collection, analysis and report by a hospital-controlled or private laboratory back to the ordering physician through the hospital's IT system, and forwarded to the patient's family physician, a payor, the system's administrator, and so forth. Some or all of the functions, including (but not necessarily limited to) IT collection, transmission, storage, backup and networking functions may have also been "outsourced" to third-party providers some of which may be located or controlled in another jurisdiction. In some situations, the analysis of ownership of information versus right to control versus right to access versus ownership of medium can be quite challenging, and the answer will routinely be different depending upon the purpose of the analysis.

(i) *McInerney v. MacDonald* [1992] 2 S.C.R. 138

In *McInerney*, the Supreme Court of Canada noted the increasing importance and sensitivity of medical records due to increased physician specialization, increased patient mobility, increased referrals, the "army" of potential care givers contributing to the care of a single patient and patients' needs to ensure the accuracy of their medical records. Due in part to increased dissemination of medical records to insurance companies, government payers, law enforcement, welfare departments, schools, researchers and employers, this case was important in recognizing concern about disclosure and accuracy of these records.

McInerney involved a patient who requested that her physician provide her with copies of her medical file. The physician agreed to provide all notes and reports the physician had prepared, but refused to provide copies of consultants' reports and records from other physicians the patient had seen in the past on the grounds that full disclosure would be unethical since the balance of the patient's medical information was the property of the other physicians.

Prior to reaching the Supreme Court, New Brunswick courts had ordered the physician to provide the patient with copies of the entire file. The Supreme Court of Canada dismissed the physician's appeal from those orders.

At the time, there was an absence of legislative guidance, although the Court's end result was consistent with a relevant Canadian Medical Association Policy. The Court concluded that a fiduciary duty (meaning in part that the physician was in a position of trust and confidence) exists between patients and their own physicians. Physicians owe certain duties to patients including duties to act with the utmost good faith, loyalty, to hold the patient's Health Information in confidence and to make proper disclosure of the information to the patient. There is a broad public interest in ensuring the confidentiality of the information entrusted by the patient to her doctor. Were it otherwise, the patient's healthcare may be compromised by her reluctance to be forthright and complete in discussing her health with her doctor.

Additionally, physicians (and health care providers generally) are in the position of having more specialized knowledge and skill, and thus patients must rely upon the care-giver's good faith in seeking, collecting, and disclosing (and keeping) personal Health Information. As well, care-givers are very much more in control of, and knowledgeable about, the systems (including IT systems) engaged with respect to H.I. in patient interactions.

The Health Information shared by the patient was said to ultimately remain her own. Generally, the duty to provide access to medical records is grounded in the nature of the patient's interest in receiving the information and having a type of proprietary interest in the contents of her own medical file. The Court said that, although a patient has these interests in the contents of her medical files (the "informational component"), the physician owns the actual record or physical file.

However, the Court commented that the right to one's own Health Information is not absolute. A physician may deny access to a medical file in those very situations where the physician reasonably believes that it would not be in the patient's best interest to receive a copy if, for example, there was a risk of potential injury to the patient or a third party. The onus will be on the physician to justify the exception to the rule of disclosure.

Thus, the physician's role as fiduciary or trustee of the patient's informational well-being (as well as healthcare) comes into play, giving rise to these enhanced duties of good faith, loyalty, and care when dealing with a dependant patient's information.

(b) Who gets to see H.I. at the Physician's Office level? At the Hospital level?

Generally, we all assume that a patient will want everyone who needs to see that patient's H.I. to administer care to protect the patient's health to have access to the patient's H.I. There is probably an implied consent of the patient to the sharing

between physicians involved in the patient's care of that patient's H.I. on a "need to know" basis, at least to the extent that the information is relevant to the management of the patient's health concerns, and useful in the context.

In some physician practices, formally documented consents to collection, use, safekeeping, and disclosure of a patient's H.I. will be collected, most likely either at the initial enactment of H.I. legislation or at the beginning of the physician-patient relationship. As well, patients routinely direct or consent to requests that H.I. be shared with others, most notably health, life and disability insurers, specialist and laboratory referrals, driver or pilot licensing authorities, employers, and others.

In the Hospital setting, there are typically a series of posted privacy and information-sharing policy statements, and operating policies and procedures which include standard forms with consents to collection, use and disclosure policies, and extensive training of personnel with respect to information sharing and confidentiality and patient privacy. Legally, the analysis follows the *McInerny* style of conclusion, tempered and tailored by the practical requirements of operating a large and collaborative multi-practitioner environment, the patient's reasonable expectations, special patient requirements, and the region's hospitals' policies and procedures (which may set a sort of standard of care or an environment of reasonable expectations and behaviors).

Health Information privacy legislation adds a layer of basic rules, some realignment of responsibility, and some more or less predictable procedures and forums for managing patient H.I. in a setting of institutional healthcare. Most modern Canadian regimes are designed to facilitate relatively unimpaired sharing of H.I. when done for legitimate reasons within a so-called 'circle of care' with impunity (or immunity from complaint).

(c) What is the "circle of care"?

The 'circle of care' concept is meant to include physicians, nurses, pharmacists, laboratories, hospital management and other direct care-givers, and is often expanded to include government (payor and regulator), police, and other officials working in other similar roles. Theoretically, the regulators' desire is to include all parties who "need to know" a patient's H.I. to provide appropriate care, as well as those who "need to know" in order to manage modern healthcare provider facilities and systems under an "umbrella" of substantially unregulated and free information-sharing (within the "circle of care").

(d) Who regulates H.I. and how are rights and interests of the various stakeholders balanced?

1.3 Impact on IT Systems and Physicians

(a) How do the Health Information Act, and other provincial statutes relate to SSH or POSP?

The topics of patient privacy, data security, record retention, off-shoring and outsourcing are included in the analysis of "approved" IT systems; and data flows analyses and systems (hardware, software and procedural or human-operated systems of policies and processes) documentation are now required to be specifically analysed from a privacy perspective, in order for IT systems to meet what governments are attempting to impose in various Healthcare IT "standards setting" activities. Alberta's Physician Office System Program ("POSP") and HIA/PIA requirements are cases in point: POSP or Vendor Conformance and Usability Requirements ("VCUR") compliance includes minimum standards for P.I./H.I.; installation of any new record-keeping systems in Alberta now require Privacy Impact Assessments to be delivered to the Alberta Privacy Commissioner's office for review. Other similar programs (e.g. Smart Systems for Health in Ontario) are similarly becoming more integrated with privacy law requirements (as well as security).

These requirements have forced IT vendors and users alike to analyse both existing and proposed systems from the perspective of patient privacy rights.

(b) How are physicians' roles as "trusted gatekeeper" affected?

Physicians proposing to purchase electronic systems are encouraged through funding mechanisms such as POSP and SSH to deal with "approved" vendors. In addition, the requirement to analyse new procedures in terms of relatively formal Privacy Impact Assessment documents forces physicians' attention to focus directly on the management of information in a context of patients' privacy rights.

It is also becoming increasingly impossible for a physician to practice in "information isolation", so the ability of physicians to exercise the control they might once have had as "exclusive holder" of certain Health Information must now be reconsidered (and, for instance, this is the motivation for the Ontario H.I. regulatory regime's inclusion of "lock-boxing" certain portions of P.I./H.I.).

1.4 Conclusion

In our next article, we will visit some of the potential and already-real impacts of IT in the healthcare arena, including a review of some potential benefits and some privacy-related risks of Healthcare IT systems implementation, both on a broad regional scale and a physician-office scale.



<i>For further information contact:</i>	Alberta	Ontario	Montreal
British Columbia	Michael Whitt mwhitt@blgcanada.com (403) 232-9571	Mark J. Fecenko mfecenko@blgcanada.com (416) 367-6711	Patricia Galella pgalella@blgcanada.com (514) 954-2514
Andrew Loh aloh@blgcanada.com (604) 640-4069	Andrea Malekos amalekos@blgcanada.com (403) 232-9722	Bernadette Eischen beischen@blgcanada.com (613) 787-3721	Patrice Martin pmartin@blgcanada.com (514) 954-2546
Robert Deane rdeane@blgcanada.com (604) 640-4250		Jennifer Aitken jaitken@blgcanada.com (613) 787-3554	