



Privacy 201 Healthcare Privacy and Information Technology in Canada - Part II

Michael Whitt

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 precursor in the last issue of this publication – Volume 19 #4) is designed to be informative and accessible to informatics professionals, medical professionals, and non-specialist managers. The 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.

First, an introduction to legal theory about regulatory schemes, and then back to the Frequently Asked Questions format.

When legal scholars talk about the "regulation of human behaviours", most of the time they talk about "modalities of regulation" and discuss different mechanisms, which have the effect of motivating or de-motivating certain targeted behaviours, grouping the various specific mechanisms into broad categories, or "modalities".

Lawrence Lessig, a legal scholar of some note, currently at Stanford Law School, has written extensively about four "modalities": 1) coercion, 2) market forces, 3) social mores, and 4) system architectures. Coercion means the power of the state to enforce laws. Market forces refers to things like shifts in tort liability (e.g. seatbelt laws which apportion liability to injured passengers not wearing seatbelts), public disclosure requirements, fines or penalties, tax systems which motivate investment behaviours, and so on. Social mores are societal beliefs or standards of behaviour. System architectures refers to concepts like placing walls and doors in a floor plan to force traffic entry and exit behaviours to take place in a desired way.

Casting our mind to the regulation of personal informational privacy, it becomes apparent that most privacy regulatory regimes exercise some mechanisms in each of these "modalities". Examples of the modalities include modern privacy law requirements: to notify data subjects of unlawful disclosures of their personal information and to provide credit-watch services to them, moving the cost of mitigation strategies to the collecting organization and away from the data subject; providing civil liability for privacy breaches; permitting data subjects to collect consequential damages arising from the statutory breach; order-making and "Privacy Impact Assessment" (PIA) rules allowing Privacy Commissioners to require organizations to follow new and different processes (and undertake new costs) in order to come into compliance; and publication of findings, commonly called the "power to embarrass", resulting in negative publicity for findings of breaches of privacy rules.

From an IT practitioner's perspective, it is probably most useful to understand that the "architectural" modality of regulation of behaviours is one of the areas where systems design and implementation design can very much cause user behaviours, whether individual or organizational, to comply or fail to comply with informational privacy rules or other rules.

It has been tempting, during the initial phases of privacy regulatory schemes, to be quite cynical, to view the rules as having no teeth. However, we are beginning to see the solutions to concerns addressed in earlier days by privacy advocates (including some very astute people in early-stage healthcare informatics – see the COACH retrospective recently published here and look at the dates of some of the conferences with patient informational privacy as a key concern!). We now think that these new privacy regulations are a good beginning at providing IT vendors and users in the healthcare realm with some relative "immunity" from concern about personal information privacy,

in exchange for following a regime which recognizes the concepts of consent, limited collection, directed and thoughtful use, limited and ethical re-use, secure retention, limited sharing and destruction.

In those regards, these “‘data collectors’ immunity acts” are beginning to look more successful.

Now, for some FAQ’s on more specific concerns in the Healthcare IT realm:

Q1: How should Healthcare IT professionals “attack the problem” of personal informational privacy? Is there a point of entry to these issues, or a methodology which might help IT professionals get started?

A1: What we first need to conceive, on a “high level”, is a useful definition of “personal information”. To my mind, personal information includes information about an identifiable human individual, and can include inferred information such as place/time/identity in a video-surveillance, place/time/activity/identity in an email log or tracking mechanism, time-and-motion information in a surveillance record of a telephone operator’s job.

“Protected” personal information seems to mean all personal information, but the “protection” offered by the privacy statutes is only what is “reasonable in the circumstances”, and depends upon the “nature of the information” and sometimes the “reasonable and legitimate expectations of the data subject”. The types of behaviours that are regulated by privacy legislation are: collection, disclosure, use, storage and retention/destruction.

The next thing we need to identify, once we’ve identified that personal information is being collected, disclosed, or used, is the purpose behind the collection/disclosure/use. The purpose will tell us whether there is a legitimate and reasonable “rationale” for the collection/disclosure/use, and should give us some idea about whether the collection/disclosure/use needs to be “announced” to the data-subject, as well as whether consent (other than some form of implied consent through participation in the underlying activity) is also required.

Finally, we should examine whether the personal information that we properly collect/disclose/use is kept “securely” and “for a reasonable length of time and not longer”, which will raise some policy issues in an IT systems and operational sense.

Q2: How should a Healthcare IT Manager think through issues of Privacy law compliance? When should that thinking now be done?

A2: Healthcare IT Managers should be thinking about impacts of IT systems on the privacy and security of patient information (meaning patients’ personal information and health information) as a fundamental concern at all times. This is not news to Healthcare IT professionals, and in fact has been a “hot button” topic

of discussion and concern in Canadian Healthcare Informatics circles for decades.

Perhaps the best time to focus on privacy and security of patient information is whenever systems are proposed to be altered or changed (“systems” can be thought of as both hardware/software systems as well as personnel policies and training, and systems, policies or procedures with regard to collection, recordation (data-entry), access, sharing, disclosure, storage, processing or retention/destruction.

In most privacy regimes, whenever a patient-record system is altered, a PIA must be undertaken, documented, and provided to the relevant Privacy Commissioner or regulator.

Good PIA’s will include a step-by-step analysis of each collection, storage, access, disclosure, communication or transmission, retention or destruction and other “transaction” undertaken with patient information. Each of those transactions will be identified, and the authorization for the transaction will be understood (for example, patient information is collected in a physician’s private office with authorization from the patient; it may be disclosed to a third party such as a specialist, lab or insurer under a different authorization), and any required notices or consents (express or implied) will also be recorded with policies or procedures to obtain and record (if necessary) the consents and provide notices of different types. This type and level of analysis is now required by law, as well as being prudent practice in a Healthcare IT setting.

In addition, contractual obligations should be imposed upon IT software/hardware and service providers, along the lines outlined in the list below. Vendors should not quibble or equivocate with regard to contractual terms which are required by Canadian privacy law. In addition to those terms, we often see “indemnification” language where vendors will be forced to agree to assume liability suffered by healthcare organizations in consequence of a vendor failure with regard to privacy matters, and in a growing number of settings, we are seeing those indemnities being unlimited in amount. Finally, breach of obligations by Vendors with respect to personal information protections is increasingly being treated in contract settings as grounds for “immediate termination or suspension” of the contract.

Q3: What minimum contract terms are required in arrangements between the healthcare provider and its IT outsource provider in order to comply with Canadian privacy law?

A3: Generally, the following terms should be included in any healthcare outsourcing arrangement in order to comply with Canadian privacy laws, where personal information is transmitted to or handled by a third party processor or service-provider:

Ownership of the data does not pass to the service-provider, but is maintained by the healthcare organization (or the patient).

The IT service provider is required to maintain safeguards to protect any data in its hands from corruption, erasure, alteration, copying, accessing, modification, or disclosure by or to third parties, including administrative procedures and policies, and technical and physical security mechanisms which are adequate in the context of the sensitivity of the personal information in the data.

The healthcare organization maintains a constant right to access the data and to audit the data's integrity and the IT service provider's uses, disclosures and other dealings with the data, and the integrity of the service provider's procedures.

The healthcare organization must control the destruction of the data, and should also maintain direct management of all aspects of its relationship with its patients (no secondary uses).

Transmissions of the data should be via secure mechanisms, such as encryption to suitably robust standards, compression which is acceptable in terms of "lossiness" or error/artifact-introduction, and using means which are suitably free from third party ability to access or intercept (e.g. Over private – or "virtually private" - versus public networks).

Q4: What "notice" would be prudent to give to patients if outsourcing IT services to a US provider, particularly in light of the US PATRIOT Act? Is this a realistic concern?

A4: First off, we should remember that the US PATRIOT Act is currently under review, and there is every likelihood that some semblance of more typically expected "due process" rules and controls over "state surveillance of private citizens" in the US will be restored.

Secondly, we should also remember that there are similar electronic surveillance tools available to Canadian state officials, including police and security personnel having responsibility for national security and anti-terrorist and anti-criminal activities, which permit access to private information without court order or notice to the data subjects; and that access to Canadian citizens' personal information may be acquired by foreign states through a variety of crime and terrorist related bi-lateral and multi-lateral treaties.

Health information is similar to other types of regulated personal information in some important senses, and there is therefore some merit in making analogies from private sector commercial or consumer settings dealing with personal information, where there has been more activity, in order to provide some reliable guidance with regard to this issue.

In the CIBC Patriot Act complaint (PIPEDA Case Summary #313 – 19 October 2005), the Federal Privacy Commissioner found the following wording was appropriate in the Terms and Conditions published by CIBC/VISA to its customers:

"I acknowledge that in the event that a Service Provider is located in the United States, my information may

be processed and stored in the United States and that United States governments, courts or law enforcement or regulatory agencies may be able to obtain disclosure of my information through the laws of the United States... I acknowledge and agree that the... paragraphs above constitute prior written notice to me of, and my consent to the collection, use and disclosure of my personal information as described above..."

The federal Privacy Commissioner in that case (and in other settings) says that:

"at the very least, a company in Canada that outsources information processing to the United States should notify its customers that their information may be available to the US Governments or their agencies under a lawful order made in that country."

In a similar vein, in an informal discussion with the Alberta Privacy Commissioner's office, the following language was thought to be adequate in the case where a subscription computer service provider with Albertan retail customers proposed to outsource billing and back-office information systems off-shore:

"...XXXX Co. will be implementing a number of process improvements in the months ahead that will result in outsourcing some back office administrative functions. Specifically, invoicing, payment processing, service agreement renewal and other activities will be performed on XXXX Co.'s behalf by a specialist third party organization with international locations. This will deliver expert support to all of our customers while allowing XXXX Co. to focus on our area of expertise – providing outstanding <type of business> solutions.

The process improvements will require us to disclose some personal information to the third party organization such as your name, address, payment information (credit card or bank account detail) and customer number. We will make every reasonable effort to minimize the amount of information that is shared, and please be aware that all parties are contractually required to comply with all laws established to protect your privacy."

In 2005, The British Columbia Privacy Commissioner provided a good analysis of the impact of the US PATRIOT Act on outsourcing of certain British Columbia government healthcare informatics processes to US service providers. The British Columbia legislature has responded to some of those concerns by prescribing conditions limiting outsourcing off-shore of Canada. We expect other jurisdictions to approach this difficult problem in different ways, but by giving the notices set out above, and by following proper analysis and embedding proper contract terms, most healthcare providers should be in good shape in complying with privacy regulation.

Conclusion:

We hope that this "short course" introducing personal informational privacy regulation, proves thought-

provoking and useful, and provides a framework or toolkit for your own rigorous thinking and analysis. It should not take the place of fact-specific legal and other professional advice in this area. If there are any questions or concerns, we would welcome them, either through this publication's editor, or directly to any of professionals listed below.

The views expressed here are solely the author's and should not be attributed to Borden Ladner Gervais LLP or its clients. The author makes no claims, promises

or guarantees about the accuracy, completeness or adequacy of any information referred to or contained herein. No person should act or refrain from acting in reliance on any information found in this publication without first obtaining appropriate professional advice. This publication is presented for informational purposes only and does not constitute legal or other professional advice and does not create a solicitor-client relationship between you and the author. ●

For Further Information Contact:

British Columbia

Andrew Loh
Robert Deane

Email

aloh@blgcanada.com
rdeane@blgcanada.com

Direct Phone

(604) 640-4069
(604) 640-4250

Alberta

Michael Whitt
Andrea Malekos

Email

mwhitt@blgcanada.com
amalekos@blgcanada.com

Direct Phone

(403) 232-9571
(403) 232-9722

Ontario

Mark J. Fecenko
Bernadette Eischen
Jennifer Aitken

Email

mfecenko@blgcanada.com
beischen@blgcanada.com
jaitken@blgcanada.com

Direct Phone

(416) 367-6711
(613) 787-3721
(613) 787-3554

Montreal

Patricia Galella
Patrice Martin

Email

pgalella@blgcanada.com
pmartin@blgcanada.com

Direct Phone

(514) 954-2514
(514) 954-2546

Introducing...



CLINICARE has some things that are new for 2006.

New Electronic Medical Records software, new pricing, new ASP (Application Service Provider) offerings and new communication and education programs.

Oh yes... we won some awards as well.
#1 Rated EMR since 2003* and Canadian Health Informatics '**Company of the Year**'.

New Pricing! A New Look! Reasons to look at us again!

Find out how we've changed and how we can enhance productivity and help improve the quality of patient care in your practice.

Call us.

* Ranking conducted by KLAS Enterprises, LLC for Ambulatory EMR groups of 6 – 25 physicians. (www.healthcomputing.com)

Trusted. Affordable. Easy.

1-800-563-0579

www.clinicare.com



Best in KLAS



Company of the Year