SASKATCHEWAN

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

INVESTIGATION REPORT H-2010-001

L & M Pharmacy Inc.
Sunrise Regional Health Authority
Ministry of Health

Summary: The Saskatchewan Information and Privacy Commissioner (the Commissioner) was alerted to an apparent privacy breach by a pharmacist in the Sunrise Health Region (Region). This involved the unauthorized viewing of personal health information of three individuals by a pharmacist employed by L & M Pharmacy Inc. (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 User at the hospital within the Region for which he was a contractor.

The Commissioner's office undertook a breach of privacy investigation under the authority of *The Health Information Protection Act* (HIPA). He found that L & M was responsible for the actions of its employee. He 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 Commissioner recommended that the 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 the subject of regular monthly audits by HISC for a one year period to ensure HIPA compliance. The Commissioner 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, he 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, he also recommended improvements to HIPA training for pharmacists that focuses on the twin problems of carelessness and curiosity.

Statutes Cited: *The Health Information Protection Act*, (S.S. 1999, c. H-0.021) ss. 2(m), 2(t), 2(u), 9, 10, 16, 18, 23, 24, 24(2), 24(3), 24(4), 25, 25(1)(f), 27, 27(3), 27(4)(a), 27(4)(l), 27(4)(n), 27(4)(o), 27(4)(p), 28, 29, 30, 42(c), 43(2)(f), 52(b), 52(c), 52(d) 52(e); *The Pharmacy Act, 1996* (S.S. 1996, c. P-9.1); *Personal Information Protection and Electronic Documents Act* (S.C. 2000, c.5 as amended) s. 13(2)(b).

Authorities Cited: Saskatchewan Information and Privacy Commissioner (OIPC) Report H-2008-002 and Investigation Reports H-2007-001, H-2005-002 and H-2004-001; Alberta OIPC Investigation Report H2008-IR-001; British Columbia OIPC Investigation Report F10-02.

Other Sources Cited: Saskatchewan OIPC, *2008-2009 Annual Report; Saskatchewan FOIP FOLIO Newsletter* (February 2007); Saskatchewan Ministry of Health, *For Patient's Sake: Patient First Review Commissioner's Report to the Saskatchewan Ministry of Health, Pharmaceutical Information Program (PIP), Pharmaceutical Information Program (PIP) – Frequently Asked Questions*; Saskatchewan College of Pharmacists, *Patient Confidentiality and the Release of Confidential Records* (Aug. 2004), *Policy Statement – Pharmacists Accessing Patient-specific Information from the Medication Profile Viewer (MPV) Available Under the Pharmaceutical Information Program (PIP)* (Sept. 2006), *Guidelines – Pharmacists Accessing Patient-specific Information from the Medication Profile Viewer (MPV) Available Under the Pharmaceutical Information Program (PIP)* (March 2006), *Preparing Your Community Pharmacy for HIPA and PIPEDA* (Aug. 2004), *Sample Employee Privacy Pledge, Privacy Policies*; Canada Health Infoway, *EHRS Blueprint – an interoperable EHR framework, Executive Overview* (April 2006).

I. BACKGROUND

The Complaint

[1] In the spring of 2009, an individual (C) contacted the Drug Plan and Extended Benefits Branch of Saskatchewan Health and requested a report[1] from Saskatchewan's Pharmaceutical Information Program (PIP) on who had viewed his drug profiles and those of two family members. He expressed a concern that someone may have viewed these profiles improperly. This led to a prompt investigation by the Sunrise Regional Health Authority (Sunrise). Following certain preliminary findings from that internal investigation, our office was consulted.

Initiating our Investigation

[2] This is the first alleged privacy breach that had come to the Office of the Information and Privacy Commissioner (OIPC) with respect to PIP. On August 19, 2009 I wrote to L & M Pharmacy Inc. (L & M) and the pharmacist (A) implicated in the Sunrise internal investigation, advising that we would undertake an investigation under section 52(b), (c), (d) and (e) and section 42(c) of *The Health Information Protection Act* (HIPA). Those sections provide as follows:

> **52** The commissioner may:
>
> …
>
> (b) after hearing a trustee, recommend that the trustee:
>
> (i) cease or modify a specified practice of collecting, using or disclosing information that contravenes this Act; and
>
> (ii) destroy collections of personal health information collected in contravention of this Act;
>
> (c) in appropriate circumstances, comment on the collection of personal health information in a manner other than directly from the individual to whom it relates;

[1] The Pharmaceutical Information Program (hereinafter PIP) allows a patient to request information about which PIP users have viewed that person's medication profile. To exercise that right, the patient can call the PIP Privacy Service at 1-800-667-1672 and request an 'access report' on their medication profile.

(d) from time to time, carry out investigations with respect to personal health information in the custody or control of trustees to ensure compliance with this Act;

(e) comment on the implications for protection of personal health information of any aspect of the collection, storage, use or transfer of personal health information.

Application for review

42(1) A person may apply to the commissioner for a review of the matter where:

(a) the person is not satisfied with the decision of a trustee pursuant to section 36;

(b) the person requests an amendment of personal health information pursuant to clause 40(1)(a), and the amendment is not made; or

(c) the person believes that there has been a contravention of this Act.

(2) Subject to subsection (3), an application must be made in accordance with the regulations:

(a) in the case of an application pursuant to clause (1)(a), within one year after:

(i) the applicant is given written notice of the decision of the trustee; or

(ii) the period mentioned in subsection 36(2) or 37(1) expires;

(b) in the case of an application pursuant to clause (1)(b), within one year after the expiry of the period mentioned in subsection 40(3); and

(c) in the case of an application pursuant to clause (1)(c), within one year after the discovery of the alleged contravention.

(3) Where a person has commenced another review process, procedure or mechanism of a trustee, an application pursuant to subsection (1) must be made within one year after the day on which the other review process, procedure or mechanism is completed.[2]

[3] I provided similar notice to Sunrise, to the Ministry of Health (Saskatchewan Health) that is the responsible trustee for PIP and to the Saskatchewan College of Pharmacists (the College).

[2] *The Health Information Protection Act*, S.S. 1999, c. H-0.021. (hereinafter HIPA)

[4] I attended at a hospital (the hospital) in the Sunrise region and interviewed A on August 29, 2009. I subsequently interviewed A in our Regina office on December 8, 2009. I have gathered information that was promptly provided by Sunrise and the Health Information Solutions Centre (HISC). HISC is the agency within Saskatchewan Health that is responsible as an information management services provider[3] for the management of PIP. I also interviewed C as well as two physicians in the same community and the other pharmacist (B) who is also a Director and shareholder in L & M.

Pharmaceutical Information Program (PIP)

[5] A description of PIP appears on the Saskatchewan Health website as follows:

> **What is the Pharmaceutical Information Program?**
>
> The Pharmaceutical Information Program (PIP) will improve the health of Saskatchewan residents, by providing authorized health care professionals (e.g. pharmacists and physicians) with confidential access to patient medication records. Having access to quality information about their patients will help Saskatchewan health care professionals offer the highest quality of care.
>
> Prior to the introduction of PIP, there was no centralized, complete source of prescription records for health care providers to use when making decisions about a patient's drug therapy. PIP will ensure that individuals and their health care providers have the information needed to make the best decisions about their health care.
>
> The Pharmaceutical Information Program is a major step forward in enhancing patient safety. The program will help prescribers select the best medication to avoid drug interactions and duplications of therapy, including prescription drug abuse. PIP will also help health professionals sort through the numerous medications a person may be taking when treating medical conditions, or where several prescribers are involved in a patient's care.[4]

[3] An information management service provider (hereinafter IMSP) is defined by section 2(j) of HIPA as "a person who or body that processes, stores, archives or destroys records of a trustee containing personal health information or that provides information management or information technology services to a trustee with respect to the records of the trustee containing personal health information, and includes a trustee that carries out any of those activities on behalf of another trustee, but does not include a trustee that carries out any of those activities on its own behalf." The role and function of an IMSP is addressed by section 18 of HIPA.

[4] Saskatchewan Health, *Pharmaceutical Information Program (PIP)*, available online at www.health.gov.sk.ca/pip.

[6] Each trustee organization that participates in PIP must have a designated Approver who approves User accounts for their organization. The Approver in the case of L & M was pharmacist B. In this case I am advised by B that his concern was to ensure that all pharmacists employed by L & M could benefit from PIP as quickly as possible. There was no screening process to ensure that these pharmacists had an appropriate familiarity with HIPA and the privacy features of PIP. Users of PIP require a user name and a password in order to log onto PIP. Approvers also have the ability to audit the PIP activities of the individuals they approve as a user but there was no such audit by the Approver at any time prior to this investigation.

[7] Under PIP any patient can request that their drug profile be masked. The procedure for masking is described on the Saskatchewan Health website as follows:

> **If I don't want my personal prescription information shared, what do I do?**
> While there are many benefits to the Pharmaceutical Information Program, we recognize that some people may not be comfortable with the electronic sharing of their personal health information. Residents may choose a masking option (request that prescription information be hidden from view). Individuals who may choose this option should call 1-800-667-1672 for more information. A downloadable Request to Mask form is available.
>
> When authorized health care professionals log into the PIP application and select a masked record, the health care professional will be prevented from seeing any drug profile information, except in three circumstances:
>
> > **With consent:** At any time, you may give your health care provider (such as your physician or pharmacist) consent to view your masked medication profile. This authorization can be time-limited (such as a specified number of days or months) or indefinite.
> >
> > **In an emergency,** when the person is unable to provide consent: This would allow a health care provider to access the history in an emergency, such as if the person is unconscious or unable to provide consent due to their illness. The information could be life-saving in these circumstances.
> >
> > **Dangerous use of prescription drugs:** A list of drug categories has been developed in consultation with the regulatory bodies that license physicians and pharmacists. Health care providers may unmask a profile when

> considering prescribing or dispensing one of these drugs, because there is potential for harm if these drugs are used inappropriately.[5]

[8] Saskatchewan Health is the Trustee with custody of the PIP database.

Subject of our Investigation

[9] The pharmacist A has been licensed since 1975 to practice pharmacy in the province of Saskatchewan. He is also a 50% shareholder and a director of L & M. L & M operates a pharmacy in a community in Sunrise. The other shareholder and Director of L & M (B) is also a licensed pharmacist.

[10] In addition, L & M entered into a *Contract for Supply of Pharmacy Services* (the Contract) with Sunrise to provide a range of pharmaceutical services on site at the hospital. The hospital is an acute care facility operated by Sunrise.

[11] The Contract is dated March 24, 2000 and remains in force from year to year unless and until the agreement expires by one party providing written notification to the other party of not less than 90 days. Apparently no such notification has been given and both the hospital and L & M have proceeded on the basis that the contract remains in force. Clause 6 of the Contract provides as follows:

> 6. Confidentiality as a Contractor of [the hospital] is essential. L & M Pharmacy Inc. will have knowledge of privileged or confidential information about [the hospital] and/or its patients. Any such information must be shared only professionally to serve the best interests of the hospital and its clientele and be kept in the strictest confidence.

[12] There is a detailed description of the services to be provided under the contract but given my findings it is not necessary to discuss those services in this Report. There is an addendum dated June 11, 2008 that provides for a senior pharmacist:

> General Accountability
> The Senior Pharmacist is directly accountable to the Manager of [the hospital].

[5] Saskatchewan Health, *Pharmaceutical Information Program (PIP) – Frequently Asked Questions*, available online at www.health.gov.sk.ca/pip-faq.

> The Senior Pharmacist, as a member of the patient care team, provides visible, proactive leadership and promotes the delivery of patient centred care through the application of established professional best practice standards and within established Sunrise Health Region and [the hospital] policies, procedures and budgetary guidelines.

[13] I was advised by A that he was not aware of who was the 'senior pharmacist' but assumed both he and B would qualify as a 'senior pharmacist' for purposes of the contract.

[14] I understand that approximately 60% of L & M's work at the hospital was performed by A; the balance of the contracted work was performed by B and two other pharmacists employed by L & M.

[15] I was advised that A was a registered user for purposes of PIP in two different capacities. One was utilizing the connection from the pharmacy and the other was utilizing the connection at the pharmaceutical facility in the hospital.

[16] As a direct result of Sunrise's internal investigation, HISC undertook an audit of A's use of PIP and furnished our office with a 26 page printout of transactions in which someone who had signed in as '[A]' from either the pharmacy or the hospital viewed drug profiles for individuals. A acknowledged that the printout accurately represented his activities save for the location recorded for each of the transactions in the printout.

[17] According to the printout, in early 2009 A entered the PIP database to view the drug profiles for an individual (C) and two of that individual's family members. He did this on the following nine different occasions:

Date	**Time**	**Location**
Jan 12, 2009	11:55:00 PM	[hospital] Pharmacy
Jan 12, 2009	11:55:25 PM	[hospital] Pharmacy
Jan 12, 2009	11:55:53 PM	[hospital] Pharmacy
Jan 14, 2009	03:50:44 AM	[hospital] Pharmacy
Jan 14, 2009	03:51:35 AM	[hospital] Pharmacy
Jan 16, 2009	05:01:11 PM	[hospital] Pharmacy
Jan 16, 2009	05:01:37 PM	[hospital] Pharmacy
Jan 27, 2009	12:44:10 PM	[hospital] Pharmacy
Jan 27, 2009	12:44:50 PM	[hospital] Pharmacy

[18] I was advised by A that he may have entered "[hospital] Pharmacy" in the PIP system in error and likely had been viewing the drug profiles on some or all of those nine occasions from either the pharmacy or from his personal computer at his residence. The information available to me indicates that none of the nine viewing transactions in question would likely have originated in the hospital pharmacy and that all of them would have been generated from a computer at the pharmacy or a personal computer at A's residence.

[19] I learned that C and his family had been patients of L & M for many years. In addition, the evidence is consistent that there was a long-standing friendship between A and C's family.

[20] On January 5, 2009 a business arrangement between A and C was dissolved in circumstances that created strong reactions and 'bad feelings' between the two. It was acknowledged by A that he understood that their professional relationship as pharmacist and patient was severed on January 5, 2009 and has not been reinstated since that date. In other words, since January 5, 2009 neither C nor his family members made any use of pharmaceutical services offered by L & M. In addition, the evidence was clear that neither C nor his family members received health services in the hospital on any of those dates when A viewed their drug profiles.

[21] On no occasion when viewing the database did A respond to the prompt on his computer screen for him to enter a "reason code". In other words, the prompt to identify the reason for viewing the drug profile of an individual was ignored on each of the nine occasions when the drug profiles in question were viewed by A. The item on the PIP page states:

> Reason for Accessing Profile (optional):
> __Consultation
> __Prescribing
> __Dispensing
> __Other _____

[22] The default is "other" in the sense that the pharmacist isn't required to do anything other than rely on the default in order to proceed to view patient profiles.

[23] I am advised that the PIP program has *(optional)* listed beside the *Reason for Accessing Profile* field and the narrator on the online training states that completion of this field is "completely optional".

[24] Significantly, both A and B advised that it was their customary practice not to complete the reason code for any of their PIP viewing activities. Indeed this has been confirmed by the printout of PIP transactions from HISC.

[25] The existing PIP system has no ready way of determining whether A, when he signed on as a User to view the PIP database, was physically at the pharmacy or at the hospital or even some other remote location at the time. The user name and the password is the same even if the User has two separate organizations he is working for as is the case with A, L & M and Sunrise. The User printout is only evidence of information concerning the account that the particular User volunteers when doing the viewing. As noted earlier, A acknowledges that a number of his transactions may have inaccurately referenced the hospital as the active account for the query when he was actually conducting the query for former patients of the pharmacy.[6]

[26] I learned that L & M's pharmacy has its own electronic database of its patients and their prescription activity. In other words, PIP is not the only means by which a pharmacist such as A can readily check the prescription history of an individual patient of the pharmacy. What that L & M database would not provide would be information about prescriptions filled by other pharmacies. I learned that there are plans in many pharmacies in Saskatchewan to adopt a new software system that will to some extent integrate PIP with a pharmacy's internal and formerly stand-alone patient data system.

[27] I have considered that A is a former President of the College. He advised that he had been on the governing board of the College when the College was preparing for the proclamation of HIPA. He stated that he was aware of the kinds of tools that the College had made available on its website for Saskatchewan pharmacists to assist them in

[6] In Investigation Report F10-02 the acting British Columbia Information and Privacy Commissioner recommended that Users working in particular clinical setting or program area can only view the records of clients who are receiving services in that setting. Report available online at www.oipc.bc.ca at [86].

becoming compliant with HIPA. He advised that he could not recall any specific HIPA training that he experienced prior to the subject investigation.

[28] I am advised by Sunrise that they undertook their internal investigation in response to the query from C and interviewed A. When asked why he had viewed the personal health information of C and his family members, A could offer no specific reason but speculated that he may have been wondering where they were getting their prescriptions filled after they severed their professional relationship with L & M. Several days after that initial interview he contacted Sunrise to supplement his previous explanation and that the real reason why he had viewed PIP was his concern for the well being of the family since they ceased to be patients of L & M. He stated that he had no malicious intent with the personal health information. At that same time, he apparently acknowledged that his feelings of concern for C and his family did not justify looking at their PIP profiles but he wanted to clarify his reason for doing so.

[29] When I questioned A in August 2009 about his reasons for the nine viewing transactions, he stated that he had a concern with the health of C and suggested that if he found C was not getting the appropriate medication he would share that with the physician who he knew was treating C. This would not apply to the two family members however even if one were to accept that explanation as being sufficient for viewing the information of C.

[30] My office gathered information about the policies and procedures of L & M, such as existed, for the "collection", "use" and "disclosure" of personal health information under HIPA.

[31] Our usual practice is to encourage HIPA complainants to attempt to resolve their concern by dealing first with the appropriate regulatory body.[7] A separate complaint investigation process by a regulatory body however does not bar our office from undertaking a HIPA investigation. In this case, although we were aware that a complaint was being

[7] Section 43(2)(f) of HIPA speaks to professional regulatory bodies. A listing of Saskatchewan regulatory bodies is available online at www.health.gov.sk.ca/health-professional-associations.

investigated by the College, I determined that the interests of accountability to the public for HIPA compliance warranted an OIPC investigation that would examine not only the conduct of the individual pharmacist (A) but also the conduct of the pharmacy operator, L & M, Saskatchewan Health and Sunrise. I am also mindful that this first reported breach by a trustee of PIP required a fuller and more transparent treatment for the benefit of all trustees in Saskatchewan.

[32] I am advised by A that the College investigated this matter in 2009. I have learned that the College advised A by letter dated October 30, 2009 that it will take no disciplinary action against A. This is so notwithstanding that the College apparently determined that the viewing of PIP by A was "not appropriate". It was apparently agreed by A that such viewing of PIP profiles will not occur in the future. The College apparently accepted his affirmation that he will not view the PIP information for any reason other than the primary purpose of providing health services to the subject individual or for an authorized secondary purpose[8].

[33] I was advised by Sunrise that at an early date after the concerns were raised by C, Sunrise suspended the PIP viewing privileges of A. I was further advised that after the College's decision to take no disciplinary action, A's viewing privileges were restored. I understand that A's viewing privileges through the pharmacy operated by L & M did not change at any time.

II. ISSUES

1. **As between A and L & M Pharmacy Inc., who is the responsible trustee(s) under *The Health Information Protection Act*?**

2. **Is the information in question personal health information within section 2(m) of *The Health Information Protection Act*?**

3. **Did L & M Pharmacy Inc. have the policies and procedures required by section 16 of *The Health Information Protection Act*?**

[8] A secondary disclosure is for a purpose unrelated to diagnosis, treatment and care of the patient. Refer to the February 2007 Saskatchewan Information and Privacy Commissioner (hereinafter OIPC) FOIP FOLIO available online at www.oipc.sk.ca, p.4.

4. **Did L & M discharge its "general duties" under *The Health Information Protection Act* aside from section 16?**

5. **Was the action of L & M Pharmacy Inc. a "collection", "use" or a "disclosure" under *The Health Information Protection Act*?**

6. **Were the requirements for a *Health Information Protection Act* collection satisfied by L & M Pharmacy Inc.?**

7. **Was there a further disclosure by L & M Pharmacy Inc. to other trustees?**

8. **Did the Sunrise Regional Health Authority have the policies and procedures required by section 16 of *The Health Information Protection Act*?**

9. **Did the Ministry of Health have appropriate policy and procedures as required by section 16 of *The Health Information Protection Act*?**

III. DISCUSSION OF THE ISSUES

1. As between A and L & M Pharmacy Inc., who is the responsible trustee(s) under *The Health Information Protection Act*?

[34] L & M operates the pharmacy and qualifies as a "proprietor" as defined in *The Pharmacy Act, 1996*.[9] L & M therefore appears to be a "trustee" for purposes of HIPA by reason of section 2(t)(ix). To qualify as a trustee one must be included in the definition in section 2(t) of HIPA but must also have custody or control of personal health information. I have defined custody as physical possession. Control need only be considered if there is no custody by an organization. In this case, L & M had custody of C's personal health information and that of two of C's family members. There was additional information that would be personal health information of C and his family members that was viewed by A when he entered the PIP system for the purpose of the nine transactions described above and that all occurred after the termination of the pharmacist-patient relationship on January 5, 2009. I find that when A entered the system as a User approved by L & M that was effectively a collection by L & M of that personal health information that was being disclosed by Saskatchewan Health as the trustee responsible for PIP.

[9] *The Pharmacy Act, 1996,* S.S. 1996, c. P-9.1.

[35] As a licensed pharmacist, A might qualify as a trustee for purposes of HIPA but only to the extent that he has custody or control of personal health information.[10] On the evidence, at all material times, A was utilizing either the pharmacy computer, his home computer or the computer at the hospital operated by L & M and under contract with Sunrise. In any of the three scenarios however, A was viewing the PIP information under the auspices of L & M. I confirmed this with L & M as well as the pharmacists A and B. I therefore conclude that A was not, in the circumstances of this investigation, a trustee since it was L & M that had either custody or control of the personal health information of C and his family members.

2. Is the information in question personal health information within section 2(m) of *The Health Information Protection Act*?

[36] All of the information in question appears on the drug profile for a patient of a pharmacy. This is all either registration information or information about the physical or mental health of the patient or information about health services provided to the patient or it is information collected incidental to the provision of health service. I find that the information about C and his family members is all "personal health information" within the meaning of section 2(m) of HIPA.

3. Did L & M Pharmacy Inc. have the policies and procedures required by section 16 of *The Health Information Protection Act*?

[37] Section 16 provides as follows:

> **Duty to protect**
>
> **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;

[10] *Supra* note 2 section 2(t)(xii)

(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.

[38] At all relevant times, L & M did not have policies and procedures as required by section 16 of HIPA. This is remarkable given that the College has published on its website a number of tools presumably to assist its pharmacist members and HIPA has now been in force in this province for more than six and one-half years.

[39] I was advised by A on August 28, 2009 that HIPA had been discussed at several staff meetings at the L & M pharmacy but this focused on the 'understanding' that disclosure of personal health information is at the discretion of the pharmacy employee. In fact, that understanding is inaccurate and at odds with sections 27, 28 and 29 of HIPA. Disclosure of personal health information, without patient consent, is unlawful unless one of the prescribed circumstances in those three sections apply.

[40] Section 16 is one of the most important features of HIPA. Without comprehensive written policies and procedures, the risk that a trustee will fall short of its many statutory responsibilities is dramatically increased. We have attempted to underscore this feature in a number of our publications including Review Report H-2008-002 and Investigation Reports H-2007-001, H-2005-002 and H-2004-001.[11]

[41] The tools on the College's website[12] include the following:

1) ***Patient Confidentiality and the Release of Confidential Records*** **(Aug. 2004)**

[11] Saskatchewan Information and Privacy Commissioner (hereinafter OIPC) Report H-2008-002 and Investigation Reports H-2007-001, H-2005-002 and H-2004-001 available online at www.oipc.sk.ca.
[12] Saskatchewan College of Pharmacists, www.napra.org/pages/Saskatchewan/default.aspx.

[42] This document provides in part:

> The *Code of Ethics* of the Saskatchewan College of Pharmacists states that "a pharmacist shall protect the patient's right of confidentiality". During the course of practice, pharmacists acquire medication and other medical and personal information about their patients. Therefore, the pharmacist is ethically obliged to respect the confidential nature of this information.

[43] The same document states that it is recognized that this confidential information must be disclosed in certain circumstances and in other cases should not be disclosed. It then enumerates six different circumstances when confidential patient information may be disclosed to third parties. One of these is as follows:

> Pharmacists and other health care professionals for bona fide medical and/or pharmaceutical reasons where, in the judgement of the pharmacist, it is prudent to provide this information in the interests of **the patient** to protect the mental or physical health or safety of **the patient**.
> [emphasis added]

[44] This 2004 document, it should be noted, makes no reference to HIPA save for a reference at the bottom of the page "Please refer to supplemental guidelines entitled "Preparing Your Community Pharmacy for HIPA and PIPEDA"[13] and "Release of Confidential Records of Minors to Parents/Guardians" although it is dated one year after HIPA came into force. It adequately describes 'confidentiality' concerns but makes no reference to privacy and how HIPA has now created privacy rights that go beyond simply a requirement to protect patient information in the custody or control of the pharmacist. These privacy rights include transparency obligations for trustees, a right of access and to request correction of their personal health information and the right to appeal to an independent OIPC. It would be helpful for the College to revise this document to reflect developments since 2004 and the primacy of HIPA obligations.

[13] When *Personal Information Protection and Electronic Documents Act* (hereinafter PIPEDA) commenced application to organizations collecting, using and disclosing personal health information in the course of commercial activity there was a good deal of attention paid to the requirements of PIPEDA, a federal law. Over time due to the PARTs document as well as section 13(2)(b) of PIPEDA, Saskatchewan trustees have come to recognize HIPA as the primary law of application to them. The PARTs document is available online at: http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/h_gv00207.html.

2) ***Policy Statement – Pharmacists Accessing Patient-specific Information from the Medication Profile Viewer (MPV) Available Under the Pharmaceutical Information Program (PIP)*** **(Sept. 2006)**

[45] This document appropriately references HIPA. It states, among other things,:

> **Access to information within PIP is provided to pharmacists to assist them to deliver** the best possible quality of pharmaceutical **care to their patients**.
>
> **Access, using** or disseminating **information from the PIP Program, other than as permitted in this policy is professional or proprietary misconduct.**
> [emphasis added]

[46] It sets out a nine general principles for pharmacists including:

> 1) Must be able to justify the reason for accessing information through PIP.
> 2) Should only access **information through PIP when the information that the pharmacist expects to obtain may reasonably affect the pharmaceutical care provided to the patient;**
> 3) Should only access the minimum amount of information through PIP that is reasonably required for the purpose for which the information was accessed.
> 4) Should ensure that only those persons who have a need to know the information should be permitted to access the information;
> 5) Should only **use the information from PIP for the purpose of providing pharmaceutical care to their patient, or as is otherwise permitted by privacy legislation or other applicable laws.**
> 6) Should only disclose the information from PIP for the purpose of providing pharmaceutical care to their patient, with the consent of the patient, or as is otherwise permitted by privacy legislation or other applicable laws;
> 7) Should have **appropriate policies and procedures in place to protect the information accessed through PIP from being seen by persons who are not authorized** to see that information;;
> 8) Must **comply with privacy legislation in connection with the information accessed through PIP**; and,
> 9) Should ensure that **persons who the pharmacist authorizes to access the information within PIP are aware of and understand their responsibilities**
>
> [emphasis added]

[47] This instrument is clear that collection, use or disclosure of PIP data is for the benefit of the patient. In the case under investigation, the professional relationship of pharmacist and patient had been severed effective January 5, 2009. The viewing transactions in question however occurred a full week later when the pharmacist A no longer had a professional relationship with the patient or his family.

[48] Pharmacists are also required by this document to report breaches:

> Pharmacists must report to the PIP, or such other person or organization as may be specified by the PIP, all activities by any individual or entity that the pharmacist suspects may compromise the privacy of the patient or confidentiality of the confidential information or be a breach of this policy.

[49] I cannot assess what the other pharmacists in L & M did or did not suspect about the nine viewing transactions in question by A but, in any event, there was to our knowledge no reporting by any other employee or pharmacist of what appeared to be obvious breaches of the College's Policy Statement.

3) ***Guidelines – Pharmacists Accessing Patient-specific Information from the Medication Profile Viewer (MPV) Available Under the Pharmaceutical Information Program (PIP)*** **(March 2006)**

[50] This document, published two and one-half years before A's nine viewing transactions, provides as follows:

> 2. Accountability
> Saskatchewan Health is the trustee for the PIP Database. Personal health information accessed through the PIP is being shared on a trustee to trustee basis under HIPA. The pharmacy proprietor becomes the trustee for all PIP data accessed by the pharmacy. **The pharmacy proprietor is responsible for ensuring that all pharmacists or other persons with access to patient and PIP data within the pharmacy comply with these guidelines.**
>
> 3. Purpose
> The primary purpose for **accessing and use of the PIP data is to support or provide a health service to the patient to whom the personal health information relates**.
> Authorized secondary purposes include using and disclosing the PIP data in the following circumstances:
> (a) where required to collect payment for the health services provided (i.e. benefit under the Drug Plan);

(b) in emergency circumstances where the pharmacist believes on reasonable grounds that the use or disclosure will avoid or minimize a danger to the health or safety of any person;
(c) where the pharmacist believes on reasonable grounds that the prevention of fraud or abuse as it relates to the use or disclosure is necessary for the prevention of fraud or abuse as it relates to prescription drugs in contravention of federal or provincial laws;
(d) where authorized by the patient's express consent.

Care must be taken to ensure only a minimal amount of information is used or disclosed. De-identified information should be used or disclosed if possible**. <u>The pharmacist must notify the patient in writing if they have relied on section 3(b) to disclose information</u>**.

<u>Reasonable grounds means the pharmacist has knowledge of reasonable facts. It does not include a mere suspicion or conclusion based on racial or socio-economic profiling</u>.
…

6. Limiting Use and Disclosure
The Pharmacist will only use and disclose the PIP data on a need to know basis for the primary purpose of providing health services to the subject individual or for an authorized secondary purpose. The PIP data **<u>shall not be accessed, used or disclosed by a pharmacist for personal interest, gossip</u>** or financial gain.
…

7. Safeguards
The pharmacy manager and the pharmacy proprietor must:
(a) implement the security standards outlined in the PIP Security Standards prior to connecting to the PIP;
(b) implement any changes to the PIP Security Standards when advise to do so by the PIP Administration Office;;
(c) ensure **<u>all staff and third parties who will access the PIP data have signed a confidentiality undertaking in the form called "Sample Employee Privacy Pledge</u>** attached to the guidelines entitled "Preparing Your Community Pharmacy for HIPA and PIPEDA"; and
(d) ensure **<u>reasonable security and confidentiality policies, procedures and practices are in place in compliance with applicable law</u>**.

[emphasis added]

[51] After carefully considering the evidence and submissions from A, I have no hesitation in finding that his viewing of PIP information about his former patients was done not for a professional reason but rather for his own personal interest. To the extent that A advised at one point that his viewing of the PIP data was out of concern for the health of the former patient and his family members, he was required by paragraph 3 above to notify the former patient in writing of his viewing activity. He failed to do so. In any event, even if A's motive was genuinely one of concern for C and his family members that does not excuse or justify a breach of HIPA.

4) *Preparing Your Community Pharmacy for HIPA and PIPEDA* (Aug. 2004)

[52] This document available to Saskatchewan pharmacists since August 2004, five years before the nine viewing transactions in question in this investigation, lists "top ten to-do's" recommended by a Saskatchewan law firm. This apparently summarizes key messages from earlier privacy law continuing education sessions in Regina and Saskatoon.

[53] The top ten to-do's include:

1. Designate one or more individuals within your pharmacy who will be responsible for implementing and overseeing privacy compliance.
2. Ensure that proper confidentiality agreements are in place with service providers, affiliates, etc.
3. Identify the various purposes for which the pharmacy collects, uses and discloses personal information.
4. Develop an external communications plan that will provide patients with reasonable notice of the pharmacy's privacy practices.
5. Develop and implement privacy policies and practices for the pharmacy.
6. Implement privacy awareness training for employees
7. Obtain express consent from patients where the patient's consent cannot be implied in the circumstances.
8. Review existing security safeguards to ensure personal information under the control of the pharmacy is properly protected.
9. Develop policies and procedures for dealing with requests by individuals for access to their personal information.
10. Develop policies and procedures for dealing with privacy related complaints.

[54] We have seen no evidence in the course of this investigation that any one of those ten steps recommended in August 2004 were taken by L & M at any time prior to our HIPA investigation in 2009.

5) Sample Employee Privacy Pledge

[55] This includes the statement "The confidentiality of its client's personal health information is a key concern of _____[insert name of pharmacy]…"

[56] The undersigned agrees as follows:

(a) That I will **only access personal health information on a need-to-know basis** for performing services on behalf of the Pharmacy;
(b) That I will **keep all personal health information in my possession in the strictest of confidence and only use such information for the purposes of performing services on behalf of the Pharmacy**;
(c) That upon no longer requiring the personal health information for the purposes of providing services on behalf of the Pharmacy, I will return or destroy all copies of the personal health information in my possession as instructed by the Pharmacy;
(d) That I will **follow all applicable Pharmacy security and confidentiality policies, procedures and practices**;
(e) I acknowledge that I have **read this Confidentiality Pledge and understand that a breach of it may be in contravention of the *Health Information Protection Act* or other applicable laws**.

[emphasis added]

[57] Our investigation found that no such pledge was required or collected from the employees of L & M including A and the other pharmacist employees.

6) Privacy Policies

[58] This document is focused on "collection", "use" and "disclosure" of personal information and the personal health information in the custody of the College itself. It is only relevant insofar as it is yet more evidence of the efforts of the College to signal to its members the importance of meeting statutory privacy obligations.

[59] In addition, Saskatchewan Health has published on its website the following document:

7) The Pharmaceutical Information Program

[60] Under the heading, *Safeguarding Your Information* appears the following:

> Your personal health information is confidential and **only authorized health care professionals involved in your care will access it**.
>
> Saskatchewan Health takes great care to protect the personal health information under its control. Information is kept in strict confidence, and is used or disclosed as authorized by law. Privacy safeguards outlined in *The Health Information Protection Act* (HIPA) apply to the Pharmaceutical Information Program.
>
> Safeguards are in place to ensure **only health professionals involved in your care** access your personal health information in PIP:
>
> - All health care providers are made aware of their responsibilities and agree to maintain confidentiality of information and use it only on a need-to-know basis.
> - All access to the PIP data is tracked and recorded for audit purposes. You can request a printout of who has accessed your information in PIP.
>
> In addition, strict security safeguards are also in place. We have policies and/or practices and computer systems that are designed to protect your information from unauthorized use, error and loss. User access is restricted to authorized health care professionals. High-quality network security is in place and all electronic messages are encrypted.
> [emphasis added]

[61] Contrary to the statement of Saskatchewan Health that confidentiality needs to be maintained and PIP data can be used only on a need-to-know basis, the evidence is that A embarked on a personal initiative outside of any professional pharmacy-patient relationship in his PIP viewing. In other words, he had no legitimate need-to-know the prescription data in PIP about his former patients.

[62] I am advised by the HISC that at the time L & M enrolled in the PIP system, it was required to first execute a *Data Access Agreement*. Once the *Data Access Agreement* was signed the User could "Register for PIP Access".

[63] I have reviewed the document *User Organization Data Access Agreement* dated September 30, 2005 that has been executed by A and B on behalf of L & M. The relevant portion of the *Terms of Use and Disclaimer* are as follows:

> Terms of Use and Disclaimer
>
> By accessing the Pharmaceutical Information Program ("PIP") application, the User Organization's users are viewing confidential personal health information.
>
> Access to the PIP application and the associated data is restricted to trustees and employees of trustees. The Saskatchewan Department of Health (the "Department") is the trustee of the data associated with the PIP application while it is stored or transmitted within the Department's systems. At such time as data associated with the PIP application moves from the Department's systems to those of the User Organization, the User Organization assumes the role of trustee and the responsibilities associated therewith.
>
> The exchange of data associated with the PIP application is intended to be a trustee to trustee disclosure as contemplated under *The Health Information Protection Act* ("*HIPA*").
>
> As a condition to allowing the User Organization's users to access the PIP application, the User Organization agrees to abide by and be legally bound by the following terms and conditions:
>
> (1) Restrictions on Collection, Use and Disclosure of Information in the PIP Application
>
> (a) The User Organization agrees that the information in and accessible through the PIP application (the "Information") is private and confidential and that the User Organization shall take all reasonable steps to maintain the confidentiality of the Information;
>
> (b) The User Organization agrees that any information collected and provided by the User Organization is reasonably accurate and that the User Organization has taken reasonable steps to ensure the accuracy of such information;
>
> (c) The User Organization agrees that the Information in the PIP Application shall only be used for the purpose of providing health care services and that the User Organization will not use the application or information therein for any other purpose, unless authorized under *HIPA*; and
>
> (d) The User Organization agrees that a person or organization who knowingly collects, uses or discloses health or personal information in contravention of *HIPA* or other applicable law may be found guilty of an offence and be liable for a fine.
>
> ...

(3) User Organization Responsibilities

(a) The User Organization will be responsible to manage all users and user IDs within the User Organization. This will include:

(i) determining who within the User Organization is to access the Information and the appropriate level of access for each user; and

(ii) advising the Department as soon as possible of any employee who has been terminated or who may pose a security risk. It is important that the Department is advised as soon as possible so that appropriate steps may be taken to disable the employee's user ID.

(b) The User Organization will be responsible for the facilitation of any training recommended by the Department within the User Organization;

(c) The User Organization will be responsible to assist with the implementation within the User Organization of any security guidelines or user procedures associated with the PIP application provided to the User Organization in writing or by email from the Department. Please see the User Manual provided to the User Organization for the initial set of security guidelines and user procedures for the PIP application;

(d) The User Organization will be responsible to ensure appropriate safeguards are in place within the User Organization to protect the Information as required by HIPA;

(d) The User Organization will be responsible to advise the Department if the User Organization becomes aware of or reasonably suspects that there has been a security or confidentiality breach, or if a client or other individual has raised a privacy or security concern with respect to the PIP application; and …

[64] Before the User is given their account, the policy of Saskatchewan Health is that they must have completed the PIP training and confirm with the HISC Transition and Change Management Team that they have completed the training. In this case, B advises that he can recall attending a training session on HIPA. HISC advises that prior to the roll-out of PIP, there was a large training session held in Yorkton with pharmacists from the subject community attending. As Users signed up for PIP, they were told to complete the training and to call HISC to confirm that the training has been completed. Neither HISC nor Saskatchewan Health have a method of tracking if specific pharmacists actually took the training or not. That training, I am advised by HISC, also included training on consistent completion of the reason code when utilizing PIP. At this point, the User was granted access to PIP. If the User changed locations or became employed at another location, they had to contact the HISC Service Desk to request that the location be added. The Approver at that location was responsible for approving the request.

[65] HISC is moving from having all Users sign a *Data Access Agreement* before they get the right to utilize the PIP data to a new system that Users must accept and agree to be bound, without a signature requirement, by the terms of the *PIP Joint Service and Access Policy*.

[66] In the transition, L & M was subject both to the *Data Access Agreement* described above and the *PIP End User Licence Agreement* below:

[67] This document is headed by a large-size bold printed caution:

> **IMPORTANT – This application is for the use of authorized users only. Unauthorized access to this application is prohibited and may result in sanctions.**
>
> TERMS OF USE AND DISCLAIMER
>
> Please read these terms of use carefully before accessing or using this or any other Electronic Health Record (EHR) application.
>
> By accessing any EHR application you will agree to be legally bound and to abide by these terms.
>
> Restrictions on Collection, Use and Disclosure of Information in EHR applications
>
> 1. You agree that the information in and accessible through any Electronic Health Record (EHR) application (the "Information") is private and confidential and that you will take all reasonable steps to maintain the confidentiality of the Information. **You further agree that you are aware of and will comply with the provisions of *The Health Information Protection Act***, the *Personal Information Protection and Electronic Documents Act* or other relevant legislation, as applicable, with respect to the Information.
> 2. You specifically agree that **the information in any EHR application shall only be accessed and used for the purpose of providing health services or as otherwise authorized or required by law**.
> 3. You understand that a person who knowingly contravenes *The Health Information Protection Act* may be found guilt [sic] of an offence and liable to a fine or imprisonment.
>
> Disclaimer and Limitation of Liability
>
> 4. You understand that any EHR application, and the Information accessible through it, are provided by the Health Information Solutions Centre ("HISC") and Saskatchewan Health ("Health") on an "as is" and "as available" basis. Use of EHR applications and the Information is at your sole risk and is in no

> way intended to replace or be a substitute for your professional judgment. HISC and Health makes no representation or warranty, express or implied, as to the operation of any health application, and assume no legal liability or responsibility for the accuracy, completeness, or usefulness of any information provided through the application.
>
> Security Notice
>
> 5. You are aware that HISC monitors access to all EHR applications for security purposes and to protect the Information. By accessing EHR applications you are expressly consenting to these monitoring activities.
>
> [emphasis added]

[68] Notwithstanding clause 5 above, I have determined that HISC does regular monitoring to guard against breaches arising from external sources and has a capability to do monitoring or auditing of User practices but did so only in response to a complaint or concerns such as arose in this case.[14] Approvers also have the opportunity to audit User practices and, in some respects, this may be more useful since they will usually be much closer to the point of service and may be able to make better use of the audit capability. In this case, it appears that neither L & M's Approver nor Sunrise's Approver actually did any auditing of User PIP activity prior to the concerns raised by C.

[69] I am further advised that when the User first goes to the PIP "splash page" (https://pip.shin.sk.ca/) that appears on the computer screen as soon as the PIP system is accessed, there is information about the *PIP Joint Service and Access Policy* that does speak to privacy and security. The current User cannot view the personal health information of anyone through PIP unless and until that User clicks "accept" to the *PIP Joint Service and Access Policy.*

[70] In addition, on the left side of the splash page are various links, including a link to privacy information.

[14] Office of the Information and Privacy Commissioner for British Columbia, Investigation Report F10-02 available online at www.oipc.bc.ca.

[71] In my August 28, 2009 interview with A, I specifically asked him whether he was familiar with the foregoing eight documents. He advised that he had seen and was familiar with *Patient Confidentiality and the Release of Confidential Records*, the *Policy Statement: Pharmacists Accessing Patient-specific Information from the Medical Profile Viewer (MPV) Under the Pharmaceutical Information Program (PIP)*, and *Guidelines: Pharmacist Accessing Patient-specific Information from the Medical Profile Viewer (MPV) Under the Pharmaceutical Information Program (PIP)*. He stated he was not familiar with the document *Preparing your Community Pharmacy for HIPA and PIPEDA* but expects that he would have followed those guidelines when HIPA was introduced around 2004. He was unsure if he saw the *Sample Employee Privacy Pledge*. He could not recall seeing the *Privacy Policy.* Significantly, A could not recall seeing the *PIP End User Licence Agreement* that must be signed before a User could be enrolled in PIP. My view is that whether or not A specifically recalls reading each of these documents, he must be taken to have constructive knowledge of each of them. They are publications of his College, they are readily available on the College website and as a pharmacist he has a responsibility to make himself familiar with the policies, procedures that his regulatory College is mandated to create. He also did not recall reading the Saskatchewan Health brochure, *The Pharmaceutical Information Program*.

[72] After my initial interview with A, he advised that once L & M learned of this office's investigation L & M drafted a number of policies and he provided us with drafts of those documents. This office has provided input and advice with respect to those documents and a training program that has now apparently been implemented by L & M.

[73] The fact that A was able to view PIP from his home computer is another area of concern. For this information to be viewed remotely, there has to be equivalent protection as is required in the hospital or office. In other words, the trustee must ensure there are physical, administrative and technical safeguards at any remote location in order to meet its section 16 requirements.

[74] One would expect that quite apart from A's actions in respect of the nine viewing transactions with PIP in question in this investigation, he would have had responsibility as one of the Directors of L & M and as a senior pharmacist within L & M to model best HIPA practices and to ensure that he was providing leadership to the other pharmacists in the pharmacy in complying with the requirements of HIPA. The evidence is clear he failed to model best practices and he failed to provide appropriate leadership in HIPA compliance within L & M.

4. Did L & M Pharmacy Inc. discharge its "general duties" under *The Health Information Protection Act* aside from section 16?

[75] In my Investigation Report H-2005-002, I discussed the two kinds of duties imposed by HIPA on Saskatchewan trustees. One kind is the transaction-specific duties depending on whether the relevant activity is a "collection", or a "use" or a "disclosure". In addition, there are a number of "general duties" for any Saskatchewan trustee. These include sections 9 (prospective transparency to patients), 10 (retrospective transparency to patients), 16 (policies and procedures for HIPA compliance), 23 (data minimization and 'need-to-know').

[76] Those sections are as follows:

> **9**(1) An individual has the right to be informed about the anticipated uses and disclosures of the individual's personal health information.
>
> (2) When a trustee is collecting personal health information from the subject individual, the trustee must take reasonable steps to inform the individual of the anticipated use and disclosure of the information by the trustee.
>
> (3) A trustee must establish policies and procedures to promote knowledge and awareness of the rights extended to individuals by this Act, including the right to request access to their personal health information and to request amendment of that personal health information.
>
> **10**(1) A trustee must take reasonable steps to ensure that the trustee is able to inform an individual about any disclosures of that individual's personal health information made without the individual's consent after the coming into force of this section.
>
> (2) This section does not apply to the disclosure of personal health information for the purposes or in the circumstances set out in subsection 27(2).

> **23**(1) A trustee shall collect, use or disclose only the personal health information that is reasonably necessary for the purpose for which it is being collected, used or disclosed.
>
> (2) A trustee must establish policies and procedures to restrict access by the trustee's employees to an individual's personal health information that is not required by the employee to carry out the purpose for which the information was collected or to carry out a purpose authorized pursuant to this Act.
>
> (3) Repealed. 2003, c.25, s.13.
>
> (4) A trustee must, where practicable, use or disclose only de-identified personal health information if it will serve the purpose.

[77] With respect to those general duties, I offer the following comments:

[78] I have already found that at the material times, L & M did not have the required policies and procedures for HIPA compliance in accordance with the "general duty" in section 16 of HIPA.

[79] In this case, L & M could not point to any poster, brochures, web notices or any other material that would provide accessible information to patients as to the information practices of L & M.

[80] The facts of this case demonstrate no effort to inform the affected individuals that their information had been collected and disclosed without consent.

[81] There were no written policies and procedures to ensure compliance with HIPA by L & M employees. Although A asserted that he was familiar with HIPA, it became clear in the course of the investigation that he did not have an adequate understanding of HIPA requirements or even the basic elements of HIPA.

[82] The purpose for which the information of the former patients was accessed through PIP, and then viewed, was in no way necessary for the purpose for which the information of the patients was collected in the first place.

[83] In the result, the Trustee L & M failed to discharge its general duties under HIPA.

[84] Next it is appropriate to consider the transaction-specific statutory duties that HIPA imposed on L & M.

5. Was the action of L & M Pharmacy Inc. a "collection" or a "use" or a "disclosure" under *The Health Information Protection Act*?

[85] In HIPA, the term "use" is defined as including "reference to or manipulation of personal health information by the trustee that has custody or control of the information, but does not include disclosure to another person or trustee."[15] For purposes of HIPA, I have previously determined that "use" also means "the internal utilization of personal information by a public body and includes sharing of the personal information in such a way that it remains under the control of that public body."[16] I have not previously considered in a report whether viewing PIP information is a "use" or a "disclosure" for purposes of HIPA. Since PIP is primarily to accommodate viewing by trustees other than the pharmacy that is responsible for the prescription information it has uploaded to PIP it would not be a "use". A use relates to any sharing of personal health information within a single trustee organization such as a regional health authority or medical clinic. If personal health information is shared by one trustee with any other entity whether a trustee or non-trustee in such a way that it no longer has control over the shared information that would be a "disclosure".[17] I find that when a pharmacist utilizes the PIP database by viewing information on a screen whether or not it is copied or recorded, that is a "collection" within the meaning of HIPA.

[86] "Access" in a privacy context is understood to refer to the process whereby the patient or 'data-subject' is able to obtain a copy of or to view their personal health information. The transaction whereby a health care provider views a patient's personal health information would be either a "use" or a "disclosure" depending on whether the provider is employed by the particular trustee organization that has custody of the information or

[15] *Supra* note 2 section 2(u).
[16] Saskatchewan OIPC, *2008-2009 Annual Report* available at www.oipc.sk.ca p. 71
[17] A similar approach is evident in Alberta OIPC Investigation Report H2008-IR-001 available online at www.oipc.ab.ca at [56].

not. If a particular trustee organization has custody of patient information and an employee views or does something with that information, this is a "use" transaction. If the information is moving from one organization to another so that the second organization can view the information, this would be a "disclosure" of the information[18] unless there is some contractual arrangement that means the second has possession but only under the control of the first organization.

[87] Given that this is the first OIPC Report that addresses one of the domain repositories in Saskatchewan's emerging electronic health record (EHR), I have decided to consider the related transactions as well as the direct transactions raised in this investigation.

[88] Before dealing with those transactions however, it may be useful to offer some information about the EHR in Saskatchewan. The EHR is a lifetime record of the key health history and care within the health system for each person residing in Saskatchewan. This record is available or will be available electronically to authorized health providers, 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."[19] The EHR includes a number of Domain Repositories. PIP is one of those Domain Repositories. Each Domain Repository is a subset of clinical data about patients. Saskatchewan is also rolling out other Domain Repositories such as the diagnostic imaging system and the laboratory results system. Much of this work in Saskatchewan is funded by Canada Health Infoway. A good deal of information about the EHR is available at the website, www.infoway-inforoute.ca. The EHR Infostructure (EHRi) is a collection of common and reusable components in support of a diverse set of health information management applications. It consists of software solutions, data definitions and messaging standards for the EHR.

[18] The exception would be when personal information is shared with a second organization that by reason of contract or some other arrangement may not be free to do what it wishes with the information in which case the transaction would be considered still a 'use' since the information remains under the control of the first organization. An example might be sharing with an IMSP by contract remains accountable to the first organization for what is done with the personal information.

[19] Canada Health Infoway, *EHRS Blueprint – an interoperable EHR framework, Executive Overview*, April 2006, available online at www.infoway-inforoute.ca, p.5.

[89] Saskatchewan Health is the trustee responsible for PIP and the action of pharmacists uploading prescription data to the EHR is a disclosure by those pharmacists. Saskatchewan Health, in the same transaction, is collecting personal health information. When a pharmacist downloads or views PIP data, this is a disclosure of personal health information by Saskatchewan Health and a collection by the pharmacist or pharmacy.

[90] The relevant provisions for a collection under HIPA are found in sections 24 and 25 as follows:

> **24**(1) A trustee shall ensure that the primary purpose for collecting personal health information is for the purposes of a program, activity or service of the trustee that can reasonably be expected to benefit the subject individual.
>
> (2) A trustee may collect personal health information for a secondary purpose if the secondary purpose is consistent with any of the purposes for which personal health information may be disclosed pursuant to section 27, 28 or 29.
>
> (3) Nothing in this Act prohibits the collection of personal health information where that collection is authorized by another Act or by a regulation made pursuant to another Act.
>
> (4) A trustee may collect personal health information for any purpose with the consent of the subject individual.
>
> **25**(1) Subject to subsection (2), a trustee shall collect personal health information directly from the subject individual, except where:
>
> (a) the individual consents to collection of the information by other methods;
>
> (b) the individual is unable to provide the information;
>
> (c) the trustee believes, on reasonable grounds, that collection directly from the subject individual would prejudice the mental or physical health or the safety of the subject individual or another individual;
>
> (d) the information is collected, and is necessary, for the purpose of:
>
> (i) determining the eligibility of the individual to participate in a program of the trustee or receive a product or service from the trustee, in the course of processing an application made by or on behalf of the individual; or
>
> (ii) verifying the eligibility of the individual who is participating in a program of the trustee or receiving a product or service from the trustee;
>
> (e) the information is available to the public;

> (f) the trustee collects the information by disclosure from another trustee pursuant to section 27, 28 or 29; or
>
> (g) prescribed circumstances exist.
>
> (2) Where the collection is for the purpose of assembling the family health history of an individual, a trustee may collect personal health information from the individual about other members of the individual's family.
>
> (3) Where a trustee collects personal health information from anyone other than the subject individual, the trustee must take reasonable steps to verify the accuracy of the information.
>
> (3.1) Subsection (3) does not apply to personal health information collected by the Saskatchewan Archives Board for the purposes of *The Archives Act, 2004.*

[91] Since section 25(1)(f) incorporates by reference sections 27, 28 and 29, those provisions are as follows:

> **27**(1) A trustee shall not disclose personal health information in the custody or control of the trustee except with the consent of the subject individual or in accordance with this section, section 28 or section 29.
>
> (2) A subject individual is deemed to consent to the disclosure of personal health information:
>
> (a) for the purpose for which the information was collected by the trustee or for a purpose that is consistent with that purpose;
>
> (b) for the purpose of arranging, assessing the need for, providing, continuing, or supporting the provision of, a service requested or required by the subject individual; or
>
> (c) to the subject individual's next of kin or someone with whom the subject individual has a close personal relationship if:
>
> (i) the disclosure relates to health services currently being provided to the subject individual; and
>
> (ii) the subject individual has not expressed a contrary intention to a disclosure of that type.
>
> (3) A trustee shall not disclose personal health information on the basis of a consent pursuant to subsection (2) unless:

(a) in the case of a trustee other than a health professional, the trustee has established policies and procedures to restrict the disclosure of personal health information to those persons who require the information to carry out a purpose for which the information was collected or to carry out a purpose authorized pursuant to this Act; or

(b) in the case of a trustee who is a health professional, the trustee makes the disclosure in accordance with the ethical practices of the trustee's profession.

(4) A trustee may disclose personal health information in the custody or control of the trustee without the consent of the subject individual in the following cases:

(a) where the trustee believes, on reasonable grounds, that the disclosure will avoid or minimize a danger to the health or safety of any person;

(b) where, in the opinion of the trustee, disclosure is necessary for monitoring, preventing or revealing fraudulent, abusive or dangerous use of publicly funded health services;

(c) where the disclosure is being made to a trustee that is the successor of the trustee that has custody or control of the information, if the trustee makes a reasonable attempt to inform the subject individuals of the disclosure;

(d) to a person who, pursuant to *The Health Care Directives and Substitute Health Care Decision Makers Act*, is entitled to make a health care decision, as defined in that Act, on behalf of the subject individual, where the personal health information is required to make a health care decision with respect to that individual;

(e) if the subject individual is deceased:

(i) where the disclosure is being made to the personal representative of the subject individual for a purpose related to the administration of the subject individual's estate; or

(ii) where the information relates to circumstances surrounding the death of the subject individual or services recently received by the subject individual, and the disclosure:

(A) is made to a member of the subject individual's immediate family or to anyone else with whom the subject individual had a close personal relationship; and

(B) is made in accordance with established policies and procedures of the trustee, or where the trustee is a health professional, made in accordance with the ethical practices of that profession;

(f) where the disclosure is being made in accordance with section 22 to another trustee or an information management service provider that is a designated archive;

(g) where the disclosure is being made to a standards or quality of care committee established by one or more trustees to study or evaluate health services practice in a health services facility, health region or other health service area that is the responsibility of the trustee, if the committee:

(i) uses the information only for the purpose for which it was disclosed;

(ii) does not make a further disclosure of the information; and

(iii) takes reasonable steps to preserve the confidentiality of the information;

(h) subject to subsection (5), where the disclosure is being made to a health professional body or a prescribed professional body that requires the information for the purposes of carrying out its duties pursuant to an Act with respect to regulating the profession;

(i) where the disclosure is being made for the purpose of commencing or conducting a proceeding before a court or tribunal or for the purpose of complying with:

(i) an order or demand made or subpoena or warrant issued by a court, person or body that has the authority to compel the production of information; or

(ii) rules of court that relate to the production of information;

(j) subject to subsection (6), where the disclosure is being made for the provision of health or social services to the subject individual, if, in the opinion of the trustee, disclosure of the personal health information will clearly benefit the health or well-being of the subject individual, but only where it is not reasonably practicable to obtain consent;

(k) where the disclosure is being made for the purpose of:

(i) obtaining payment for the provision of services to the subject individual; or

(ii) planning, delivering, evaluating or monitoring a program of the trustee;

(l) where the disclosure is permitted pursuant to any Act or regulation;

(m) where the disclosure is being made to the trustee's legal counsel for the purpose of providing legal services to the trustee;

(n) in the case of a trustee who controls the operation of a pharmacy as defined in *The Pharmacy Act, 1996*, a physician, a dentist or the minister, where the disclosure is being made pursuant to a program to monitor the use of drugs that is authorized by a bylaw made pursuant to *The Medical Profession Act, 1981* and approved by the minister;

(o) in the case of a trustee who controls the operation of a pharmacy as defined in *The Pharmacy Act, 1996*, where the disclosure is being made pursuant to a program to monitor the use of drugs that is authorized by a bylaw made pursuant to *The Pharmacy Act, 1996* and approved by the minister;

(p) in prescribed circumstances.

(5) For the purposes of clause (4)(h), where the personal health information in question is about a member of the profession regulated by the health professional body or prescribed professional body, disclosure may be made only:

(a) in accordance with clause (4)(i);

(b) with the express consent of the subject individual; or

(c) if the trustee has reasonable grounds to believe that the personal health information is relevant to the ability of the subject individual to practise his or her profession, on the request of the health professional body or prescribed professional body.

(6) Disclosure of personal health information pursuant to clause (4)(j) may be made only where the person to whom the information is to be disclosed agrees:

(a) to use the information only for the purpose for which it is being disclosed; and

(b) not to make a further disclosure of the information in the course of carrying out any of the activities mentioned in that clause.

28(1) The minister may disclose registration information without the consent of the subject individual:

(a) to a trustee in connection with the provision of health services by the trustee;

(b) to another government institution, a regional health authority or an affiliate, for the purpose of verifying the eligibility of an individual to participate in a program of, or receive a service from, the government institution, regional health authority or affiliate:

(i) in the course of processing an application made by or on behalf of the individual; or

(ii) if the individual is already participating in the program or receiving the service;

(c) to another government institution, a regional health authority or an affiliate, for the purpose of verifying the accuracy of registration information held by the government institution, regional health authority or affiliate; or

(d) with the approval of the Lieutenant Governor in Council, to another government institution on any terms or conditions that the Lieutenant Governor in Council may determine.

(2) For the purposes set out in subsection (3), registration information may be disclosed without the consent of the subject individual:

(a) by the minister to a regional health authority or affiliate;

(b) by a regional health authority or affiliate to the minister; or

(c) by one regional health authority or affiliate to another regional health authority or affiliate.

(3) Registration information may be disclosed pursuant to subsection (2) for the purpose of planning, delivering, evaluating or monitoring a program of the minister, a regional health authority or an affiliate that relates to the provision of health services or payment for health services.

(4) The minister or a regional health authority may, without the consent of the subject individuals, disclose the names, dates of birth, telephone numbers and addresses of individuals under the age of seven years to a board of education or the Conseil scolaire fransaskois within the meaning of *The Education Act, 1995* for the purpose of planning or administration by the board of education or the Conseil scolaire fransaskois.

(5) With the approval of the Lieutenant Governor in Council, the minister may enter into agreements for the sharing of registration information with:

(a) the Government of Canada or the government of a province or territory of Canada; or

(b) a prescribed person or body.

(6) An agreement pursuant to subsection (5) must specify that the party to whom the registration information is disclosed shall use the information only for the purposes specified in the agreement.

(7) The minister may disclose registration information without the consent of the subject individual in accordance with an agreement entered into pursuant to subsection (5).

(8) Registration information may be disclosed without the consent of the subject individual in accordance with the regulations.

29(1) A trustee or a designated archive may use or disclose personal health information for research purposes with the express consent of the subject individual if:

(a) in the opinion of the trustee or designated archive, the research project is not contrary to the public interest;

(b) the research project has been approved by a research ethics committee approved by the minister; and

(c) the person who is to receive the personal health information enters into an agreement with the trustee or designated archive that contains provisions:

(i) providing that the person who is to receive the information must not disclose the information;

(ii) providing that the person who is to receive the information will ensure that the information will be used only for the purpose set out in the agreement;

(iii) providing that the person who is to receive the information will take reasonable steps to ensure the security and confidentiality of the information; and

(iv) specifying when the person who is to receive the information must do all or any of the following:

(A) return to the trustee or designated archive any original records or copies of records containing personal health information;

(B) destroy any copies of records containing personal health information received from the trustee or designated archive or any copies made by the researcher of records containing personal health information received from the trustee or designated archive.

(2) Where it is not reasonably practicable for the consent of the subject individual to be obtained, a trustee or designated archive may use or disclose personal health information for research purposes if:

(a) the research purposes cannot reasonably be accomplished using de-identified personal health information or other information;

(b) reasonable steps are taken to protect the privacy of the subject individual by removing all personal health information that is not required for the purposes of the research;

> (c) in the opinion of the research ethics committee, the potential benefits of the research project clearly outweigh the potential risk to the privacy of the subject individual; and
>
> (d) all of the requirements set out in clauses (1)(a) to (c) are met.

[92] I might also refer to section 30 of HIPA that provides as follows:

> **30**(1) No person who is aware, or should reasonably be aware, that he or she has received personal health information in contravention of this Act shall use or disclose the information without the consent of the subject individual or, where the subject individual is deceased, without the consent of a prescribed person.
>
> (2) Subsection (1) does not apply to personal health information disclosed by a trustee to a member of the subject individual's immediate family or to anyone else with whom the subject individual has a close personal relationship.

[93] On the evidence, A had discussions with two physicians in the Sunrise region about C and this included discussions that entailed the personal health information of C. At the time of these discussions, C no longer had a professional relationship with A. On the basis of my investigation, I conclude that A did not disclose personal health information of C that he obtained from the nine PIP viewing transactions in question but rather shared personal health information that can be attributed to their former personal relationship and acquired through the personal relationship. Nonetheless, the line between personal health information gleaned through the professional relationship and that acquired from other sources may not be clear. Surely the best practice for any health professional would be to avoid entering into this kind of gossip about the personal health information of a former patient unless this is a disclosure authorized by HIPA.

[94] I find that, in this case, anything said by A to the two physicians after January 5, 2009 was a disclosure and was not authorized by HIPA. That leads me to the next question in my analysis.

6. Were the requirements for a *Health Information Protection Act* collection satisfied by L & M Pharmacy Inc.?

[95] As noted earlier, when A undertook the nine PIP viewing transactions on behalf of L & M, L & M was collecting personal health information.

[96] Section 24(1) contains three key elements:

- The collection must be for a service of the trustee
- That service must be one that can reasonably be expected to benefit the patient
- The service to the patient must be the primary purpose for the collection activity

[97] On the facts of this case, the trustee L & M was not providing a professional service to C or to his family members at the time he undertook the nine viewing transactions a week after the professional relationship had been severed. Also, there was no consent from C in accordance with section 24(4). Furthermore, I have found that the reason for the collection was for personal reasons of A. On the basis of the evidence, I conclude that there would be no reasonable expectation of benefit to the patient. The actions of A, after his viewing transactions, are consistent with that finding. In any event, on August 28, 2009 A admitted that what he did was wrong.

7. Was there a further disclosure by L & M Pharmacy Inc. to other trustees?

[98] I might add that A indicated to me that he wanted to view the PIP patient profile for C after the severance of their professional and personal relationship on January 5, 2009 to look for certain prescription information and if that information was revealed, he intended to contact C's physician and alert that physician to the new PIP information about C. In our interview, A asserted that he would raise this with C's physician. He stated that his motive was to ensure that C was being properly cared for.

[99] I spoke with C's physician on January 26, 2010. He assured me that the discussion with A, subsequent to January 5, 2009, was principally in the nature of him providing support to a friend and colleague (A) who was grieving the loss of a relationship with C. No information was shared with the physician by A about prescriptions related to C.

Apparently, A shared some generalized concerns about C with the physician but this was information that would be known to A from his long term relationship with C and not from viewing C's drug profile on PIP. I therefore discount this reason proffered by A for his viewing or collection of the PIP profile on C and his family members.

[100] L & M has provided no submission that section 24(3) applies and I find that it does not apply.

[101] I must also consider if the collection by L & M could be justified by section 24(2) as a secondary purpose. I have carefully reviewed sections 27, 28 and 29 of HIPA. Those provisions that might possibly be relevant are section 27(3) and 27(4)(a), (l), (n), (o) or (p). There is no evidence that viewing the prescription information of a former patient via PIP would be a collection "in accordance with the ethical practices of the trustee's profession". Although A at one point offered an explanation for his nine viewing transactions that related to concern for the health of C and his family members, I find that there was no reasonable basis for him to conclude that his viewing of this prescription data on PIP could be justified under section 27(4)(a) of HIPA. I further find that this amounted to a kind of rationalization after the fact by A. Section 27(4)(a) is therefore of no help to L & M and A. I am unaware of any Act or regulation that permits collection of this personal health information by pharmacists about former patients for their own personal reasons and therefore find that section 27(4)(l) has no application. A has not suggested any way that sections 27(4)(n) or (o) would apply in this case. Finally, I have not found any prescribed circumstances in accordance with section 27(4)(p) that would legitimize the collection. There is no evidence to support the application of sections 28 or 29 of HIPA.

8. Did the Sunrise Regional Health Authority have the policies and procedures required by section 16 of *The Health Information Protection Act*?

[102] In my analysis I have determined that the nine PIP viewing transactions in question most likely occurred from a facility and using equipment independent of Sunrise. I have also determined that Sunrise acted promptly and appropriately in initiating an immediate

investigation and suspending A's privileges to access PIP from Sunrise facilities and utilizing Sunrise computers.

[103] Nonetheless, up until those determinations were made, this office considered Sunrise's possible role in terms of HIPA compliance. Sunrise has a designated Privacy Officer and has done a good deal of work in order to implement HIPA compliance policies and procedures. It does have written policies and procedures for general HIPA compliance by its employees and contractors. This includes the following:

a. A section on the Sunrise website dedicated to Privacy[20]

b. Regional policies pertaining to use and disclosure of personal health information including:

- *Collection, Use and Disclosure of Personal Health Information to Support the Provision of Care* – Approved July 1, 2006.
- 24 additional Sunrise approved policies pertaining to personal health information

c. Communication pieces including:

- *HIPA – A Guide for Staff* brochure circulated with pay slips in February 2006.
- *Did You Know* confidentiality awareness campaign – sent to all employees on July 4, 2008

d. Education initiatives including:

- On-site presentation at the hospital in question in Sunrise region explaining basic concepts of HIPA, Presented by a lawyer – March 23, 2006
- Further education presentation in the subject community on October 24, 2007
- Over 80 HIPA presentations between 2003-2009 conducted at every Sunrise facility. HIPA education sessions are open to all staff

e. Sunrise Intranet including:

- Privacy Information
  - What's New – Latest OIPC Newsletter
  - Education – Powerpoint, video resources and upcoming on-site presentations
  - Questions – Frequently Asked Questions and Answers related to HIPA
  - Documents – HIPA brochures and posters
  - Forms – Fax cover sheet
  - Related Policies – I

[20] Sunrise Regional Health Authority, www.sunrisehealthregion.sk.ca/default.aspx?page=66

    - Region Privacy Officers – contact information for Region Privacy Officers
    - Links – to website for OIPC and HIPA
- PIP Training (Links to SK Health Resources)
    - PIP background
    - Registering for the PIP System
    - The PIP System (training and usage)
- Privacy Surveys
    - SHR Privacy Survey circulated to all staff to ensure understanding of obligations under HIPA.
- Network Account Application
    - Application includes confidentiality agreement to those employees accessing electronic systems which contain personal health information

[104] This case highlights however four areas of concern arising from the material and information supplied by Sunrise:

[105] The *Contract for Supply of Pharmacy Services* antedates the proclamation of HIPA. Earlier in this Report I quoted clause 6 of that Contract. The OIPC has described the responsibilities of a trustee that contracts out any services involving personal health information in its brochure: *A Contractor's Guide to Access and Privacy in Saskatchewan*.[21] Since September 1, 2003, Saskatchewan trustees have needed to revise and update existing contracts and ensure that all new contracts incorporate by reference all of the obligations of any trustee to collect, use and disclose personal health information only in accordance with HIPA. The confidentiality clause in the Contract is inadequate. The 'privacy rights' that are codified in HIPA are much broader than simply a requirement to keep patient information confidential. 'Confidentiality' is a much narrower concept than privacy since it is focused solely on the patient's information rather than the patient. Privacy on the other hand is the patient's right to a measure of control of his or her own personal health information. Confidentiality is an element subsumed in the scope or definition of privacy.

[106] It was Sunrise's responsibility to determine which Users would be approved as 'users' on behalf of and under the auspices of Sunrise for purposes of PIP. In this case, there was no attempt by Sunrise to independently assess whether or not A had the requisite training

[21] Saskatchewan OIPC, *A Contractor's Guide to Access and Privacy in Saskatchewan* available online at www.oipc.sk.ca.

and familiarly with HIPA before approving him as a 'User' for purposes of PIP. Sunrise's Approver advised that she relied on A's professional certification in approving him as a User. On its face, this does not seem like an unreasonable assumption, particularly given the various tools and materials the College has produced for its members and which have been discussed earlier in this Report. As well, the College had provided some training sessions which were attended by a number of pharmacists in the Sunrise region although we could find no confirmation that A actually attended any of these sessions. Now that we know that A had a very weak understanding of HIPA fundamentals and was all too ready to ignore the various safeguards created to minimize this risk of abuse, we can see that such an assumption can be dangerous. I have noted earlier in this Report the manner in which the College concluded its considerations of A's actions under its particular legislation. From a patient perspective, further and better screening of prospective PIP Users as well as more vigilant monitoring is warranted. This monitoring needs to happen at the level of the region as well as the monitoring done by HISC. In addition, I recommend that the consequences of breaching HIPA, and the User Agreements should entail an array of penalties to include a forfeiture of 'User' privileges or at least a suspension for a significant period of time. Since I am also concerned about prejudice to the health services for patients, perhaps a reasonable compromise in the unique circumstances of this case is to require that A's use of PIP be audited on a regular monthly basis for a one year period.

[107] Even though PIP asks the User to identify a reason code for their intended viewing of a patient medication profile, as noted earlier this is described as an option and the pharmacist discussed in this report simply relied on the default mode and consistently failed to complete the reason code field. I recognize that even if the User was required to enter a reason code before they could proceed to view any patient's medication profile, there is no certainty that the breaches described in this Report would not have occurred. It may however have discouraged A from his wrongful actions and it would certainly have simplified the audit undertaken after the concerns were raised by C. I encourage Saskatchewan Health and its HISC office to consider developing a technical solution that

would make completion of the reason code a compulsory element for any User.[22] This would mean that a pharmacist or any prospective User could not proceed to view any patient profile unless and until that User indicates whether the purpose is for consultation, or prescribing or dispensing. If there is another reason then the User should be required to adequately describe that purpose before they are permitted to proceed into the PIP database. I suspect that this may have originally been deemed unnecessary given other safeguards described elsewhere in this Report but this case demonstrates how relatively easy it was for a pharmacist to either ignore or circumvent all of those safeguards. Until such a technical solution can be implemented, there should be a mandatory requirement that the User of PIP must complete the reason code each time they enter the database and this requirement be communicated to all Users.

[108] Despite a prodigious amount of HIPA education material produced by Sunrise and a comprehensive set of tools and documentation to ensure HIPA compliance and an ambitious education campaign, I discovered in this investigation that at least one senior employee of its PIP contractor, L & M, demonstrated a remarkable lack of awareness of HIPA requirements. It appears that it will be necessary for Saskatchewan Health, health regions and the College to take steps in the future to actually record attendance at education sessions and/or require some form of certification that its trustee contractors such as L & M have an adequate detailed understanding of HIPA requirements.

9. Did the Ministry of Health have appropriate policy and procedures as required by section 16 of *The Health Information Protection Act*?

[109] In my Investigation Report H-2005-002 I considered Saskatchewan Health's compliance with its general duties under HIPA. That discussion can be referenced by means of the *Annotated Section Index for HIPA* that is available on my office's website, www.oipc.sk.ca. In this Report I choose to consider two aspects of Health's policies and procedures under section 16 of HIPA.

[22] A similar recommendation was made by the acting British Columbia Information and Privacy Commissioner in his Investigation Report F10-02 [85] to [87].

[110] One aspect is the accreditation process employed by designated Approvers. Although for purposes of PIP, each trustee organization is required to designate an Approver, since Saskatchewan Health is the trustee responsible for the PIP database, it has the responsibility for ensuring that each organization's Approver applies adequate rigour in considering the suitability of each prospective User. This investigation exposes the frailty of an accreditation system that appears to rely solely on the professional status of the prospective User. In other words, it appears that at both L & M and at Sunrise, A was accredited as a User solely on the basis that he was a licensed pharmacist. In this case, while he was certainly a licensed pharmacist he was not in any sense prepared to discharge the serious responsibilities of a PIP User under HIPA. There was an obvious lack of training, no signed undertaking to protect personal health information, no familiarity with HIPA policies and practices of Sunrise in the one respect and no policies or procedures for HIPA compliance in respect of L & M. More rigour in the accreditation process would have entailed at the very least a requirement that the prospective User provide a copy of his signed undertaking, proof of HIPA and PIP training, and production of the prospective User's policies and procedures for section 16 compliance in his or her own professional practice. I urge Saskatchewan Health to ensure that designated Approvers for purposes of PIP require the above described documentation before handing the 'key' to the PIP database to any new User.

[111] In the course of our investigation, I discovered an odd feature of PIP. Although A had been approved in two different respects, one as an authorized User for L & M's pharmacy and the other as an authorized User for the pharmacy office in the hospital, there was only one User name and one password involved. That means that the 'suspension' by Sunrise would have been unenforceable and ineffectual since it did not prevent A from entering the system by indicating that he was entering from the other location. One might reasonably expect that a User approved for more than one occasion would have different passwords and perhaps even User names. That would facilitate auditing of the User's separate viewing activity at each location and would mean if his accreditation as a User was suspended or terminated at one location, he could not readily circumvent that suspension by simply entering his User name and password at the other location and then gain access to all of PIP.

[112] Given the weaknesses in PIP exposed by this investigation, I recommend that Saskatchewan Health take immediate remedial action that would involve both a technical solution and revised policy.

IV. ACKNOWLEDGEMENT

[113] I want to specifically thank a number of individuals who played key roles in this investigation. Since this was our first formal consideration of the EHR or at least a component of the EHR, I relied on the advice and assistance of front-line workers with detailed working knowledge of the PIP system. This includes Lorelei Stusek, the Sunrise Privacy Officer, her colleague Tim Kasparick, Privacy Consultant to Sunrise, and Christine Underwood, the Manager of the IT/IM Privacy/Data Access Unit at HISC. These individuals responded promptly and appropriately to the initial concern about a possible HIPA breach and then provided our office with full cooperation in the course of our investigation. I also acknowledge that the principals of L & M were forthcoming and cooperative with our office throughout this investigation.

V. FINDINGS

[114] That as between A and L & M Pharmacy Inc., L & M Pharmacy Inc. is the responsible Trustee under *The Health Information Protection Act*.

[115] That the Ministry of Health is the Trustee responsible for the Pharmaceutical Information Program database.

[116] That the information viewed by A in the Pharmaceutical Information Program is personal health information pursuant to section 2(m) of *The Health Information Protection Act*.

[117] That when a registered User views the Pharmaceutical Information Program database to obtain the prescription information of an individual this constitutes a “collection” under *The Health Information Protection Act*.

[118] That L & M Pharmacy Inc. failed to develop policy and procedures as required by section 16 of *The Health Information Protection Act*.

[119] That L & M Pharmacy Inc. failed to train its staff in the requirements of *The Health Information Protection Act*.

[120] That L & M Pharmacy Inc. did not discharge its general duties aside from section 16 of *The Health Information Protection Act* such as transparency to patients as required under sections 9 and 10 and violated the 'need-to-know' rule incorporated into section 23.

[121] That, in this case, the requirements for a *Health Information Protection Act* collection were not satisfied by L & M Pharmacy Inc.

[122] That neither L & M Pharmacy Inc. nor Sunrise Regional Health Authority carried on random audits of Pharmaceutical Information Program Users accredited by those two organizations.

VI. RECOMMENDATIONS

[123] That L & M Pharmacy Inc. prepare a comprehensive set of written policies and procedures for *The Health Information Protection Act* compliance within 60 days and provides this office with a copy.

[124] That L & M Pharmacy Inc. ensure that any Pharmaceutical Information Program registered User in its employment completes the reason code each time he or she enters the Pharmaceutical Information Program.

[125] That L & M Pharmacy Inc. arrange for detailed training of pharmacists and other support staff in its employ with respect to *The Health Information Protection Act* with particular emphasis on general duties of a trustee including the data minimization principle and the 'need-to-know' principle.

[126] That L & M Pharmacy Inc. ensure that there is prompt written notification to any patient in the event that any employee of L & M Pharmacy Inc. views Pharmaceutical Information Program information about that patient for any purpose other than diagnosis, treatment or care of that individual.

[127] That L & M Pharmacy Inc. immediately ensure that all staff members download and sign the Privacy Pledge available on the Saskatchewan College of Pharmacists website.

[128] That L & M Pharmacy Inc. ensure that any employee, including pharmacists of L & M Pharmacy Inc. properly identifies the location from which entry is sought to the PIP database.

[129] That L & M Pharmacy Inc. ensure that A's use of the Pharmaceutical Information Program is suspended until it has implemented the appropriate policies and procedures described in paragraph [123].

[130] That once A's use has been restored, the Health Information Solutions Centre audit A's use of the Pharmaceutical Information Program on a monthly basis for a one year period and immediately report to the College of Pharmacists any suspicious or irregular patterns of use.

[131] That the Ministry of Health and its Health Information Solutions Centre undertake on a sustained basis random audits of activity by pharmacists in their use of Pharmaceutical Information Program and this pro-active audit policy be brought to the attention of all Saskatchewan pharmacists.

[132] That the Ministry of Health and its Health Information Solutions Centre effect a technical change to Pharmaceutical Information Program so that any User must enter a reason code before they can view the personal health information of anyone.

[133] That the Ministry of Health and its Health Information Solutions Centre take steps to ensure that when a User has two or more ways to view Pharmaceutical Information Program patient profiles the User is identified separately to allow proper tracking of that User's Pharmaceutical Information Program viewing activity.

[134] That the Ministry of Health and its Health Information Solutions Centre develop a policy to revoke or suspend User access temporarily or permanently for a registered User that views personal health information for personal reasons or for any other reason contrary to *The Health Information Protection Act*.

[135] That the College of Pharmacists ensure that *The Health Information Protection Act* training is mandatory for every licensed pharmacist and every licensed pharmacy in the province and that it develop a system to confirm when every pharmacist completes that training.

[136] That the College of Pharmacists ensure that the training described in paragraph [135] is renewed at least every three years and that it develop a system to confirm when every pharmacist completes that additional training.

[137] That the training and training materials produced by the College of Pharmacists incorporate a specific focus on the twin problems of curiosity and carelessness.

[138] That the Sunrise Regional Health Authority should ensure that its contracts with pharmacists and other health professionals explicitly refer to *The Health Information Protection Act* and the need to meet the general duties and the transaction-specific duties defined in *The Health Information Protection Act*.

[139] That the Sunrise Regional Health Authority should ensure that it requires all of its Pharmaceutical Information Program registered Users, including contractors that may be registered Pharmaceutical Information Program Users, to complete the reason code before collecting any personal health information from Pharmaceutical Information Program.

[140] That all trustee organizations ensure they have a policy and procedures to address Pharmaceutical Information Program viewing by employees from off-site home or personal computers such that there are adequate security measures to protect personal health information.

[141] That the Ministry of Health revise its policies so that any designated Approver for purposes of Pharmaceutical Information Program must require documentation from any prospective User that establishes that the prospective User has signed a suitable written privacy pledge, has provided satisfactory proof of *The Health Information Protection Act* training completed and of adequate *Health Information Protection Act* policy and practices in his or her own practice.

[142] That Sunrise Regional Health Authority's designated Approver for purposes of Pharmaceutical Information Program must require documentation from any prospective User that establishes that the prospective User has signed a suitable written privacy pledge and has provided satisfactory proof of *Health Information Protection Act* training completed.

[143] That the Ministry of Saskatchewan Health develop a technical solution that means if a User is entitled to enter the Pharmaceutical Information Program database from more than one trustee's system that there be a separate User name and separate password for each system.

Dated at Regina, in the Province of Saskatchewan, this 23rd day of March, 2010.

R. GARY DICKSON, Q.C.
Saskatchewan Information and Privacy Commissioner

POSTSCRIPT

Since this is the first Report issued by my office dealing with a component of the developing electronic health record (EHR), I wanted to offer some general observations about this experience. This investigation highlights a significant weakness with the EHR that is being constructed in this province. 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 illuminated in this investigation – the risks posed by the carelessness of trustee organizations and the curiosity of their employees and contractors.

There is evidence that reinforces the proposition that the biggest threat to data security is likely to be the employees of a trustee. This investigation demonstrates how relatively easy it can be for a health professional to slip past or ignore the 'safeguards' currently in place. How do we protect against a health professional that ignores the general duties and the transaction-specific duties in *The Health Information Protection Act* (HIPA) and also ignores the warnings that appear on his computer screen when he enters PIP? In this case, neither the offence provision and severe penalties in HIPA nor the College of Pharmacists' disciplinary power proved to be a meaningful deterrent. It is clear to me that a good deal more attention needs to be paid to the carelessness of trustee organizations and the curiosity of health workers who know how to obtain the personal health information of patients without the patients' consent.

I'd suggest that this means a review of how Saskatchewan trains, approves and monitors health care workers and their use of the personal health information. This will be an ongoing challenge for not only Saskatchewan Health, regional health authorities and the regulatory colleges but also for each separate trustee organization. There is also a compelling need for not just audit capability but for a rigorous, ongoing audit program by the Health Information Solutions Centre (HISC). This must include the need to suspend and, when warranted, to terminate the viewing privileges of a User who abuses their accreditation. How can we expect HIPA rules to be consistently followed if there are no significant consequences to the curious health care worker for a breach?

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 records which may be accessible by many more individuals than was ever the case with paper records.

The development of an EHR requires a complex balancing of a number of competing goals or values. Obviously the success of any iEHR initiative will require the cooperation and full participation by Saskatchewan health care professionals. There are many examples of features of the iEHR plan in Saskatchewan designed to address the convenience of those professionals. It is also true that while privacy of Saskatchewan residents is important it is not an absolute right and from time to time may be limited to accommodate certain legal requirements, safety requirements and public policy imperatives. The challenge is to find a way of balancing those values which may from time to time be in conflict. In my view, the evident preoccupation with making the iEHR simpler for health care professionals – the providers - has to a large degree eclipsed the need to make our iEHR sufficiently respectful of the expectations and rights of the patient. This preoccupation with accommodating the preferences as well as the needs of providers perhaps accounts for some of the vulnerabilities exposed in this investigation. Fortunately, our iEHR is still a work in progress. There is still the opportunity to recalibrate – to implement stronger controls and safeguards to better protect the interests of the patient. I think such action is consistent with the thrust and recommendations of Commissioner Dagnone in his *Patient First Review Report* and specifically the following observation:

> Fundamental to achieving patient- and family-centred care is patient-centred governance and policy-setting, beginning with the Ministry of Health and supported by unified, prudently managed, high-performing health care administration that enables, empowers and expects everyone to put the patient first.[23]

Finally, this investigation highlights the practical challenges in dealing with HIPA breaches that involve EHRs. In this case, there was some form of investigation undertaken by not just our office but also by Saskatchewan Health's HISC office, the College of Pharmacists and the regional health authority. Each of these investigations proceeded under different statutory authority and took different approaches. Even with excellent cooperation from all parties, our investigation becomes more complicated and longer. It will be essential for protocols to be developed jointly with all of these organizations to streamline the response to any future alleged EHR breach.

[23] Saskatchewan Health, *For Patient's Sake: Patient First Review Commissioner's Report to the Saskatchewan Ministry of Health* available online at www.health.gov.sk.ca/patient-first-review p. 12.