

Welcome to the Brave New World of Electronic Health Records

Saskatchewan CBA Mid-Winter Conference - February 4, 2011

R. Gary Dickson, Q.C.
Saskatchewan Information and Privacy Commissioner
gdickson@oipc.sk.ca

WHY SHOULD SASKATCHEWAN LAWYERS BECOME FAMILIAR WITH THE EHR?

Why should Saskatchewan lawyers become familiar with the new initiative to create electronic health records (EHR)¹ for every man, woman and child in this province? There are many reasons that can be identified even at this early stage of EHR development.

The EHR will profoundly change the way that health care providers, and health care organizations collect, use and disclose the personal health information of patients. It will change the way patients access their own health information. It will impact the role and activities of the regulatory colleges and provincial organizations such as the Saskatchewan Cancer Agency. It is already creating new venture opportunities for corporations that will act as information management services providers or will offer patient portals that can be utilized by patients wishing to book appointments, review different kinds of test results and to communicate with their care providers. It will also have implications for malpractice litigation, employment cases that turn on return to work assessments, Workers Compensation Act and *Automobile Accident Insurance Act* files.

The kind of personal information that will be the feedstock for the EHRI is generally considered by Saskatchewan residents as their most sensitive and prejudicial information. It will be the kind of information that the Supreme Court of Canada has described in privacy law jurisprudence as close to “the biographical core”² of the individual. At the same time, the advent of the EHR means that personal health information about any given patient hitherto exposed to a relatively small number of care providers with some direct connection to the patient will potentially be available to many thousands of providers throughout Saskatchewan and in time to many more providers in other parts of Canada.

The EHRI technology and the issues spawned by the utilization of this technology will require a reevaluation of legal concepts and practices developed over a long period of time to address paper records. It will also require a revised glossary of terms that borrows heavily from 27 years of Canadian privacy jurisprudence and practice.

WHAT IS THE EHR?

To create a framework to consider some of the legal issues associated with the EHRI it is necessary to consider the nature of the EHRI itself.

¹ In the related literature, there is often reference to EHRI. This relates to the electronic health infrastructure designed to support and enable the EHR.

² R. v. Plant, [1993] 3 S.C.R. 281

An EHR is an integrated health information system that provides authorized users a shared view of health information in a secure environment.

An EHR allows information from specified registries and clinical domain repositories to be accessed by authorized users to inform treatment decisions. Registries or repositories from which information is accessed with an EHRi system normally includes provincial pharmacy, laboratory and diagnostic imaging clinical repositories, and patient and provider registries that contain registration information necessary to properly identify patients and providers to the system. Saskatchewan already has in place several domain repositories- the Pharmaceutical Information Program (PIP), the Diagnostic Imaging and Picture Archiving System (RIS-PACS), Lab Results Repository (SLRR) (so far only in part of the province).

A non-profit corporation, Canada Health Infoway (Infoway), has been created by the federal, provincial and territorial governments to coordinate the design and implementation of the EHRi. The Board of Directors is comprised of the Deputy Ministers of Health from the federal and provincial governments. Infoway has funded a number of projects in Saskatchewan and has required certain standards and oversight in those funded projects. A key concern of Infoway is to ensure that each jurisdiction's EHRi regime will facilitate inter-operable electronic health records across provincial and territorial boundaries.

Within the EHRS Blueprint, Canada Health Infoway says, "An EHR provides each individual in Canada with a secure and private lifetime record of their key health history and care within the health system. The record is available electronically to authorized health providers and the individual anywhere, anytime in support of high quality care. This record is designed to facilitate the sharing of data – across the continuum of care, across healthcare delivery organizations and across geographical areas."

ELECTRONIC HEALTH RECORD OR ELECTRONIC MEDICAL RECORD?

It is important to recognize the difference between the electronic health record and the electronic medical record. As a result of the recent collaboration between the Saskatchewan Medical Association and Saskatchewan Health and new funding for physicians to implement electronic medical records, many more Saskatchewan physicians are creating electronic medical records for use in their medical practice. The goal of the SMA is that 50% of this province's physicians will be using the EMR by March 31, 2012. This EMR will typically be the personal health information of a patient created by the family physician or primary care provider. Unlike the EHR it is not intended to be interoperable and will have fewer fields and less data than the EHR. It will be a much narrower slice of patient information than

may be available to staff in a regional health authority acute care facility who will likely rely more on the EHR for each patient.

STAND-ALONE HEALTH INFORMATION LAWS

In the 1998 Throne Speech of the Saskatchewan Government, it was announced that this province would create the Saskatchewan Health Information Network (SHIN)³ to build and run an electronic health record system. Government also announced at the same time that it intended to enact *The Health Information Protection Act* (HIPA) to enable the EHR and to facilitate sharing of personal health information among trustees.

This initiative paralleled the enactment of the *Personal Health Information Act* in Manitoba in 1997 and the introduction of a stand-alone health information bill in Alberta in that same year⁴. Ontario followed suit in 2004 with the proclamation with the *Personal Health Information Protection Act*. In 2010 a similar law was proclaimed in New Brunswick⁵. Such a law was adopted in 2010 in Newfoundland and Labrador⁶ and awaits proclamation in 2011. The Northwest Territories and Prince Edward Island are likely to introduce similar bills in 2011.

HIPA is focused on certain providers and organizations that are defined as “trustees”. This includes physician clinics, laboratories, diagnostic centres, regional health authorities, pharmacies and pharmacists and a long list of other organizations that have custody or control of personal health information⁷.

Although HIPA was introduced as a bill in the 1999 spring sitting of the Legislative Assembly, it had an unusually long gestation period. The bill didn’t attract Royal Assent until 2003 after several amendments were passed that spring. HIPA was proclaimed on September 1, 2003.

³ Although the original plan was to have SHIN, a separate entity from the Ministry of Health, build the EHRI, the Health Information Solutions Centre (HISC) within the Ministry, has assumed that responsibility for the EHRI to date. On December 21, 2010 the Health Minister announced the creation of eHealth Saskatchewan, a Treasury Board Crown Corporation that will oversee the completion of the provincial electronic health record system.

⁴ The original bill was the subject of significant criticism and was withdrawn at the same time work started on redesigning such a law. The new bill led to the *Health Information Act* c.H-5, RSA 2000 that was proclaimed in 2001.

⁵ *Personal Health Information Privacy and Access Act*, c. P-7.05, SNB 2009

⁶ *Personal Health Information Act*, c.P-7.01, SNL 2008

⁷ The definition of “trustee” in HIPA also includes any government institution for purposes of FOIP but it is unlikely that most of these government ministries or boards, commissions or agencies or their employees will be accredited as users of the EHRI.

HIPA sets out the rules for the collection, use and disclosure of personal health information. This includes a number of transaction specific duties and a smaller number of general duties. The general duties include:

- An obligation for trustees to be transparent about their HIPA activities⁸,
- Duty of trustees to have policies and procedures for HIPA compliance including physical, administrative and technical safeguards for personal health information⁹,
- The data minimization rule, i.e. a trustee must collect, use or disclose the least amount of identifying personal health information necessary for the purpose¹⁰,
- The need-to-know rule that only those persons with a legitimate need to know (for purposes of diagnosis, treatment or care or ancillary support of same) would be exposed to personal health information.¹¹

There are specific rules for the use of PHI of employees for employment purposes¹² by any trustee organization and for Research Ethics Committee approval¹³ of research projects that engage personal health information.

One of the most important features of HIPA is the right of a patient to request in writing access to their own personal health information from any particular trustee¹⁴. This triggers an obligation on the trustee receiving the request to respond within 30 calendar days. There are six circumstances¹⁵ in which the trustee can refuse to provide access but the circumstances will rarely apply. There is also provision for a patient to request the correction of errors in their medical record¹⁶ although this is restricted to factual errors and not differences of opinion.

The Office of the Information and Privacy Commissioner (OIPC) is charged with oversight of trustees in their HIPA duties and responsibilities. The Commissioner has broad powers to investigate but has no order-making power and can only make recommendations to a trustee. There is a right of a de novo

⁸ HIPA, ss. 9, 10

⁹ HIPA, s. 16

¹⁰ HIPA, s. 23(1)

¹¹ HIPA, s. 23(2)

¹² HIPA, s. 26(3)

¹³ HIPA, s. 29

¹⁴ HIPA, s. 32

¹⁵ HIPA, s. 38

¹⁶ HIPA, s. 40

appeal to the Court of Queen's Bench¹⁷ in the event that a trustee rejects the recommendations from the OIPC.

The OIPC has undertaken a number of investigations of breach of privacy complaints and a number of reviews of the refusal of trustees to provide a patient with access to their own personal health information. In the vast majority of cases, these matters are resolved informally through mediation but in the event that is not possible the OIPC publishes on its website (www.oipc.sk.ca) full-text reports that identify the trustee but, in the interests of the complainant or applicant's privacy, do not identify the complainant or applicant. There is an *Annotated Section Index* on the website specifically for reports issued by the Commissioner under HIPA. In addition, since the first major breach of privacy investigation undertaken by the Commissioner resulted in Report H-2005-002 (Prevention Program for Cervical Cancer) that considered approximately sixty provisions and many of the 'moving parts' of HIPA, there is a separate section index for that Report.

The OIPC has an advisory or consultative role and has created a number of tools and resources for trustees that are available on the OIPC website. These include:

- *Glossary of Commonly Used Terms – HIPA*
- *Privacy Breach Guidelines*
- *Best Practices - Mobile Device Security*
- *Faxing Personal Information and Personal Health Information – Best Practices*
- *Systemic Review of Misdirected Faxes*
- *The Management of Access Requests from Patients by Regional Health Authorities*
- *Video Surveillance Guidelines for Saskatchewan Public Bodies*
- Annual Reports of the OIPC including: 2008-2009, pp. 26-30 and 2009-2010, pp. 20-26.

RELATED LEGISLATION

In Saskatchewan there are a number of statutes other than HIPA that may have application in the health information context. This includes *The Mental Health Services Act*¹⁸, *The Regional Health Services Act*¹⁹, *The Workers Compensation Act*²⁰ and *The Automobile Accident Insurance Act*²¹.

¹⁷ HIPA, s. 50

HIPA includes a paramountcy provision²² although Parts II (Rights of the Individual), IV Limits on Collection, Use and Disclosure of PHI by Trustees) and V (Access of Individuals to Personal Health Information) of HIPA do not apply to personal health information obtained for the purposes of certain laws including, Part VIII of *The Automobile Accident Insurance Act*, *The Mental Health Services Act*, *The Public Health Act*, 1994.

There is also the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA)²³ that applies to most organizations in Saskatchewan that collect, use or disclose personal information in the course of commercial activities. In fact, the reach of PIPEDA in practical terms is very limited in the health care context even though “personal information” for purposes of PIPEDA includes personal health information. It will not apply to regional health authorities or to universities that are engaged in training programs for health providers such as physicians since those organizations are already subject to provincial regulation, namely the *Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP)²⁴. In addition, even though HIPA is highly unlikely to be designated as “substantially similar” to PIPEDA so as to displace PIPEDA pursuant to section 26(1)(b) of the federal law, the use by the federal Privacy Commissioner of her discretion under section 13(2)(b) means that for practical purposes trustees need to focus on compliance with HIPA.

The foregoing discussion focuses on Saskatchewan statutes or regulations but the pan-Canadian sweep of an interoperable EHRi for every Canadian requires some consideration of the approach in other jurisdictions. The reality is that Saskatchewan would presumably not be willing to share the personal health information of Saskatchewan patients with organizations in other provinces and territories unless there is adequate reciprocal protection for the privacy of Saskatchewan patients and the confidentiality of their PHI. The concern that flows from the need for reciprocity led directly to the development of the *Pan Canadian Health Information Privacy and Confidentiality Framework*²⁵ (the Framework) in 2003. A key feature of the Framework was that the consent model chosen as a national standard was implied consent. This instrument was endorsed by all Canadian jurisdictions except for Quebec (for the usual

¹⁸ c. M-13.1, S.S. 1984-85-86 as am.

¹⁹ C.R-8.2, S.S. 2002, as am.

²⁰ c. W017.1, S.S. 1979

²¹ c. A-35, S.S. 1978

²² HIPA, Section 4

²³ 2000, c. 5

²⁴ c. L-27.1, S.S. 1990-91 as am.

²⁵ Available at <http://www.hc-sc.gc.ca/hcs-sss/pubs/ehealth-esante/2005-pancanad-priv/index-eng.php>

constitutional reasons) and Saskatchewan. Saskatchewan's opt-out can likely be attributed to its original concern about a stronger consent provision. Despite the fact that HIPA permits a trustee to use any one of three different consent models (express, implied or deemed (no consent)) the early explanatory materials from Saskatchewan Health, regional health authorities and the regulatory colleges relied almost exclusively on the deemed consent or no consent provision. This was presumably done to convenience trustees and trustee organizations. Significantly, as the EHR has progressed in Saskatchewan and other jurisdictions, Saskatchewan has modified its approach and now is featuring *implied consent* in the initial domain repositories constructed for this province's EHR.

Of concern is that there are still many examples of Saskatchewan trustees focused on deemed consent as the preferred option. The OIPC is concerned that relying on implied consent for most EHR applications and yet deemed or no consent for many other collection, use and disclosure activities outside of the EHRi will increase the risk of confusion, indecision and resistance from patients.

There has been very little guidance from Saskatchewan courts on interpretation of HIPA. There is one decision of Mr. Justice Ottenbreit²⁶ of the Court of Queen's Bench that provided brief comments about HIPA but which was focused on the exclusion provision in section 4(4) of HIPA. There have been no judicial decisions to the best knowledge of the OIPC dealing with Saskatchewan's developing EHRi.

In its oversight role, the OIPC has published a number of Reports that involve interpreting different elements of HIPA. The sole OIPC Report that focused specifically on the EHRi is Investigation Report H-2010-001 (L & M Pharmacy Inc., Sunrise Regional Health Authority and Saskatchewan Health)²⁷.

SIGNIFICANT CHALLENGES WITH THE EHR

1) ACCOUNTABILITY

The Legislative Assembly has not included a purpose or object clause in HIPA notwithstanding this is a quasi-constitutional law that describes fundamental rights of patients. Although there is no purpose clause, neither the debate in the Assembly nor the 71 different sections in HIPA are particularly helpful

²⁶ Germain v. Automobile Injury Appeal Commission (2009 SKQB 106 CanLII)

²⁷ There are number of OIPC Reports dealing with HIPA and paper records that would have application to the EHR as well. These include: Investigation Reports H-2007-001, F-2007-001, F-2005—001, H-2004-001 and Review Reports H-2009-001, H-2008-002, H-2008-001, H-2007-001, H- 2006-001 and F-2004-006. All of these Reports are available at www.oipc.sk.ca under the *Reports* tab.

in identifying the key purposes of HIPA. While a preamble is generally not evidence of the Assembly's intentions, it has been considered by the OIPC as a useful guide as to the purpose of HIPA. The preamble to HIPA includes the following:

WHEREAS the Legislative Assembly recognizes the following principles with respect to personal health information:

...

That trustees shall be accountable to individuals with respect to the collection, use and disclosure and exercise of custody and control of personal health information.

Significantly, accountability is the first of the 10 principles in the *Model Code for the Protection of Personal Information*²⁸. It is viewed as perhaps the most fundamental of those principles and the foundation for the other nine principles. Accountability means accountable to the individual – the patient in this case.

While it appears quite straight forward that a health trustee who uploads patient information to the EHR will be responsible and accountable for that information and for that action, the situation is much murkier beyond that initial transaction. That uploaded personal health information will now be collected, used and disclosed by other trustees unknown to the initial trustee. The initial trustee exercises no control over other trustees who will be able to use that personal health information contributed by the initial trustee. That information may to some extent be comingled with other kinds of personal health information about the same patient. This other information will come from other domain repositories over which the initial trustee will have no control.

Which trustee will be responsible to the patient for improper collection, use and disclosure and how will that be evident to the patient and his or her counsel? HIPA contemplates the trustee which has custody or control of the personal health information as being accountable to the patient. The issue of custody becomes much more complex with the EHR. When HIPA was developed the contemplation was that there would be a single massive database. In fact the EHRi now under construction is utilizing a different model – one of a distributed network which links information from a number of different domain repositories. It was originally intended that a separate agency- SHIN would be responsible for the EHR. In practice, responsibility was assumed by the Ministry of Health which created the Health

²⁸ Available online at www.cas.ca/cm/ca/en/privacy-code

Information Solutions Centre (HISC) to manage the developing EHRI. It is not clear what the role will be for the recently announced eHealth Saskatchewan. Will this be a trustee for purposes of HIPA? Since it will have a “six member board composed of representatives from partnering groups, including the Saskatchewan Medical Association, the Saskatchewan Cancer Agency, health regions, the business community and the provincial government”²⁹, will this clarify accountability to the patients or make it more difficult? Some of the partnering groups identified in the news release would not qualify as trustees.

Another consideration in terms of accountability is a web of agreements between different trustees that purport to define responsibility for the personal health information involved in any particular EHR program. Some of these agreements may involve bodies that are not trustees. Some of these agreements may create a kind of shared responsibility. Mindful that when everyone takes responsibility it may effectively mean no one is truly responsible, these agreements between trustees are generally opaque to the patient. They are not normally available on the websites of trustee organizations.

It should be noted that the Conceptual Privacy Impact Assessment (PIA)³⁰ for the EHR developed by Infoway clearly identifies the issue of accountability to the patient as an outstanding or unresolved matter.

The problem for a lawyer acting for an aggrieved patient is obvious if the appropriate trustee cannot be readily identified.

2) PATIENT ACCESS TO THEIR OWN PERSONAL HEALTH INFORMATION

As noted earlier, one of the most important features of HIPA is the patient’s right to access their own personal health information. The patient will still be able to make a request for their own information from their primary provider but what will be the process to access all of their information in the EHR? How will this be made transparent to patients?

3) SECURITY

An important feature of the EHRI is role-based access to the electronic health record. This is independent of the individual patient but turns on the role of the particular health care worker in the

²⁹ Government of Saskatchewan News Release – December 21, 2010: EHEALTH SASKATCHEWAN ADVANCES ONE PATIENT: ONE RECORD HEALTH CARE SYSTEM.

³⁰ Available online at https://www2.infoway-inforoute.ca/Documents/CHI_625_PIA_rj13.pdf

system. Each trustee organization must designate an Approver. Each Approver determines which employees in that organization will become an approved User and therefore given the right to enter one of the domain repositories and to use the EHR information. At this early stage of the Saskatchewan EHR no one can accurately predict exactly how many users may be so designated. Given that we have more than 1500 physicians and 9200 registered nurses in Saskatchewan, there could conceivably be 10,000 approved users with access to the EHR and its domain repositories. Contrast that kind of exposure with what happens currently when our phi is in hard copy form – on paper in a file folder in your family doctor’s office. This is not in many cases particularly secure. File cabinets are sometimes not used or not locked. It is likely that almost anyone working in the office can get access to any patient’s file. Although this is not a perfectly secure system the risk is relatively modest. Potentially three or four persons in a sole practitioner’s office could view a patient’s information and perhaps not all would have a legitimate need to know that patient’s information. The risk of improper, unauthorized exposure is qualitatively and quantitatively different with the EHR. It no longer becomes necessary to even enter the file room since access may be as accessible as every desk top computer in any medical facility in the province. It becomes very important to recognize that the injury resulting from a breach of the electronic health record will be to the affected individual but also and perhaps more significantly to the confidence that the broader community has in the security of their most confidential personal information.

The key HIPA provision for purposes of security is section 16. That provides as follows:

16 Subject to the regulations, a trustee that has custody or control of personal health information must establish policies and procedures to maintain administrative, technical and physical safeguards that will:

- (a) protect the integrity, accuracy and confidentiality of the information;*
- (b) protect against any reasonably anticipated:*
 - (i) threat or hazard to the security or integrity of the information;*
 - (ii) loss of the information; or*
 - (iii) unauthorized access to or use, disclosure or modification of the information; and*
- (c) otherwise ensure compliance with this Act by its employees.*

Section 16 was considered in some detail in the OIPC Investigation Report H-2010-001 (L & M Pharmacy Inc., Sunrise Regional Health Authority and Ministry of Health)³¹. The OIPC was alerted to an apparent privacy breach that involved a pharmacist in the Sunrise Health Region. This involved the unauthorized viewing of personal health information of three individuals by a pharmacist employed by L & M. This viewing involved nine different viewing transactions at a time when none of the individuals were patients of that pharmacy. All of the viewing by the pharmacist was done by means of his accredited role as a User of the Pharmaceutical Information Program (PIP) and as an employee of L & M. The pharmacist was accredited as a User for purposes of the pharmacy in which he worked and also as a User at the hospital within the Region for which he was a contractor. The OIPC undertook a breach of privacy investigation under the authority of HIPA. It found that L & M was responsible for the actions of its employee. It also found that L & M breached HIPA in a number of respects, chiefly by failing to adopt policies and procedures to protect the personal health information in its custody or control as required by section 16 of HIPA. The viewing of the drug profiles was a “collection” of personal health information under HIPA that was improper.

The OIPC recommended that User privileges of the pharmacist be suspended until L & M implement appropriate policy and procedures. That pharmacist’s use of PIP, once his User status is restored, should be subject of regular monthly audits by HISC for a one year period to ensure HIPA compliance. The OIPC also recommended changes to the PIP accreditation process and to log-on procedures by any pharmacist who seeks to view the PIP database. In addition, the OIPC recommended that Saskatchewan Health develop a policy to revoke or suspend User access temporarily or permanently for a registered User that views personal health information contrary to HIPA. Finally, the OIPC recommended improvements to HIPA training for pharmacists that focused on the twin problems of carelessness and curiosity.

In a Postscript to Investigation Report H-2010-001, the OIPC highlighted a significant weakness with the EHR that is being constructed in Saskatchewan as follows:

While there has been a lot of attention to the risk that some outsider may attempt to compromise the relatively elaborate technical safeguards and security features attached to the EHR domain repositories, there has been much less attention paid to the more likely risks

³¹ The full text Report is available online at www.oipc.sk.ca under the Reports tab.

*illuminated in this investigation – the risks posed by the carelessness of trustee organizations and the curiosity of their employees and contractors.*³²

In addition to discussing the threat posed by carelessness and curiosity, the OIPC considered the apparent reaction by some administrative trustees as follows:

*This investigation also underscores the dangerous misconception that a breach of someone's privacy is somehow less serious if the wrongdoer is not motivated by malice or financial gain. In my experience, it is cold and empty comfort to the violated patient whose information has been collected, used or disclosed unlawfully to be advised that the perpetrator was not an identity thief. It is critically important that all persons involved in our health care system recognize that motive is largely irrelevant when some patient's privacy is violated. This attitudinal change requires a clear understanding that privacy is about each of us having a significant measure of control about the information that relates to us. Given the prejudicial nature of personal health information, there may be no arena where privacy is more important than that involving diagnosis, treatment and care of patients. There are already a percentage of patients who refuse to disclose certain health history to their primary care providers. As Saskatchewan constructs an ambitious and expensive EHR system, it will be important for trustees to demonstrate that patients can be confident that their privacy will not be at risk with the move to electronic record which may be accessible to many more individuals than was ever the case with paper records.*³³

It would be hard to exaggerate the importance of training health care staff to a comfortable understanding of what HIPA requires of trustees. This includes acquiring familiarity with the function-specific rules for collection, use, disclosure, access and correction but also with the general rules enumerated above.

4) PRIVACY SUBSUMES CONFIDENTIALITY

Saskatchewan health care workers have long worked in a tradition of confidentiality. It is important for them to recognize that with the advent of HIPA and electronic health records, they are now expected to operate in a privacy sensitive fashion as well. What is new, due to HIPA, is the privacy piece. This is a

³² Page 52

³³ Investigation Report H-2010-001, p. 53

set of elements that speak to a degree of patient control and go significantly beyond the culture of confidentiality. Confidentiality speaks only to keeping the information safe once it is in the custody of the trustee. The new privacy requirements however include:

- the patient's right to transparency from trustees as to what personal health information they will collect, how they will use it and who and when they will disclose it;
- the patient's statutory right to obtain access to their own personal health information within 30 calendar days of making a written request;
- the patient's right to request that errors be corrected; and,
- the right for an aggrieved patient to request that an independent Information and Privacy Commissioner investigate an alleged breach of privacy.

5) BREACH NOTIFICATION

In the event of a breach of privacy under HIPA, there is no explicit duty to notify the affected individual. Section 10 of HIPA has a passive provision that requires a trustee to be able to respond to an inquiry from a patient about any disclosure of the individual's personal health information made without consent. This would not apply to disclosures made in the course of providing or supporting the provision of health services. Nonetheless, it appears that a number of trustees are committing to voluntarily provide notice to the individual consistent with privacy best practice. This practice is encouraged by the OIPC . The OIPC has produced a set of *Privacy Breach Guidelines*³⁴ that codify Canadian best practices for dealing with privacy breaches. One issue with the advent of the EHR is the likelihood that the affected patient may not even be aware of the breach if there is no notification.

6) SO, WHAT HAPPENS WHEN THE PROACTIVE ACTIONS DON'T STOP BREACHES?

What happens when the HIPA education is inadequate, when all users are not exposed to it, when auditing is only done after the fact and privacy breaches are treated too casually by trustees?

The offence provision is section 64 of HIPA. This captures:

- Knowingly contravening any provision of this Act or the regulation
- Obstructing the OIPC
- Wilfully destroying any record to evade an access request

³⁴ Available at www.oipc.sk.ca under the *Resources* tab.

- Obtaining another's personal health information by false representation

This is by summary conviction process with maximum fine of \$50,000 and imprisonment for one year or less for an individual and \$500,000 for a corporation.

Prosecution must be commenced within two years and then only with the express consent of the Attorney General.

No prosecution has been initiated to date in Saskatchewan under HIPA. There has been only one prosecution in Manitoba that resulted in an absolute discharge. This occurred shortly after that province's stand alone health information law came into force and involved the sale of a list of customers of an optician. The single prosecution in Alberta resulted in a \$10,000 fine for an employee in a medical clinic. This employee was having an affair with the husband of a patient. The employee shared test results and other personal health information of the patient with the husband.

DISCIPLINE BY REGULATORY BODY

A number of physicians, at least one pharmacist and several other health professionals have been disciplined by means of fines for violating the confidentiality of a patient. See also the discussion of the role of the College of Pharmacists in OIPC Investigation Report H-2010-001 (L & M Pharmacy Inc., Sunrise Regional Health Authority and Saskatchewan Health).

DISCIPLINE BY EMPLOYER

A relatively small number of employees of regional health authorities have been dismissed for cause for breaching HIPA. In two major cases (one in Saskatoon Regional Health Authority and one in Regina Qu'Appelle Regional Health Authority) arbitrators quashed the termination and substituted suspensions of 20 days and two weeks respectively without pay.

In CUPE, Local 3967 and Regina Qu'Appelle Health Region the employee in question worked as a Health Records Clerk in the Health Information Management Services at an acute care hospital. She would have had extensive training with respect to HIPA and worked in the office that would be seen within that Region as a key resource in understanding and complying with HIPA. Nonetheless she chose to utilize her access privileges to view the electronic record of treatment provided to a one of her work colleagues without that person's consent and contrary to the provisions of HIPA. The Panel however

found that “while, in our view, the breach was prompted by a combination of concern for the colleague in question and curiosity, it can not be said that the breach was done out of malice or for personal gain.” The Panel also found as a mitigating circumstance that the employee had apologized to the colleague whose confidentiality was breached and when questioned about the incident readily admitted her wrong doing.

In SEIU-West and Saskatoon Regional Health Authority (St. Paul’s Hospital) an employee not only had experience as a Patient Registration Clerk and had been an employee in the Department of Health Information Services at an acute care hospital but she was a trainer of users of these computerized patient information systems. Part of her training was to reinforce the Employer’s Confidentiality Policy with the trainees, particularly as it related to logging on and off computers. She had signed a Statement of Understanding on Confidentiality which confirmed that she had read this Policy and understood that all health information to which she may have access is confidential and is not to be communicated to anyone, in any manner, except as outlined by the Employer’s policy and provincial legislation. In that role she had access privileges to a computer system that tracked everything that happened to a patient in any of the Region’s 22 facilities.

It is interesting that in both Saskatoon and RQHR cases, the employee grieving dismissal would presumably have been much more familiar than the majority of health region employees with HIPA and the corresponding rules with respect to health records. What is striking about these arbitration decisions is that in each, the analysis reflects consideration only of the employee and the individuals whose personal health information was compromised. In neither decision is there any reference to the EHR nor the risks associated with role based access. Nor is there any explicit discussion of HIPA and its application to the information in question.

There is no discussion in either decision of the potential impact and injury to public confidence in trustees who will soon have access to an unprecedented amount of personal health information for each individual. It must be said that the precedent set by the two arbitration decisions is most unhelpful in the campaign by health trustees in the province to emphasize the importance of protecting the personal health information that will be available to many thousands of health sector employees in the EHR era.

The challenge is to recognize the fundamentally different kind of risk to privacy which is associated with the electronic health record and the importance of serious consequences for those users who view, use

or disclose personal health information for personal purposes. Part of the challenge in Canadian provinces with laws like HIPA will be to consider the expectations of patients and to recognize that different times and circumstances warrant different attitudes than those that traditionally have prevailed in a paper-driven healthcare system.

RESOURCES

SASKATCHEWAN

Saskatchewan OIPC (www.oipc.sk.ca)

Investigation Report H-2010-001

Glossary of Commonly Used Terms – HIPA

Annual Report 2009-2010, pages 20-26

(<http://www.oipc.sk.ca/Annual%20Reports/Annual%20Report%202009-2010%20FINAL.pdf>)

Annual Report 2008-2009, pages 26-30

(http://www.oipc.sk.ca/Annual_Report_2008-2009.pdf)

Saskatchewan College of Physicians and Surgeons (www.quadrant.net.com/cpss)

Privacy Toolkit

CANADIAN MEDICAL ASSOCIATION/SASKATCHEWAN MEDICAL ASSOCIATION

Health Care Transformation in Canada

Principles for the Protection of Patients' PHI

Data Sharing Agreements: Principles for Electronic Medical Records/Electronic Health Records

Physician Guidelines for Online Communication with Patients

Still in development – a new Privacy Code to supplant the *Privacy Code* (1998)

Saskatchewan Health

<http://www.health.gov.sk.ca/health-information-protection-act>

CANADA HEALTH INFOWAY

White Paper on Information governance of the Interoperable Electronic Health Record

*Conceptual Privacy Impact Assessment of Canada's Electronic Health Record Solution Blueprint
Version 2*

Pan-Canadian Health Information Privacy and Confidentiality Framework

CANADA HEALTH INFORMATICS ASSOCIATION (COACH)

*Putting it into Practice: Privacy and Security for Healthcare Providers Implementing Electronic Medical
Records 2010 Guidelines for the Protection of Health Information Special Edition*

([http://www.coachorg.com/publications/privacy & security_/2010_special_edition.htm](http://www.coachorg.com/publications/privacy_and_security_/2010_special_edition.htm))

ALBERTA

PIA Requirements – http://www.oipc.ab.ca/Content_Files/Files/PIAs/PIA_Requirements_2010.pdf

HIA Guide – http://www.oipc.ab.ca/Content_Files/Files/Publications/HIA_Guide_August_2010.pdf

Netcare Investigation Report – <http://www.oipc.ab.ca/downloads/documentloader.ashx?id=2256>

AHW Netcare website link – <http://www.albertanetcare.ca/>

AHW Guidelines Manual- [http://www.health.alberta.ca/documents/HIA-Guidelines-Practices-
Manual.pdf](http://www.health.alberta.ca/documents/HIA-Guidelines-Practices-Manual.pdf)

CPSA – Data Stewardship Framework-

http://www.cpsa.ab.ca/Libraries/Res/CPSA_Data_Stewardship_Framework.sflb.ashx

CPSA – Secondary Use of Health Information – [http://www.cpsa.ab.ca/Libraries/Res/Secondary_Use
of_Health_Information_-_Final_December_2009.sflb.ashx](http://www.cpsa.ab.ca/Libraries/Res/Secondary_Use_of_Health_Information_-_Final_December_2009.sflb.ashx)

Also, Alberta OIPC Investigation Reports: H2009-IR-003, F2009-IR-001, H2009-IR-06 and H2008-IR-001 all available at www.oipc.ab.ca

ONTARIO

Toolkit for doctors making the transition from paper-based to electronic records-

<http://www.ipc.on.ca/images/Resources/hipa-toolforphysicians.pdf>.

Order No. 2 – Ottawa Hospital breach – http://www.ipc.on.ca/images/Findings/up-HO_002.pdf

BRITISH COLUMBIA

OIPC Investigation F10-02 (http://www.oipc.bc.ca/orders/investigation_reports/InvestigationReportF10-02.pdf)