SASKATCHEWAN

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

INVESTIGATION REPORT H-2013-001

Regina Qu'Appelle Regional Health Authority

Summary: The Commissioner was notified of three separate but similar cases where employees of the Regina Qu'Appelle Regional Health Authority (RQRHA) used their employee user privileges to electronic information systems to view and/or modify personal health information without proper authority. The Commissioner undertook investigations into each incident. He determined that the administrative safeguards that RQRHA had in place were inadequate, including the reliance on the non-statutory concept of 'circle of care' in RQRHA's policies, procedures, and privacy training materials. He made a number of recommendations including replacing the problematic circle of care in all printed materials with the need-to-know rule.

Statutes Cited: *The Health Information Protection Act*, S.S. 1999, c. H-0.021, ss. 2(b), 2(m), 2(t)(ii), 2(u), 16, 23, 26, 27(3), 42(1)(c), 52(b), 52(c), 52(d), 52(e); Alberta's *Health Information Act*, R.S.S. 2000, c. H-5.

Authorities Cited: Saskatchewan OIPC Review Reports: H-2006-001, LA-2009-002/H-2009-001; Saskatchewan OIPC Investigation Reports: H-2011-001, F-2009-001, H-2005-002, H-2010-001; *Timmins & District Hospital v. Ontario Nurses' Association (Peever Grievance)* [2011] O.L.A.A. No. 222; *North Bay Health Centre v. Ontario Nurses' Association (McLellan Grievance)* [2012] O.L.A.A. No.11; *British Columbia Nurses' Union and Vancouver Hospital and Health Sciences Centre (Pattison Grievance)* [1997] B.C.C.A.A.A. No. 97.

Other Sources Cited: Saskatchewan OIPC *Glossary of Common Terms: The Health Information Protection Act (HIPA)*; Saskatchewan OIPC *Helpful Tips: Privacy Breach* Guidelines; Saskatchewan OIPC Annual Reports: *2009-2010*, *2010-2011* and *2011-2012*, Saskatchewan OIPC *FOIP FOLIO* Newsletter (February 2004); Regina Qu'Appelle Health Region *2009-2010 Annual Report;* Regina Qu'Appelle Regional Health Authority Policies and Procedures: *Privacy Violations – Recommended Actions for Employees Draft Jan '11*, *Personal Health Information Protection*, 501, October 20, 2005, *Personal Health Information Protection*, 501-1, October 20, 2005, *Confidentiality*, 1.1.5, June 6, 2000, *Confidentiality and Security Agreement*, 1.1.5, June 6, 2000, *Confidentiality – Teaching Purposes*, 1.1.5.02, June 6, 2000, *Confidentiality- Volunteer/Student*, 1.1.5.03, June 6, 2000, *Regina Health District Information System Security*, 5.4.03, March 17, 1994, *Use and Disclosure of Personal Health Information within the Circle of Care*, 505, October 20, 2005, *Use and Disclosure of Personal Health Information within the Circle of Care*, 505-1, *Use and Disclosure of Personal Health Information outside the Circle of Care*, 506, October 20, 2005, *Use and Disclosure of Personal Health Information outside the Circle of Care*, 506-1, *LABLisOP8000.4 SoftSecurity User Management*, Revision 1.4, March 28, 2012, *Information Technology Acceptable Use Procedure*, DRAFT 400.0.1.1 V 4.0; Regina Qu'Appelle Regional Health Authority Pamphlets: *Protecting Clients' Privacy*, RQHR 1030, November 23, 2011, *Your Privacy Rights in the Regina Qu'Appelle Health Region,* CEAC 0706, November 2011; Regina Qu'Appelle Regional Health Authority PowerPoint presentation, *HIPA, Health Information Protection Act*; Regina Qu'Appelle Regional Health Authority Training DVD, *The Health Information Protection Act (HIPA),* September 22, 2010; Ontario IPC, *A Policy is Not Enough: It Must be Reflected in Concrete Practices*, September 2012; International Organization for Standardization, ISO Standard, *Information Technology – Security Techniques – Code of practice for information security management, International Standard* ISO/IEC 17799, (2005).

Table of Contents

I BACKGROUND

[1] This Report deals with three separate cases where employees of Regina Qu'Appelle Regional Health Authority (RQRHA)[1] viewed and/or modified personal health information on electronic information systems without authority.

[2] The first case occurred in January 2008 when employees at the Regina General Hospital, a facility within RQRHA, in the Health Information Management Services department (HIMS) learned that one of their co-workers was receiving health care within RQRHA.

[3] One of the employees (Employee A) logged onto an electronic information system called Enovation that contains personal health information of RQRHA patients. She, along with her co-workers looking over her shoulder, viewed her patient/co-worker's personal health information. To our knowledge, none of the staff present objected to the viewing of the patient/co-worker's personal health information.

[4] Later, Employee A contacted the patient/co-worker to whom the personal health information belonged and apologized for viewing the personal health information. Approximately one month later, the patient/co-worker notified RQRHA and advised it of the identity of the individual who viewed her personal health information.

[5] Employee A was terminated but was re-instated after arbitration. The other implicated employees were suspended or received written/verbal reprimands.

[6] The second case was discovered in June 2009 when a Medical Laboratory Assistant (MLA) in RQRHA's Laboratory (lab) department attempted to view her own personal health information on another electronic information system called the Laboratory Information System (LIS) by querying her last name. That attempt was unsuccessful.

[1] *The Regional Health Services Act* establishes the Regina Qu'Appelle Regional Health Authority (RQRHA) as the governing body of the Regina Qu'Appelle Health Region (RQHR). *Regina Qu'Appelle Health Region 2009-2010 Annual Report* at p. 9, available at www.health.gov.sk.ca/regina-quappelle-annual-report-2009-10.

Then, she queried her Medical Record Number (MRN). That attempt was successful in enabling her to view her own personal health information.

[7] She discovered that her name, sex, and infectious disease information in LIS had been changed. Her name was replaced with vulgarities and the acronym "RIP" appeared in her file.

[8] RQRHA began its own investigation into the matter. It discovered that between April 20, 2009 and June 4, 2009, the MLA's personal health information was changed eight times under seven user identifications. RQRHA determined that on one occasion it was the MLA who changed her own personal health information under her own user identification.

[9] RQRHA then determined it was likely that it was the same individual who viewed the MLA's file seven times under six other user identifications. RQRHA was able to identify one employee (Employee B) who was working at the time of all the changes. It appeared that employees in the lab relied on the 'time out' function on the computers as a method of logging off the computer instead of manually logging off. Employee B would therefore use other employees' user identification and changed the MLA's personal health information after the other employees walked away from the computer.

[10] RQRHA provided our office with its internal investigation report dated November 9, 2009,[2] which included details of the privacy breach. The internal investigation report included six conclusions and ten recommendations as to how RQRHA could prevent similar events in the future.

[11] In spite of the ten recommendations, RQRHA received a privacy complaint about a third case on November 24, 2010 about a very similar privacy breach. The Complainant alleged an employee (Employee C) had viewed her (the Complainant's) personal health information on LIS and disclosed the personal health information to a third party without authority. RQRHA investigated the matter and determined that Employee C indeed

[2]Regina Qu'Appelle Regional Health Authority (RQRHA) Incident Review Report dated November 9, 2009.

viewed the Complainant's and others' personal health information. RQRHA stated that the breaches "appear to be intentional, malicious and for personal gain."[3]

[12] It appears that RQRHA never implemented all the recommendations referred to in [10].

[13] An internal investigation report dated February 11, 2011 by RQRHA[4] was provided to my office. RQRHA determined that Employee C had viewed the Complainant's personal health information on LIS on multiple occasions. Further, it identified "suspicious" behavior by the employee for viewing the personal health information of eight individuals without a legitimate need-to-know to fulfill her job duties, including her own, and personal health information belonging to the Complainant, the Complainant's husband, four of her (Employee C's) family members, and one other individual of whom RQRHA was not able to determine a connection to Employee C or to the Complainant.

[14] Also, RQRHA found a connection between the Complainant and Employee C. The Complainant's husband is the father of Employee C's child. RQRHA stated that the Complainant, the Complainant's husband and Employee C were involved in child custody issues.

[15] A complicating factor was that the Complainant, the Complainant's husband, and Employee C's family members were not cooperative during RQRHA's investigation and were unwilling to provide information.

[16] RQRHA was not able to determine if Employee C disclosed any of the Complainant's personal health information to any third party.

[17] Employee C was interviewed by RQRHA on January 19, 2011. She stated that "boredom" and "curiosity" were the reasons for her accessing the personal health information. She thought that viewing personal health information without a need-to-

[3]RQRHA letter dated January 13, 2011 to Saskatchewan Information and Privacy Commissioner (hereinafter SK OIPC).
[4]RQRHA, *Incident Review Report* dated February 11, 2011.

know was permitted as long as she did not disclose the personal health information. Further, RQRHA reported in its internal investigation report dated February 11, 2011 that Employee C said that "everybody does it". RQRHA took that to mean that perhaps "there may be a culture of normalized deviance in the Lab Office related to the accessing of [personal health information]".[5]

[18] RQRHA stated that Employee C had signed three separate confidentiality agreements and she had attended privacy and security trainings on "numerous" occasions, including when she was transferred to the lab in May 2005 and then a *The Health Information Protection Act* (HIPA)[6] training session tailored to lab staff in January 2010.

[19] RQRHA included in its internal investigation report dated February 11, 2011 findings and twelve new recommendations on how to prevent similar events in the future. However, many of the recommendations were not acted upon.[7]

[20] It is important to acknowledge that RQRHA proactively reported the three cases described above to my office. I applaud it in doing so.

[21] I encourage the proactive reporting of privacy breaches so that public bodies and trustees, such as RQRHA, can take advice and be better prepared to respond to questions from the public, the media and Members of the Legislative Assembly. Generally speaking, my office will not open a formal investigation file when a privacy breach has been self-reported. Instead, we will monitor the situation and ensure that the response of the trustee is adequate. It is when the public body or trustee's response is untimely or inadequate that my office may undertake a formal investigation.[8]

[22] The first of the two cases involving LIS was reported to my office in November of 2009. RQRHA provided my office with its internal investigation report including

[5] *Ibid.*
[6] *The Health Information Protection Act*, S.S. 1999, c. H-0.021 (hereinafter HIPA).
[7] Based on enclosure that was sent with RQHR letter dated November 3, 2011 to the OIPC.
[8] SK OIPC *Helpful Tips: Privacy Breach Guidelines* at p. 5, available at www.oipc.sk.ca/Resources/Helpful%20Tips%20-%20Privacy%20Breach%20Guidelines%20-%20September%202010.pdf

recommendations to prevent future privacy breaches. My office did not immediately open a formal investigation file since we assumed the recommendations would be adequately implemented in a timely way.

[23] However, yet a third privacy breach involving electronic information systems was reported to our office in January 2011. Due to the similarities in the two privacy breaches involving LIS coupled with the privacy breach involving the Enovation system, it appeared to my office that perhaps the unauthorized viewing of personal health information involving electronic information systems at RQRHA was becoming a chronic issue. Therefore, our office commenced a formal investigation.

[24] Had RQRHA fully implemented its own recommendations resulting from its internal investigation report dated November 9, 2009, there may not have been a need for my office's formal investigation.

II AUTHORITY TO INVESTIGATE

[25] The authority for my office to investigate the above three privacy breaches is found in sections 42(1)(c) and 52(b), (c), (d), and (e) of HIPA:

> **42**(1) A person may apply to the commissioner for a review of the matter where:
>
> ...
>
> (c) the person believes that there has been a contravention of this Act.
>
> …
>
> **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;

(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.[9]

III ISSUES

1. Was the viewing of the personal health information a "collection", "use", or "disclosure"?

2. Were the requirements for a "use" of personal health information under *The Health Information Protection Act* satisfied by Regina Qu'Appelle Regional Health Authority?

3. Is Regina Qu'Appelle Regional Health Authority in compliance with sections 16 and 23 of *The Health Information Protection Act*?

a. What administrative safeguards does Regina Qu'Appelle Regional Health Authority have to protect personal health information and are they adequate?

b. What physical safeguards does Regina Qu'Appelle Regional Health Authority have to protect personal health information and are they adequate?

c. What technical safeguards does Regina Qu'Appelle Regional Health Authority have to protect personal health information and are they adequate?

[9] *Supra* note 6.

IV DISCUSSION OF ISSUES

[26] I have said in previous Reports that HIPA is engaged when three elements exist: 1) there must be a trustee within the meaning of section 2(t); 2) there must be personal health information within the meaning of section 2(m); and 3) the personal health information must be in the custody or control of the trustee.[10]

[27] Section 2(t)(ii) of HIPA provides as follows:

> **2** In this Act:
>
> ...
>
> (t) "trustee" means any of the following that have custody or control of personal health information:
>
> ...
>
> (ii) a regional health authority or a health care organization;[11]

[28] RQRHA is a regional health authority. Therefore, it qualifies as a trustee.[12]

[29] Section 2(m) of HIPA defines "personal health information" as follows:

> **2** In this Act:
>
> …
>
> (m) "personal health information" means, with respect to an individual, whether living or deceased:
>
> (i) information with respect to the physical or mental health of the individual;
>
> (ii) information with respect to any health service provided to the individual;
>
> (iii) information with respect to the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual;

[10]SK OIPC Review Report H-2006-001 at [13], Review Report LA-2009-002/H-2009-001 at [24], and Investigation Report H-2011-001 at [47], available at www.oipc.sk.ca/reviews.htm.
[11]*Supra* note 6.
[12]SK OIPC Review Report LA-2009-002/H-2009-001 at [24], available at www.oipc.sk.ca/Reports/LA-2009-002%20and%20H-2009-001,%20December%2017,%202009.pdf.

(iv) information that is collected:

(A) in the course of providing health services to the individual; or

(B) incidentally to the provision of health services to the individual; or

(v) registration information;[13]

[30] The information involved in all three cases involves the personal health information of individuals.[14]

[31] The personal health information in all three cases was already collected and stored in electronic information systems belonging to RQRHA. Therefore, the personal health information was in the custody or control of RQRHA.

[32] HIPA is engaged in all three cases.

1. Was the viewing of the personal health information a "collection", "use", or "disclosure"?

[33] Section 2(b) of HIPA defines "collect" as follows:

2 In this Act:

...

(b) **"collect"** means to gather, obtain access to, acquire, receive or obtain personal health information from any source by any means;[15]

[34] In all three cases, personal health information within the Enovation system and LIS was viewed or altered. Therefore, the actions of Employees A, B, or C were not a collection.

[35] Section 2(u) of HIPA defines "use" as follows:

[13] *Supra* note 6.
[14] For example, information about the health services received by the patient/co-worker and information about the health of individuals stored in LIS, including infectious disease information.
[15] *Supra* note 6.

> **2** In this Act:
>
> ...
>
> (u) "use" includes 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.[16]

[36] Further, in my Investigation Report F-2009-001, I defined the terms "use" and "disclosure":

> [78] In any event, section 28 relates to "use" of personal information under its control without consent yet the sharing of information by WCB [Saskatchewan Workers' Compensation Board] with E.T. [an independent claims advisor] would have been a "disclosure". In my 2008-2009 Annual Report, I defined the terms as follows:
>
> "Disclosure is sharing of personal information with a separate entity, not a division or branch of the public body or trustee in possession or control of that record/information."
>
> "Use indicates 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."[17]

[37] In all three cases, the personal health information was viewed, manipulated, or both. Therefore, the action of Employees A, B, and C constituted a use. Nothing was provided to my office to demonstrate there was a disclosure of personal health information.

[38] The next issue of this discussion will focus on the use of personal health information in question.

2. Were the requirements for a "use" of personal health information under *The Health Information Protection Act* satisfied by Regina Qu'Appelle Regional Health Authority?

[39] Section 26 of HIPA governs the use of personal health information by a trustee. Section 26 states as follows:

[16] *Ibid.*
[17] SK OIPC Investigation Report F-2009-001, available at www.oipc.sk.ca/Reports/IRF%202009-001.pdf.

> **26**(1) A trustee shall not use 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.
>
> (2) A trustee may use personal health information:
>
> (a) for a purpose for which the information may be disclosed by the trustee pursuant to section 27, 28 or 29;
>
> (b) for the purposes of de-identifying the personal health information;
>
> (c) for a purpose that will primarily benefit the subject individual; or
>
> (d) for a prescribed purpose.
>
> (3) Nothing in subsection (2) authorizes a trustee as an employer to use or obtain access to the personal health information of an individual who is an employee or prospective employee for any purpose related to the employment of the individual without the individual's consent.[18]

[40] None of the affected individuals in the three cases consented to their personal health information to be viewed or changed by Employees A, B, or C. Therefore, the use of personal health information was not authorized by section 26(1) of HIPA.

[41] When RQRHA employees view personal health information of a patient or co-worker for a purpose other than diagnosis, treatment or care, it is an unauthorized use. Similarly, when employees tamper or alter the recorded personal health information of a patient or co-worker for any purpose other than diagnosis, treatment or care, this would also be an unauthorized use. Corrupting anyone's health record poses safety issues for the patient. It also undermines confidence of other health care workers in the integrity of the medical record. In addition, it undermines public confidence in the security of their electronic medical records and personal health information.

[42] As well, if RQRHA employees use their user privileges to electronic information systems to view their own personal health information for personal purposes, this would be an unauthorized use. This is so notwithstanding that the employee may be working in close

[18] *Supra* note 6.

proximity to his or her medical record and viewing that record may be a very convenient action.

[43] When employees enter an RQRHA electronic database to view the personal health information of a patient for the purposes of diagnosis, treatment or care that would qualify as a permitted use. Should employees enter the database to view their own personal health information that would not be an authorized use and would constitute a violation of section 26 of HIPA. To be clear, although consent of the patient will permit employees to use that patient's personal health information under section 26(1) of HIPA, employees would only get direct access to the patient's personal health information in this context by virtue of their status as an RQRHA employee. In other words, they would not have any direct access to the patient's personal health information but for their employment status with RQRHA. When they are acting as a RQRHA employee, which is the only way they get direct access to their own personal health information, they do not have the status of a patient and cannot give themselves 'consent' to view their own personal health information.

[44] There are practical reasons why this is so:

1. The personal health information is in the custody of the regional health authority, not of the employee. The employee is not the trustee with custody or control of the personal health information. Staff have no lawful entitlement to collect, use or disclose that information for personal purposes, even if that is their own personal health information.

2. The employee is in the same position as any other patient and has no preferred status when it comes to access to their own personal health information. The worker must make a request like any other patient pursuant to the policy and procedures of RQRHA.

3. When an employee of RQRHA snoops in their own personal health information they are effectively interfering with their employer's (RQRHA's) suite of legal responsibilities that are defined in Part V of HIPA. This includes the six reasons enumerated in section 38 why RQRHA may decide to deny access to some or all of the snoopers personal health information (e.g. the snoopers personal health information may also include and be co-mingled with the personal health information of another or may contain information related to litigation or an investigation by a health regulatory body).

[45] It appears that Employees A, B and C viewed personal health information in the Enovation system or LIS for personal reasons rather than to fulfill job duties. Therefore, the viewing of personal health information is not authorized by section 26(2) of HIPA.

[46] Section 26(2)(a) of HIPA refers to sections 27, 28 or 29. Trustees may use personal health information for purposes for which the personal health information may be disclosed pursuant to sections 27, 28 or 29. There are no provisions in these three sections that enables trustees to disclose personal health information for personal reasons.

[47] Employee B modified his co-worker's personal health information in the LIS system to include vulgarities and the acronym "RIP". Such modifications are not authorized by section 26(2) of HIPA.

[48] Section 26(3) of HIPA clearly does not apply to any of the three cases.

[49] I find that the use of personal health information in all three cases was not authorized by section 26 of HIPA.

3. Is Regina Qu'Appelle Regional Health Authority in compliance with sections 16 and 23 of *The Health Information Protection Act*?

[50] I stated in my Investigation Report H-2011-001 that in order to satisfy HIPA, trustees must fulfill the general duties imposed upon them by HIPA:

> [136] In order to satisfy HIPA, the procedures required by any trustee would need to be more comprehensive. Such procedures must also address collection, use and disclosure practices as well as steps taken to respect the general duties in sections 9, 10, 16, and 23 of HIPA…[19]

[51] Sections 16 and 23 of HIPA are two key general duties of a trustee. Section 16 of HIPA states as follows:

[19]SK OIPC Investigation Report H-2011-001, available at www.oipc.sk.ca/Reports/IR%20H-2011-001.pdf.

> **16** Subject to the regulations, a trustee that has custody or control of personal health information must establish policies and procedures to maintain administrative, technical and physical safeguards that will:
>
> (a) protect the integrity, accuracy and confidentiality of the information;
>
> (b) protect against any reasonably anticipated:
>
> (i) threat or hazard to the security or integrity of the information;
>
> (ii) loss of the information; or
>
> (iii) unauthorized access to or use, disclosure or modification of the information; and
>
> (c) otherwise ensure compliance with this Act by its employees.[20]

[52] Section 16 is of critical importance since it constitutes the 'spine' of the HIPA skeleton. It impacts and qualifies every action contemplated by HIPA.

[53] In order for a trustee to discharge its duties under section 16, it must have administrative, technical and physical safeguards.[21] I will examine what safeguards RQRHA had in place later in this discussion

[54] Sections 23(1) and (2) of HIPA imposes a duty on trustees to minimize the amount of personal health information employees have access to. Further, employees should only view or use personal health information on a need-to-know basis to fulfill the purposes for which the personal health information was collected. Section 23(1) and (2) state as follows:

> **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

[20] *Supra* note 6.
[21] SK OIPC Investigation Report H-2005-002 at p. 97, available at www.oipc.sk.ca/Reports/H-2005-002.pdf.

> employee to carry out the purpose for which the information was collected or to carry out a purpose authorized pursuant to this Act.[22]

[55] I explained in my Investigation Report F-2009-001 what the data minimization and need-to-know principles are:

> [92] …Data minimization means that an organization should always collect, use and disclose the least amount of personal information necessary for the purpose. The need-to-know rule is that personal information should only be available to those employees in an organization that have a legitimate need to know that information for the purpose of delivering their mandated services.[23]

[56] In all three cases, employees used personal health information without a need-to-know. Therefore, it is important to understand the safeguards RQRHA has in place and determine if they are sufficient in reflecting the data minimization and the need-to-know principles.

[57] Before I discuss the three types of safeguards - administrative, physical, and technical – I must note that in the Postscript of my Investigation Report H-2010-001, I stated that the biggest threat to data security is likely to be employees of trustee organizations:

> …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 [Pharmaceutical Information Program]? 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**

[22] *Supra* note 6.
[23] *Supra* note 17.

> **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.[24]
>
> [emphasis added]

[58] The three cases discussed in this Report surely provide evidence that snooping employees constitute a major threat to the privacy of patients. I must examine the safeguards that RQRHA has in place to protect against the inappropriate use of personal health information by its employees.

a. What administrative safeguards does Regina Qu'Appelle Regional Health Authority have to protect personal health information and are they adequate?

[24]SK OIPC Investigation Report H-2010-001 at the Postscript, available at www.oipc.sk.ca/Reports/H-2010-001,%20March%2023%202010.pdf.

Circle of Care

[59] Before I discuss RQRHA's administrative safeguards I need to address a problematic theme evident in the RQRHA materials. I am referring to the frequent reference in the materials to 'circle of care'. This term does not appear in HIPA. This concept has, in our nine years of experience overseeing trustees in Saskatchewan, contributed to confusion of HIPA requirements in section 23(2) and non-compliance with HIPA. We have communicated our concern to trustees, including regional health authorities, for a number of years. I am surprised that RQRHA continues to include circle of care in its suite of HIPA resources. In my *2010-2011 Annual Report*, I stated the following:

> **Health and a number of other trustee organizations persist in utilizing 'circle of care' in their literature and education efforts. This is often done without acknowledging that 'circle of care' focuses on the provider and not the patient and is entirely variable given each individual patient and the presenting needs of each individual patient. We have found this concept has contributed to professionals misunderstanding the requirements of HIPA, particularly the 'need to know principle' in section 23(1) of HIPA.** The argument, as we understand it, is that health professions are familiar with the term and have used it for a very long time. Yet, that reliance on old concepts and assumptions has proven, in our experience, to perpetuate an over-confidence that translates into no incentive to learn what HIPA requires. We continue to urge those organizations to instead focus on the 'need to know' which is explicitly provided for in HIPA and which squarely puts the focus on the patient. [25]
>
> [emphasis added]

[60] My office produced a document entitled *Glossary of Common Terms: The Health Information Protection Act* (Glossary)[26] to assist trustees in understanding what is required of them by HIPA. In it, we explain why the term circle of care is unhelpful to health professionals:

> **CIRCLE OF CARE** is not a statutory term and has different meanings depending on whether you are considering the federal PIPEDA [*Personal Information Protection and Electronic Documents Act*] Awareness Raising Tools (PARTS) document or

[25]SK OIPC *2010-2011 Annual Report*, at p. 23 available at www.oipc.sk.ca/Annual%20Reports/2010-2011%20Annual%20Report%20-%20FINAL.pdf.
[26]SK OIPC *Glossary of Common Terms: The Health Information Protection Act (HIPA)*, available at www.oipc.sk.ca/Resources/HIPA%20Glossary%20-%20Blue%20Box.pdf .

provincial literature re: HIPA. This phrase may help explain HIPA in very basic terms to a layperson. Our view is that it is unhelpful when it comes to training of health care workers in trustee organizations. Trustees and trustee employees require a more nuanced understanding of when and how sharing of [personal health information] can occur. The weaknesses of "circle of care" are as follows:

> (1) **It puts the focus on a variety of roles and persons within trustee organizations as to whether they are or are not a member of the 'club' instead of focusing on the patient and the particular care transaction in question.** The better approach is to utilize the 'need to know' principle in section 23 of HIPA which focuses not on the provider as much as it does on the individual patient and the health needs presented in any particular health transaction.
>
> (2) **It suggests a static kind of entitlement to information.** In fact, the circle of care should likely change, even for the same patient, if the patient seeks treatment on Day 1 for a fractured femur and then returns to the same facility on Day 2 for a dietary issue or a mental health problem. There will perhaps be an entirely different group of health workers dealing with the injury on Day 2 than treated the fracture on Day 1. Every member of the Day 2 health care team may not be entitled to all of the [personal health information] collected, used or disclosed on Day 1. A number of trustee organizations in their policies and training material have developed long lists of suggested or possible circle of care members. In our experience this is often misunderstood as a kind of green light for sharing [personal health information] among all of those members without regard to the particular patient and the particular health transaction.
>
> (3) **The circle of care in the training material and policy of a number of trustee organizations is restricted to trustees and their employees. In our view this is unduly restrictive.** Reliance on need-to-know permits disclosure in appropriate circumstances to non-trustees. Using the need-to-know principle, it is not uncommon that even non-trustees may, from time to time, require certain [personal health information] in the course of the diagnosis, treatment or care of the patient (e.g. a police officer who is transporting a sick individual to a different care facility, an adult child providing temporary housing for a senior being discharged from an acute care facility or even a teacher or day care worker who needs to monitor a child for certain adverse drug reactions).

In our experience, a much better practice is to focus on the patient's particular needs and the particular health transaction. This can be done by concentrating on which individuals/roles have a demonstrable need-to-know (per section 23 of HIPA) for some or all of the patient's [personal health information].[27]
[emphasis added]

[27] *Ibid.*

[61] In spite of my office's determination that circle of care is both inadequate and misleading and contributes to HIPA violations, RQRHA has not seen fit, for whatever reason, to align its policy and procedure with HIPA as well as best practices for the management of personal health information.

[62] Over the course of the nine years since the proclamation of HIPA, my office has been advised by health care workers in Saskatchewan that they are confused by circle of care and still struggle to define who qualifies and who does not.

[63] I suggest that the employees of RQRHA in the three subject privacy breaches displayed a sense of entitlement to view and/or modify their own and others' personal health information simply by virtue of being an employee of RQRHA. These three subject privacy breaches occurred over a span of three years which suggests there may be a deep seated culture among employees of viewing and/or modifying personal health information without authority to do so and contrary to HIPA. Such a culture serves to undermine patient confidence in their providers and provider organizations. This becomes a much bigger problem as we move to an electronic health record for each man, woman and child in Saskatchewan. We will have many thousands of registered users (health sector workers) throughout Saskatchewan who will have the ability to view a vast amount of patient personal health information. The protection for patients in such a system consists of 'soft measures' including:

- HIPA training,
- Oath or undertaking of confidentiality,
- Regional health authority policies and procedures,
- Cautionary reminders to users when they sign in to view personal health information in the electronic health record, and
- Audit log of viewing activity for individual patients.

[64] In addition, one might expect that there may be some deterrent value in the following:

- Risk of dismissal for cause by the regional health authority; and
- Risk of a prosecution under HIPA.

[65] Unfortunately, given our province's experience with HIPA to date, both of the above measures now appear more illusory than real.

[66] Our experience in Saskatchewan since 2003 and in other Canadian jurisdictions with electronic medical records and electronic health records is that a significant risk to HIPA compliance is health workers snooping in the profiles of patients for personal purposes. My view is that to meet the requirement of having reasonable safeguards to protect the privacy of patients and the confidentiality of their personal health information RQRHA must take steps to provide a strong deterrent to snooping by its employees. The standard of 'reasonableness' requires some reference to industry standards and recognized best practices. This becomes particularly important too when we find in this province legacy computer systems that are deficient as they do not provide an 'audit trail' feature or offer a layered approach to viewing personal health information which allows graduated degrees of viewing.

[67] While several Saskatchewan regional health authorities, including RQRHA, have dismissed employees who worked in the health records area of hospitals for snooping in patient records, these have consistently been overturned by arbitrators under the particular collective agreements. Saskatchewan arbitrators appear to have taken the position, in spite of HIPA and the ongoing roll-out of electronic health records and the proliferation of electronic medical records, that those health care workers who snoop for personal reasons and clearly do not have a legitimate need-to-know still cannot be terminated for cause because of the principle of progressive discipline. This of course begs the question, how many times a worker should be able to snoop in patient personal health information without a need-to-know before the employer would have just cause to dismiss that worker?

[68] Even more troubling is that a number of these cases involving Saskatchewan regional health authorities involve persons working in the health records area. In our experience, these workers should be even more knowledgeable about HIPA than most other health care workers and are usually the persons dealing with HIPA most frequently as they process access requests, correction requests and security complaints. In many smaller

hospitals and clinics, it is the health records staff who have some responsibility for HIPA training of other hospital staff and responding to their questions about HIPA.

[69] Notwithstanding this pattern of overturning dismissals for cause in this province, a different theme is apparent in some other Canadian provinces. I note that more recent arbitration decisions in the province of Ontario and a decision from British Columbia support the appropriateness of dismissal for cause in cases that involve staff snooping in patient health records. These decisions include:

- Timmins and District Hospital and Ontario Nurses Association (May 11, 2011);[28]
- North Bay Health Centre and Ontario Nurses Association (January 9, 2012);[29] and
- B.C. Nurses' Association and Vancouver Hospital and Health Sciences Centre (February 13, 1997).[30]

[70] In the North Bay decision noted above, the arbitrator relied on an unreported decision from 2010 in Re Bluewater Health and the Ontario Nurses' Association which suggested that zero tolerance should be the norm and only in compelling cases should dismissal for cause not be the result of deliberate privacy breaches.[31]

[71] The effect of recent arbitration decisions in this province appears to minimize, if not ignore, the significance of snooping. That snooping undermines public confidence in electronic health records that will soon make each patient's personal health information available to thousands of health care workers throughout this large province.

[72] The point of this for RQRHA and indeed all regional health authorities is that arbitrators are limited by the type of evidence and the nature of the arguments provided by the regional health authority as employer. As we accelerate the move from paper records to digital records, it is incumbent on RQRHA and other trustee organizations to ensure that arbitrators are aware of the kind of zero tolerance approach that is taken in other jurisdictions and why that is important to protect patient privacy.

[28] *Timmins & District Hospital v. Ontario Nurses' Association (Peever Grievance)* [2011] O.L.A.A. No. 222.
[29] *North Bay Health Centre v. Ontario Nurses' Association (McLellan Grievance)* [2012] O.L.A.A. No. 11.
[30] *British Columbia Nurses' Union and Vancouver Hospital and Health Sciences Centre (Pattison Grievance)* [1997] B.C.C.A.A.A. No. 97.
[31] *Supra* note 29.

[73] What is also required is that in its policies and procedures RQRHA must ensure that all employees understand that snooping without a legitimate need-to-know is likely to result in dismissal for cause. RQRHA apparently utilized a document entitled *RQHR Privacy Violations – Recommended actions for employees DRAFT JAN'11*[32]. This document sets out three different levels:

- Level I – Unintentional;
- Level II – Intentional but Non-Malicious/Multiple Level 1 Violations; and
- Level III – Intentional and Malicious/Multiple Level 1 & II Violations.

[74] Level II includes in recommended actions discipline up to, and including, suspension. Level III recommends "suspension or termination of employee as determined by management". The difficulty with the separation between Levels II and III is that the focus is on the intention of the snooper. The problem with this is that snooping for personal, non-professional purposes is treated differently than snooping with malice. As suggested in the Postscript to my Investigation Report H-2010-001[33], it is likely cold and empty comfort to the affected patient to discover that the health care worker snooping in their personal health information was only doing it to satisfy their curiosity and not for identity theft purposes. My suggestion has been and continues to be that we recognize that the real injury may not be to the affected individual but more generally to public confidence in electronic medical records and electronic health records. In my view creating this distinction between malicious and non-malicious violations tends to minimize the greater damage to patient confidence that warrants the attention by all trustees. A further consideration is that an intention to harm can be an exceedingly difficult element for an employer to prove. Harm is done even by non-malicious violations. In my view, given the early experience of this oversight office and similar offices in other jurisdictions, to treat non-malicious violations less seriously than malicious violations falls short of qualifying as a reasonable measure to safeguard personal health information. To do so, would be a violation of the obligation of every trustee imposed by section 16 of HIPA.

[32] *RQHR Privacy Violations – Recommended Actions for Employees Draft Jan '11.*
[33] *Supra* note 24.

[75] I qualify my conclusion by noting that this presumes that the employee has received appropriate HIPA training, has provided an undertaking or pledge to comply with HIPA and works in a trustee organization that has appropriate written policies and procedures as contemplated by section 16 of HIPA.

[76] RQRHA is therefore left only with 'soft' safeguards such as policy, procedure, oath or undertaking of confidentiality, training and supervision. In my office's HIPA oversight experience, there are no meaningful deterrents to a Saskatchewan health care worker contemplating snooping.

[77] Although recommendations, at different times, have been made to the Ministry of Justice for prosecution both from my office and from regional health authorities, no prosecution has ever been initiated under HIPA in the nine year history of that law. Before there can be a prosecution under section 64 of HIPA, the Minister of Justice must provide consent. I should note that in August 2012, the Minister of Justice announced that a government working group would be created to study the issue of enforcement of HIPA to include possible amendment of the offence provision in HIPA, or possibly the creation of regulatory offences. To my knowledge no report or recommendations have been forthcoming to date. So, as matters stand, the threat or prospect of prosecution under HIPA and fines of up to $500,000 for an organization and $50,000 for an individual seems more illusory than real. I note that there have been three successful prosecutions in Alberta under that province's *Health Information Act*[34] and now a number of other charges pending.

[78] Given that neither dismissal for cause of snooping employees, nor prosecution have found any traction in Saskatchewan to this point, all that remains are the soft safeguards. Even with soft safeguards, we have seen that the utilization of legacy computer systems, such as the Enovation system used by RQRHA that cannot accommodate audit trails leaves RQRHA with only (1) HIPA training, (2) oath or undertaking of confidentiality, (3) regional health authority policy and procedures, and (4) the cautionary reminder or

[34]Alberta, *Health Information Act*, R.S.S. 2000, c. H-5.

prompt when someone signs in to view personal health information. If all we have then are those four items in the regional health authority privacy toolbox, we need them to pack more of a wallop than would otherwise be the case.

[79] It is important that RQRHA, and indeed all regional health authorities, make those soft safeguards as effective and impactful as possible. Anything less would not meet the statutory requirement for safeguarding personal health information.

[80] Given this current context, there can be no excuse for regional health authorities to not take all possible steps to ensure that there is a high standard of training for all of its employees, regular in-service refresher training, clear, simple accessible policies and procedures which mirror accurately the many relevant provisions of HIPA.

Policies and Procedures

[81] As stated earlier, the term circle of care is prevalent throughout RQRHA's policies, procedures, and HIPA training materials for its staff.

[82] In regards to the privacy breach involving Employee A and the viewing of personal health information on the Enovation system, RQRHA provided my office with two policies and their related procedures.

[83] The first policy is entitled *Use and Disclosure of Personal Health Information within the Circle of Care*.[35]

[84] The portions of the policy that would apply to this privacy breach states as follows:

> **Policy**
>
> Circle of Care **Personal Health Information may be accessed, used and disclosed, on a need to know basis**, in accordance with ethical guidelines, within the client's Care Team, for an Authorized Health Purpose. This will include disclosing Personal Health Information to members of the Care Team who are trustees (or employees of

[35]RQRHA, *Use and Disclosure of Personal Health Information within the Circle of Care*, Policy No. 505, October 20, 2005.

trustees) outside of the Region and in limited circumstances (see Procedure) a non-trustee who is a part of the client's Care Team.
…

2. Revision History

This is a new policy created as a result of the provincial Health Information Protection Act.

3. Person's Affected

All RQHR staff and agents are affected.[36]

[emphasis added]

[85] The following aspects of the related procedure that relates to the privacy breach states as follows:

1.1. Need to Know (Circle of Care) Region personnel may only access, use or disclose Personal Health Information on a need-to-know basis for an Authorized Health Purpose for a particular client. All use and disclosure must be in accordance with the applicable personnel's professional ethical guidelines and RQHR policies and procedures. Individuals shall not access, use or disclose Personal Health Information for purposes outside of their duties. Personal Health Information shall not be accessed, used or disclosed for personal reasons, or for gain, or gossip *(see section 23(1) of HIPA)*.

1.2. Care Team ... A non-trustee may be included as part of the Care Team provided they need to know the Personal Health Information for an Authorized Health Purpose and there are appropriate confidentiality agreements in place between the Region and the non-trustee. A confidentiality agreement is not required with a non-trustee in emergency circumstances.
...

1.9. Conditions Access, use or disclosure under this Policy is subject to two very important conditions:

1.9.1. the access, use or disclosure must be made in accordance with the Region's privacy and security policies and procedures (for example, care must be taken when discussing Personal Health Information in public places); and
1.9.2. if the access, use or disclosure is being made by a health provider, such access, use or disclosure must be in accordance with the ethical guidelines applicable to that health provider **(see section 27(3) of HIPA)**.

...

[36] *Ibid.*

> **3. Person's Affected**
>
> All areas, staff and agents of the region must comply with the policy and procedure.[37]
>
> [emphasis added]

[86] With the exception of using the term circle of care, the above content is appropriate in addressing the fact employees should be using (viewing) information only on a need-to-know basis to fulfill job duties. This is in keeping section 23(1) and (2) of HIPA.

[87] The second policy and its related procedure provided to my office is entitled *Use and Disclosure of Personal Health Information outside the Circle of Care*.[38]

[88] The policy, however, only discusses disclosure. Therefore, the policy would not be applicable in this particular privacy breach.

[89] The related procedure, though, mentions the following about use:

> **1. Procedure**
>
> **All access, use or disclosure must be made in accordance with the RQHR's privacy and security policies and procedures;**
> **If the access, use or disclosure is being made by a health provider, such access, use or disclosure must be in accordance with the ethical guidelines applicable to that health provider (*see section 27(3) of HIPA*).**
> …
>
> 1.4. Clear Benefit to the Health and Well-Being of an Individual. Personal Health Information may be disclosed outside of the Circle of Care (the Care Team) if the disclosure is being made for the provision of health or social services to the client and, if, in the opinion of the trustee, disclosure of the personal health information will clearly benefit the health or well-being of the individual.
> Note that this exception does not apply where it is reasonably practicable to obtain consent from the individual.
>
> Disclosure of Personal Health Information pursuant to this exception may only be made where the recipient agrees:

[37]RQRHA, *Use and Disclosure of Personal Health Information within the Circle of Car*e, Procedure Reference Number: 505-1. Undated.
[38]RQRHA, *Use and Disclosure of Personal Health Information outside the Circle of Care*, Policy/Procedure No. 506, October 20, 2005.

- **to use the information only for the purpose for which it is being disclosed;** and

- not to make further disclosure of the information in the course of carrying out any of the activities mentioned above (*see sections 27(4)(j) and 27(6) of HIPA*).

…

1.9. Billing. **Access, use or disclosure of Personal Health Information is authorized where it is made for the purpose of obtaining payment for the provision of services to the subject individual and is done in accordance with the Region's policies and procedures and all applicable ethical guidelines** (*see section 27(4)(k) of HIPA*).

…

1.14 Evaluation and Quality **Personal Health Information shall not be disclosed outside of the Circle of Care (the Care Team) in response to a request to use the information for planning, delivering, evaluating or monitoring a program of the RQHR without first having the request approved by the appropriate Region management personnel.** Appropriate safeguards must be in place to protect the information from unauthorized use and disclosure (*see section 27(4)(k)(ii) of HIPA*).[39]

[emphasis added]

[90] What is lacking in the above policies and procedures is a definitions section. For example, it appears that RQRHA is using the same definition for the terms "access" and "use". This is concerning since the terms access and use in access and privacy legislation have different meanings. The term access as understood in HIPA is "the right of an individual (or his or her lawfully authorized representative per section 56 of HIPA) to view or obtain copies of records in the custody or control of a trustee."[40] The term "use" according to HIPA, as quoted earlier, "includes 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."[41]

[91] My office recommended to RQRHA that it include a definitions section for the above policies and procedures, and such definitions should be consistent with relevant access

[39]RQRHA, *Use and Disclosure of Personal Health Information Outside the Circle of Care*, Procedure Reference Number: 506-1, Undated.
[40]*Supra* note 26.
[41]*Supra* note 6 at section 2(u).

and privacy legislation. To address our recommendation, RQRHA responded by stating it would create a "Glossary of Privacy Terms" for use within the RQRHA by the end of the current fiscal year.[42] I do not know what would be included in this proposed document. It follows that we cannot assess whether the content will be accurate and appropriate.

[92] Another concern with the policies and procedures is that RQRHA cites subsection 27(3) of HIPA as if it is a stand-alone provision. For example, the procedure *Use and Disclosure of Personal Health Information within the Circle of Care* states as follows:

> 1.9.2. if the access, use or disclosure is being made by a health provider, such access, use or disclosure must be in accordance with the ethical guidelines applicable to that health provider **(*see section 27(3) of HIPA*)**.[43]
>
> [emphasis added]

[93] Section 27(3) of HIPA is not a stand-alone provision. It applies to subsection 27(2). Section 27(2) provides for no-consent (deemed consent) in certain circumstances. Section 27(3) states as follows:

> **27**(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.[44]
>
> [emphasis added]

[94] In its preliminary analysis, my office recommended to RQRHA that it should revise its description of subsection 27(3) of HIPA. Further, my office recommended that RQRHA

[42] RQRHA email dated October 10, 2012.
[43] *Supra* note 35.
[44] *Supra* note 6.

include other applicable sections of HIPA, such as the general duties imposed upon trustees by HIPA, including 9 (prospective transparency to patients), 10 (retrospective transparency to patients), 16 (policies and procedures for HIPA compliance), 19 (accuracy) and 23 (data minimization and need-to-know).

[95] However, RQRHA responded to our office on October 10, 2012 as follows:

> RQHR policies are reviewed as issues arise that require changes to the content of the policies. A definitive timeline cannot be provided at this point. The goal of the Privacy Office has always been to develop specific tools and have detailed policies available at the department level.

[96] What remains unexplained is the lapse of time and the failure to act. The misuse of personal health information in electronic information systems in 2009 and again in 2011 would certainly, in my view, be sufficient cause to trigger a review and revisions of relevant policies and procedures in an effort to prevent similar privacy breaches from occurring again.

[97] For the other two cases in which Employees B and C used personal health information of other individuals on LIS, RQRHA provided several other policies and procedures:

1. *Personal Health Information Protection* Policies
2. *Confidentiality* Policy and Procedure
3. *Regina Health District Information System Security* Policy and Procedure
4. SIAST Clinical Forms, and
5. *LABLisOP8000.4 SoftSecurity User Management* Policy

I will deal with each of the above sequentially.

1. *Personal Health Information Protection* Policies

[98] The first policy and related procedure is entitled *Personal Health Information Protection*. The policy is very brief and it makes no specific mention of use of personal health information. The introduction to the policy states as follows:

> As a trustee of personal health information, all RQHR staff shall maintain administrative, technical and physical safeguards that protect the integrity, accuracy

> and confidentiality of the personal health information, regardless of the storage medium.[45]

[99] The procedure is slightly longer than the policy but makes very brief mention of use of personal health information. It states:

> 1.2 Internal Security The internal security procedures shall address the following areas:
>
> …
>
> - **personal health information is accessed only when there is a need to know to allow staff to complete their assigned responsibilities**
> - appropriate use, information is accessed for uses for which it was collected, and nothing more[46]
>
> [emphasis added]

[100] My office continues to stress the importance of providing staff of trustee organizations with practical, accessible, concrete and granular information about what they must do to comply with HIPA.[47] I find that the policy and procedure discussed above do not provide such information on the collection, use and disclosure of personal health information. It does explicitly state that personal health information should only be accessed when there is a need-to-know. However, I find that both the policy and procedure does not define the terms need-to-know and data minimization. As stated earlier, I explained the data minimization and need-to-know principles in my Investigation Report F-2009-001.[48]

[101] Therefore, I recommended that RQRHA revise its policies and procedures to include explanations of the terms. RQRHA responded on September 19, 2012 by stating that its "confidentiality policy" (to be discussed later) has been revised to include definitions of the terms. It stated:

> RQHR has included these definitions in a definition section in the revised confidentiality policy and procedure which is in the review and approval process.

[45]RQRHA, *Personal Health Information Protection*, Policy Reference Number: 501, Effective October 20, 2005.
[46]RQRHA, *Personal Health Information Protection*, Policy Reference Number: 501-1, Effective Date October 20, 2005.
[47]*Supra* note 19 at [149].
[48]*Supra* note 17 at [92].

2. *Confidentiality* Policy and Procedure

[102] Another policy and procedure RQRHA provided to my office includes RQRHA's *Confidentiality* policy and its related procedure. Both copies have the approval date of June 6, 2000. Since that was more than three years prior to the proclamation of HIPA, such materials needed to be revised to capture "privacy" as well as "confidentiality" and new rules for collection, use and disclosure of personal health information.

[103] RQRHA noted in its May 11, 2012 letter that they were "in the process of updating the Confidentiality Policy and Procedure".

[104] The policy states as follows:

> As part of your association with the Regina Health District, you have authority to access certain information. **This access is limited and strictly confined to information required for performance of current duties.**
>
> Breach of confidentiality includes any intentional or inadvertent unauthorized access to, or disclosure of confidential information, including but not limited to:
>
> - clinical or personal information regarding family members, visitors, friends, partners, former clients, prominent public figures, colleagues, etc.
> - non-clinical information (e.g., personnel, business or financial records).
>
> When it is deemed that an intentional breach of confidentiality has occurred, the result will be immediate disciplinary action being taken, including suspension and up to and including dismissal of the employee, or in the case of members of the medical staff, immediate loss of all privileges.
> …
>
> **.04 Data Security**
> …
>
> Access to corporate data must be properly authorized, and will be granted based on the requirements for carrying out responsibilities. The Regina Health District retains the exclusive rights to, and use of all computer assets and information which it owns, and which resides on:
>
> - Regina Health District mid-range servers.

- Regina Health District applications residing on network servers, and/or stand-alone computers.

To have authorized access to a system, a user requires a sign-on. A sign-on represents an individual's electronic signature and consists of a login ID and password.[49]

[emphasis added]

[105] In the related procedure, the portion that deals with use is as follows:

Accidental Access to a Client's Electronic Record

1. Access to a client's electronic record is defined as:

   Viewing, printing, transmitting demographic or medical information on an individual which has been collected, stored and can be retrieved in an electronic format.

2. If anyone accidentally accesses a client's electronic record, that individual must immediately submit written documentation of his/her actions to his/her supervisor.

3. Documentation of accidental access must include the following information:

   - date of access.
   - the client's ID (MRN#)
   - reason for access.
   - individual's name, ID and unit area.

The supervisor must forward this documentation to Information Technology. Information Technology will acknowledge receipt of this documentation by sending a written confirmation notice to the supervisor.[50]

[emphasis added]

[106] Finally, a form with the subject line "Confidentiality and Security Agreement" states as follows:

[49]RQRHA, *Confidentiality*, Policy No. 1.1.5, June 6, 2000.
[50]RQRHA, *Confidentiality*, Procedure No. 1.1.5, June 6, 2000.

> **Employee Confidentiality and Security Agreement**
>
> I _____ do solemnly affirm that I will faithfully discharge my duties as a member of the Regina Health District staff and will observe and comply with the policies and procedures of the Regina Health District with respect to confidentiality. **Except when I am legally authorized or required to do so, I will not access confidential information** and I will not disclose or give to any person any information or document that comes to my knowledge or possession by reason of my affiliation with the Regina Health District. I have read this policy on Confidentiality of Information and understand that a breach of this policy will be just cause for disciplinary action, including suspension, and up to and including termination of my employment or affiliation with the Regina Health District.
>
> Date: _____
> Signature: _____
> Witness: _____ [51]
>
> [emphasis added]

[107] I find that the examples of what a breach of confidentiality is helpful in providing direction to employees of what they should not be doing. It is unclear, though, the purpose of notifying Information Technology when an employee accidently accesses a client's electronic medical record. Certainly, Information Technology can play a role in preventing similar accidental viewing of personal health information by reviewing and revoking access privileges. However, the policy is unclear as to the role Information Technology would fill. My office recommended that the policy and procedure be revised so that the RQRHA Privacy Officer is notified of any breach of confidentiality, whether it be intentional or accidental, so that the RQRHA Privacy Officer can investigate the matter.

[108] Although it was not clear in the policy or procedure, RQRHA responded on September 19, 2012 to my office's recommendation by stating the following:

> The Risk Management/Privacy Office is notified of any breaches of confidentiality by the Regional Confidential Occurrence Reporting process.

[51] RQRHA, *Confidentiality and Security Agreement*, Form No. 1.1.5, June 6, 2000.

3. *Regina Health District Information System Security* Policy and Procedure

[109] The third policy and related procedure provided to our office is entitled *Regina Health District Information System Security*. Both the policy and procedure have an approval date of March 17, 1994.

[110] The policy is one sentence in length and it vaguely addresses employees' use of personal health information. It states the following:

> Security codes used by each employee to access the Regina Health District Information Systems, and **information obtained by use of the systems, shall be maintained in the strictest confidence by each individual.**[52]
>
> [emphasis added]

[111] The related procedure states the following about use of personal health information:

> …
>
> 2. In order to maintain client confidentiality, employees shall ONLY use the computer systems to:
>
> 2.1 gain access to or enter data on a client record in accordance with their job requirements.
>
> or
>
> 2.2 perform other authorized system functions.
>
> …[53]

[112] Finally, a form entitled *Acknowledgement of Regina Qu'Appelle Heath* [sic] *Region Information System Security*[54] states the following about the use of personal health information:

[52]RQRHA, *Regina Health District Information System Security*, Policy No. 5.4.03, March 17, 1994, Revised: October 5, 1995.
[53]RQRHA, *Regina Health District Information System Security*, Procedure No. 5.4.03, March 17, 1994, Revised: October 5, 1995.
[54]RQRHA, *Acknowledgement of Regina Qu'Appelle Heath [sic] Region Information System Security*, Form No. 5.4.03. Undated.

> …
>
> In order to maintain client confidentiality and the security of the Authority's information, I agree to use the computer system only to perform activities for which I have been authorized:
>
> 1. To gain access to or enter data on a clients [sic] record in accordance with my job requirements or
>
> 2. To perform other authorized system functions.
>
> …[55]

[113] I will discuss the lack of practical, accessible, concrete and granular information in the above policy and procedure after I introduce the SIAST [Saskatchewan Institute of Applied Science and Technology] Clinical Forms, *Confidentiality – Teaching Purposes Procedure*, *Confidentiality – Volunteers/Student Procedure*, *Confidentiality – Volunteer/Student Form*, and the *LABLisOP8000.4 SoftSecurity User Management*.

4. SIAST Clinical Forms

[114] RQRHA provided my office with forms that are filled out by students of the Saskatchewan Institute of Applied Science and Technology (SIAST). Employees in the lab can be SIAST students. Working in the lab is a part of the Medical Diagnostics Diploma Programs at SIAST.

[115] RQRHA provided us with information on how SIAST provides HIPA training to its students. I certainly encourage students to continue to learn about HIPA through SIAST. However, since students are working for a facility with the RQRHA, RQRHA is the trustee ultimately responsible for ensuring the students working within the facility is complying with HIPA.

[116] RQRHA provided us with the *Confidentiality – Teaching Purposes* procedure in regards to teaching students. In regards to use, it states:

[55] *Ibid.*

> …
>
> 2. Students may have direct access to clients' charts only while participating in direct client contact personally or with their teachers, or otherwise with the client's consent. In all cases it is understood that the client must have consented to be taught upon.
> …[56]

[117] The *Confidentiality – Volunteers/Student* procedure provides very little direction to students in regards to use. It states as follows:

> 1. Volunteers/Students are subject to the same code of ethics that apply to the professional staff, namely discretion in the handling of privileged information.
>
> 2. Volunteers/Students are educated about confidentiality at their orientation program.
>
> 3. Upon acceptance as a volunteer/student, all new volunteers/students will be asked to sign a "Commitment/Confidentiality" statement. This is to ensure their understanding of what is expected of them as a volunteer/student, and also to reinforce the importance of maintaining confidentiality and the commitment they are making to the Regina Health District.
> …[57]

[118] Finally, the *Confidentiality – Volunteer/Student* form does not even clearly address the use of personal health information. It states as follows:

> As a volunteer/student, you will be expected:
>
> - to consider as confidential, all information that you hear directly or indirectly concerning a client, staff member; to avoid seeking information concerning any of these, and above all to respect the client's right to privacy.
> - to accept direction from Regina Health District staff and the guidelines/limitations of what a volunteer/student can and cannot do.
> - to uphold the policies of the Regina Health District regarding volunteers/students, and in particular regarding confidentiality issues.[58]

[119] Providing definitions and examples of privacy and confidentiality would be helpful.

[56]RQRHA, *Confidentiality – Teaching Purposes*, Procedure No. 1.1.5.02, June 6, 2000.
[57]RQRHA, *Confidentiality – Volunteer/Student*, Procedure No. 1.1.5.03, June 6, 2000.
[58]RQRHA, *Confidentiality – Volunteer/Student*, Form No. 1.1.5.03, June 6, 2000.

[120] Further, students should be treated as any other employee in terms of privacy training and agreements, especially if they are exposed to patient personal health information. Students may receive HIPA training from an educational institution, but RQRHA is ultimately responsible for their patient's personal health information. RQRHA, therefore, needs to be training students the same way it trains staff on what is expected on how students collect, use, and disclose personal health information.

[121] My office recommended that RQRHA have the same expectations and standards for students as it has for staff when it comes to complying with HIPA. Students should be receiving the same privacy training as staff receives, and they should be signing the same privacy, confidentiality and security agreements that staff sign.

[122] RQRHA reassured my office on September 19, 2012 that it takes responsibility for training students working within RQRHA by stating:

> All students interacting with RQHR program must first sign the RQHR Confidentiality Agreement. Privacy Training is provided by the RQHR to students at orientation and IT training.

[123] Later in this Report, I discuss in further detail the orientation and information technology training.

5. *LABLisOP8000.4 SoftSecurity User Management* Policy

[124] Finally, RQRHA provided my office with a document entitled *LABLisOP8000.4 SoftSecurity User Management*[59]. It appears that this policy is for the purpose of adding users to LIS so that the employee can become a lab system user. This policy does not address the use of personal health information.

[125] As mentioned earlier, my office stresses the importance of providing staff of trustee organizations with practical and granular information about what they must do to comply with HIPA. Many of the above policies and procedures do not cite HIPA nor do they

[59]RQRHA, *LABLisOP8000.4 SoftSecurity User Management*, Policy Revision No. 1.4 March 28, 2012.

explicitly explain the data minimization and need-to-know principles as required by section 23 of HIPA. The instructions in regards to use are vague at best. My office pointed out to RQRHA in a letter dated August 10, 2012 that its brochure entitled *Protecting Clients' Privacy* and *Your Privacy Rights in the Regina Qu'Appelle Health Region* (to be discussed later on) contains helpful information that should be included in its policies and procedures.

[126] On October 10, 2012, RQRHA responded to this particular recommendation by providing the same response to a recommendation I described earlier to revise its policies and procedures in regards to use and disclosure of personal health information:

> RQHR policies are reviewed as issues arise that require changes to the content of the policies. **A definitive timeline cannot be provided at this point.** The goal of the Privacy Office has always been to develop specific tools and have detailed policies available at the department level.
>
> [emphasis added]

[127] I do not understand this response from RQRHA. I am mindful that when HIPA was proclaimed September 1, 2003, the Ministry of Health was unprepared for its implementation. In fact, it purported to create a 'grace period' in 2003 for an indefinite time during which no enforcement action would be undertaken. There was no manual, no sample policies or procedures, no check lists, no sample documents and what little was provided by the Ministry of Health amounted to little more than recitation of the statutory provisions in HIPA. So, there was a recognition that it would take some time for regional health authorities to develop policies and procedures and just generally a capacity to meet the requirements of HIPA. The difficulty is that too much time has passed since HIPA came into force and too little has been done in terms of creating the policies and procedures contemplated and required by that statute. RQRHA's response to my office's investigations into the three subject privacy breaches and different recommendations made during the course of the investigations is unsatisfactory. Why are there no definite timelines for changes? Why the need to wait for further study and assessment? The threats to patients' privacy are immediate and ongoing and warrants a more forceful and expedited response from Saskatchewan's second largest regional health authority.

[128] It appears that the misuse of personal health information in electronic information systems such as the Enovation system and LIS warrants more attention by RQRHA. There is certainly a need for a plan for RQRHA to revise its policies and procedures so that the use of personal health information by employees is in compliance with HIPA in a timely fashion. Revisions should include:

1. removing the concept of circle of care and focusing on the concept of need-to-know;
2. citing sections of HIPA upon which their policies and procedures are based;
3. including definitions so that the policies and procedures are easy to understand; and
4. ensuring their policies and procedures are more practical, accessible, and granular.

[129] A striking and current feature of a number of the RQRHA policies and procedures is that they not only antedate HIPA but also antedate modern electronic record systems. They are ill-suited to address modern health care delivery.

[130] Another glaring omission, which I have already discussed, in the policies and procedures is employees accessing their own personal health information. In two of the three cases, it was found that an employee accessed her own personal health information. In the case involving Employee B, it was found that the MLA herself had modified her personal health information at one point. If employees wish to view or have their personal health information amended, they must request to view or request amendment in accordance with Part V of HIPA. Therefore, I recommended to RQRHA that it address this in its policies and procedures.

[131] RQRHA responded on September 19, 2012 by stating the following: "This issue is currently being reviewed by senior management to determine a RQHR policy and procedure on this subject."

[132] On September 24, 2012, my office requested that RQRHA provide a firm timeline as to when a policy would be implemented to address the issue of employees viewing their own personal health information. RQRHA responded on October 10, 2012 as follows: "We expect the RQHR Senior Management Team **to make a decision** on this topic by end of this fiscal year." [emphasis added]

[133] It is curious to me that in dealing with two HIPA privacy breaches that occurred in 2009 the best that RQRHA can apparently do is to advise us that sometime before March 2013 the Senior Management Team may simply make a decision on this topic. The delays and inaction described in this Report reflect poorly on RQRHA. Employees helping themselves to viewing and modifying of their personal health information undermines the integrity and accuracy of the personal health information RQRHA manages. Further, if employees can simply view and modify their own personal health information, what will stop them from viewing and modifying the personal health information of others?

[134] Employees must only view personal health information to fulfill their job duties. It is imperative that RQRHA makes a commitment to address this issue immediately.

Other administrative safeguards

[135] RQRHA has provided us with two brochures it has produced. Before commenting on the specific content, I would observe that section 16 of HIPA requires written policies and procedures. I do not view brochures as policy documents or even as procedure documents. They are really an education/orientation vehicle intended to provide summary information not detailed information to the reader.

[136] Section 9 of HIPA certainly contemplates such brochures to provide some general information to patients and the public. Section 16 contemplates something much more comprehensive and detailed to particularize what is required of RQRHA staff to ensure HIPA compliance.

i. Brochures

[137] The first brochure RQRHA provided to my office is entitled *Protecting Clients' Privacy* which is for employees. It is not a formal policy or procedure. The first page of the brochure explains that the brochure contains tips and reminders for employees in protecting RQRHA clients' privacy. The remainder of the brochure covers topics about the privacy rights of patients, including informing patients of the purpose for the collection of their personal health information, using personal health information only to fulfill job duties and the consequences of non-compliance with HIPA.

[138] Pages 2 to 5 of the brochure read as follows:

> Employees are encouraged to keep in mind the following points
>
> - Only collect information that is needed for the admission, assessment, examination, or treatment of clients.
> - Be prepared to tell clients why you are collecting their personal health information and who it might be shared with.
> - You do not have a general "right" to access personal information held by the RQHR.
>
> You are only authorized to access personal health information that you need to know for the purposes of fulfilling your duties and job responsibilities.
>
> - Client health related information is not to be discussed in areas where you may easily be overheard. Staff are required to take all reasonable precautions to ensure that discussions about client related issues do not take place in public areas, including elevators, cafeterias, waiting areas, and public hallways.
> - Client health related information is not to be the subject of gossip or coffee conversation.
> - Remember that family, friends, and RQHR staff may also be clients of RQHR. You are expected to respect their privacy and not access their personal health information unless you have a need to know the purposes of fulfilling your job responsibilities. Their personal health information must be treated with the same level of protection that would be given to any other clients of RQHR, and must not form the subject of non care related conversation amongst staff.

- Protect client information by ensuring that information is not easily viewed by people or staff who do not have a need to know. Close client charts when not in use and never leave "open" while unattended. Store client charts in a central location within nursing units or in secured space located in clients' rooms.

- Client charts are to be returned to secured storage in the health information management services as soon as reasonably possible after care is completed.

- Protect client information by locking doors, filing cabinets, or rooms where client records are stored.

- Client records must be secured and protected until the moment of destruction. Remember that patient management, scheduling, and staff assignment lists often contain client information and should also be secured and protected until the moment of destruction.

- Client information that is no longer required for use or for the client's medical file/record must be shredded. All documents containing client information, including personal working notes made by staff, must be disposed of in the locked, large blue or red Crown Shred and Recycling Inc. bins located throughout RQHR's facilities, or use an approved shredder in your facility. Documents with client information must not be disposed of in regular garbage or regular recycling baskets.

- Inappropriate accessing or disclosure of personal health information can result in discipline, up to and including discharge, fines of up to $50,000 per offence, or one year imprisonment under the [sic] *Health Information Protection Act* (HIPA) legislation, and the possibility of civil litigation.[60]

[139] This brochure provides helpful and instructive information as to what employees need to do to comply with HIPA. However, section 16 of HIPA requires that trustees establish policies and procedures – not brochures – to maintain administrative, technical and physical safeguards:

> **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:

[60]RQRHA, *Protecting Clients' Privacy,* RQHR 1030, November 23, 2011 at pp. 2 to 5.

> (i) threat or hazard to the security or integrity of the information;
>
> (ii) loss of the information; or
>
> (iii) unauthorized access to or use, disclosure or modification of the information; and
>
> (c) otherwise ensure compliance with this Act by its employees.[61]
>
> [emphasis added]

[140] Therefore, if such information existed in an established policy or procedure, then that would assist RQHR in fulfilling its general duty outlined in section 16.

[141] I recommended to RQRHA that it consider revising its formal policies and procedures to contain more detailed guidance and direction to its staff.

[142] Again, RQRHA stated in its response dated October 10, 2012 that it would only review policies as issues arise that would be cause to revise the policies. It could not provide our office with a timeline as to when it would review and revise its policies.

[143] I fail to understand why RQRHA continues to rely on its current policies and procedures that have proven to be ineffective in preventing employee snooping. The occurrence of the three privacy breaches discussed in this Report suggest that RQRHA's current policies and procedures are inadequate in protecting the personal health information in its custody or control. Employees must be trained and held accountable to a trustee organization's policies and procedures, not its brochures.

[144] Further, policies and procedures are apparently not updated regularly. In some cases, such as the policy and procedure entitled *Regina Health District Information System Security*[62] referenced earlier, dates back to 1994, almost ten years before HIPA came into force.

[61] *Supra* note 6.
[62] *Supra* note 52.

[145] RQRHA also provided my office with an accompanying brochure called *Your Privacy Rights in the Regina Qu'Appelle Health Region*[63] that is meant for patients. It explains to patients the purpose for the collection of personal health information, how it will be used, under what circumstances it would be disclosed and how it will be safeguarded. It also advises patients how they may access their personal information. I find that it is an informative tool that empowers clients to make informed decisions about their personal health information.

[146] Providing brochures explaining to patients the anticipated uses and disclosures assists RQRHA in partially fulfilling the transparency requirements codified in section 9 of HIPA, which states:

> **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.[64]

[147] At page 5 of my Investigation Report H-2005-002 states the following about section 9:

> Transparency is an important requirement codified in section 9 of HIPA. Section 9(1) of HIPA provides that an individual has the right to be informed about the anticipated uses and disclosures of the individual's personal health information. By virtue of section 9(2), any trustee that collects personal health information must take reasonable steps to inform the individual of the anticipated use and disclosure by the trustee. Section 9(3) requires that a trustee must establish policies and procedures to promote knowledge and awareness of the rights extended to individuals by HIPA.[65]

[148] In my office's letter dated August 10, 2012, my office reminded RQRHA of my long-standing position on the term circle of care and how it is not particularly helpful for

[63]RQRHA, *Your Privacy Rights in the Regina Qu'Appelle Health Region*, CEAC 0706, November 2011.
[64]*Supra* note 6.
[65]*Supra* note 21 at p. 5.

trustees attempting to comply with HIPA.[66] My office recommended that RQRHA remove the term circle of care and utilize the term need-to-know.

[149] RQRHA responded in its letter dated September 19, 2012 as follows:

> The circle of care concept that has been imbedded within our organization includes the "Need to Know' [sic] requirement. In order to better orient staff to the fact that "Need to Know" is an important criteria within the "Circle of Care" the Employee Orientation Manual has been revised to clarify this. When education sessions are held, the term will be explained to include more about need to know.

[150] In an email dated September 24, 2012 from my office to RQRHA, we reiterated that we were recommending that the term and concept of circle of care be replaced by the term and concept of need-to-know. What RQRHA has created is confusing and unhelpful.

[151] RQHR responded on October 10, 2012 by stating:

> We continue to educate staff that the Circle of Care is intended as a visual depiction of Section 27(2) of HIPA and that "need to know" is a fundamental component of the circle of care model. While this may be considered in the future, at this time we are not planning to remove the circle of care from our training materials.

[152] As quoted earlier, my office's Glossary, explains that the term circle of care is unhelpful as it:

- puts the focus on health care providers instead of the patient;
- suggests a static kind of entitlement to a patient's personal health information; and
- the circle of care concept has been misinterpreted to only include trustees and their employees. However, there are those who are non-trustees who may have a demonstrable need-to-know, such as a police officer, teacher or day care worker.[67]

[153] The three cases discussed in this Report clearly indicate that the unauthorized viewing and modification of personal health information, such misuse of personal health information is clearly not a one-off stand-alone issue in the RQRHA. Revising its

[66]SK OIPC *FOIP Folio*, February 2004 at p. 4; SK OIPC Investigation Report H-2005-002 at p. 125; SK OIPC Annual Reports: *2009-2010* at p. 18, 2*010-2011* at p. 23, available at www.oipc.sk.ca under the *Newsletters*, *Reports* and *Annual Reports* tabs respectively.
[67]*Supra* note 26.

administrative safeguards so that those accurately reflect HIPA requirements would be essential in minimizing the chances of similar privacy breaches from occurring again. Eliminating circle of care and replacing it with need-to-know would be an important step to move in such a direction.

[154] No one has been able to satisfactorily explain to our office what value circle of care adds to the statutory limitation of need-to-know. Yet as snooping continues to occur, surely prudence requires that RQRHA needs to re-examine how it is educating its employees for HIPA compliance and why it has experienced these kinds of egregious, deliberate HIPA breaches.

ii. *Privacy Alerts*

[155] The RQRHA Privacy Office sends out reminders called *Privacy Alerts* to its employees. They serve as reminders as to what is expected of employees in regards to privacy. RQRHA explained to us in its letter dated May 11, 2012 as follows: "The RQHR provides HIPA training to all employees. Privacy Alerts are meant to be reminders of the training that each employee has already received."

[156] RQRHA provided us with two *Privacy Alerts*. The first *Privacy Alert* states as follows:

> …
>
> - RQHR computer system users shall lock their workstations or log off all applications and the network whenever the user leaves their workspace for an extended period of time. (Hint: to quickly lock your workstation press one of the Windows logo keys plus the L key or CTRL + ALT + Delete keys)
>
> - All access to RQHR applications or systems shall be secured with system credentials or user ID's and passwords. Each RQHR user ID uniquely identifies each user to a specific RQHR application or system. This user ID and password combination shall establish access to RQHR systems. **It is imperative that passwords are never shared with anyone.**
>
> - If your ID and password have been used to inappropriately access personal health information, you will be held accountable for this activity.
>
> …

[emphasis added]

[157] The body of the second *Privacy Alert* states as follows:

> - Region personnel may only access, use or disclose Personal health Information on a **need-to-know basis** for an Authorized Health Purpose for a particular client. All use and disclosure must be in accordance with the applicable personnel's professional ethical guidelines and RQHR policies and procedures. **Individuals shall not access, use or disclose** Personal Health Information for **purposes outside of their duties.** Personal Health Information shall not be accessed, used or disclosed for personal reasons, or for gain, or gossip (see section 23(1) of HIPA).
>
> [emphasis added]

[158] It is commendable that this *Privacy Alert* cites the need-to-know principle and refers readers to section 23(1) of HIPA. Including an explanation of the need-to-know principle (and the data minimization principle) would serve as a helpful reminder of how employees can comply with HIPA.

iii. Confidentiality Statement

[159] When RQRHA employees sign on to the RQRHA network, a *Confidentiality Statement* appears as a prompt on the screen. Employees have to click on the "OK" button to continue with their use of the RQRHA network. The *Confidentiality Statement* reads as follows:

> The Regina Qu'Appelle Health Region recognizes its obligation to respect privacy and is committed to maintaining the confidentiality of client/patient and Region information, whether written, verbal or electronic.
>
> As part of your association with the region, you have authority to access certain information. This access is limited and strictly confined to information that is required for the performance of your duties.
>
> An intentional breach of confidentiality will result in disciplinary action.

[160] As I understand it, RQRHA employees receive privacy and security training prior to acquiring access to the RQRHA network. The above appears to be a reminder of the privacy training employees have received.

[161] However, it appears that Employee B had side-stepped the *Confidentiality Statement* by using other employees' user identification when the other employees left their computers unlocked and unattended. Based on this case, it is difficult to gauge the effectiveness of the *Confidentiality Statement*.

[162] In the case involving Employee C, she signed onto the RQRHA Network with her own user identification. Therefore, she would have to come across the *Confidentiality Statement* before viewing others' personal health information. Based on her actions of accessing patient personal health information without a need-to-know, the *Confidentiality Statement* may not be as effective as it was intended to be.

[163] Since it appears that the *Confidentiality Statement* makes reference of the privacy training employees receive, I will now consider what that training achieves.

iv. Training

[164] In a letter dated September 14, 2009, RQRHA stated that it had provided "formal re-education sessions" to all staff in the HIMS department after it discovered staff viewed their coworker's personal health information on the Enovation system. Our office requested a copy of material used for the formal re-education session. Enclosed with its November 3, 2011 letter, RQRHA provided my office with a copy of the power point presentation entitled *HIPA, Health Information Protection Act*.[68]

[165] Slide #10 of the power point presentation states as follows:

[68]RQRHA, *HIPA, Health Information Protection Act* power point slides. Undated.

Rights of Individuals

The Right:

- To consent to the use & disclosure of their [personal health information] (*deemed consent)*
- To revoke consent to collection, use, or disclosure of [personal health information]
- To access their [personal health information]
- To be informed about how their [personal health information] will be collected, used & disclosed.[69]

[166] In a letter dated March 23, 2012, I provided the following comments on the above slide:

> Slide #10 "Right of Individual" misrepresents the situation. "Deemed consent" is actually *no consent*. **Someone learning from your slides would easily conclude that a fundamental element of HIPA is not to consult the patient but rather to rely on "deemed consent" for virtually all health service related transactions.** I encourage you to consider the following:
>
> (a) The approach to consent has changed significantly since HIPA was enacted. The Pan-Canadian Health Information Privacy and Confidentiality Framework, although never formally adopted by SK, has been accepted as the basis for harmonizing all provinces and territories approaches to [personal health information]. The Framework makes "implied consent" the national standard and the other provinces with No Consent features (Alberta and Manitoba) agreed to move to that standard of "implied consent". Saskatchewan, notwithstanding HIPA and section 27(2), has adopted implied consent as the standard for the EHRi.
>
> (b) HIPA actually provides for three different forms of "consent" (express, implied and deemed). Although the early materials from Saskatchewan Health focused only on deemed consent, this was inaccurate and confusing and led to a lack of clarity between "implied consent" and "deemed consent". I refer you to our *Glossary of Common Terms – HIPA* that indicates a set of cascading thresholds that your RHA staff need to understand. You can find the *Glossary of Common Terms – HIPA* on our website, www.oipc.sk.ca, under the "Resources" tab.
>
> (c) The Patient First initiative in this province is clearly offended by indiscriminate use of "deemed consent" or no consent. In other words, fundamental to a patient-first health care system is the requirement that wherever possible the patient should be consulted as to their wishes. Deemed consent disempowers that patient and flies in the face of the new patient-first policy of the Saskatchewan Government. Clearly there will be emergency situations arising

[69] *Ibid.* at slide 10.

> often in the Emergency Department of an acute care hospital or intensive care wards that would provide ample reason to rely on "deemed consent". Most health care transactions however would not justify ignoring the patient's wishes.
>
> [emphasis added]

[167] Further, since deemed consent means no consent the individual cannot revoke his/her consent. However, the slide states that deemed consent is revocable. That is inaccurate. The individual is disempowered when it comes to the control of his/her personal health information when deemed consent is relied upon.

[168] Slide #13 of the power point slides provides as follows:

> **Use of Personal Health Information**
>
> - Must be used for the purposes it was collected for unless consent has been given by the individual.
> - **May be used and shared, as required, within the "Circle of Care".**
> - Consent is deemed to exist.[70]
>
> [emphasis added]

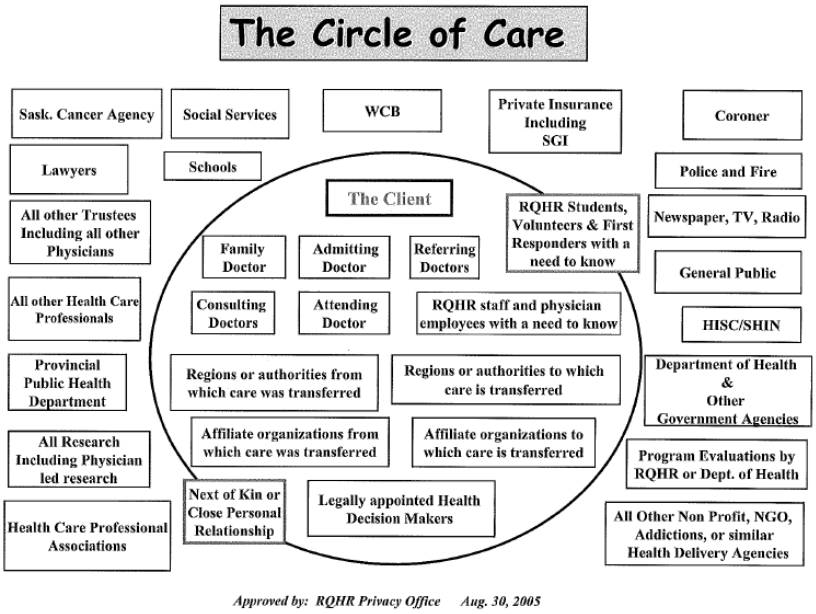
[169] I provided the following comments to RQRHA about the term circle of care in my letter dated March 23, 2012 to RQRHA:

> Slide #13 "Use of Personal Health Information" includes the phrase "Circle of Care". This term does not appear in HIPA. In the past it may have been useful in explaining to the general public some basic information about [personal health information] sharing. **It is most unhelpful however when training contemporary health care workers who need a more sophisticated understanding of the rules for [personal health information] sharing. In eight plus years of experience with HIPA, our office has found that this term is not well understood, is at odds with section 23 and the requirement that anyone who gets to view or use the [personal health information] of a patient must have a legitimate 'need-to-know' that [personal health information]. It almost invariably leads to a much larger cohort of health care workers believing they are somehow entitled to view the [personal health information] of a patient than would the cohort of those who have a legitimate need to know.** Please review our discussion of this in the *Glossary of Common Terms – HIPA* and the other resources where we have considered 'circle of care'.

[70] *Ibid.* at slide 13.

[emphasis added]

[170] Slide #14 is a depiction of the Circle of Care diagram: [71]



[171] The above diagram is confusing; any person can potentially be within the circle, on the edge of the circle, or outside of the circle. How does one person know if he or she is in the circle? As I had said earlier, circle of care's focus is whether a person is a member of 'the club' when the focus should be on the patient and the particular health care transaction in question.

[172] This office frequently hears from health care workers that they and many of their colleagues have great difficulty determining who is in the circle of care and who is not. One need only consider the Circle of Care diagram dated August 30, 2005 to understand why.

[173] Why is it only RQRHA students, volunteers, first responders, RQRHA staff and physician employees who must have a "need-to-know" to be in the so called circle of

[71] *Ibid.* at slide 14.

care? The implication from the diagram is that anyone in "Regions or authorities to which care is transferred", "regions or authorities from which care was transferred", "affiliate organizations from which care was transferred" and "affiliate organizations to which care is transferred" is not required to possess a need-to-know. Further, regional health authorities may have hundreds or thousands of employees. The circle of care diagram states that potentially hundreds or thousands of employees without a need-to-know are within a patient's circle of care.

[174] This kind of diagram makes impossibly complicated a simple proposition: anyone who is engaged in continuing care for a patient, regardless of whether they qualify as a trustee for purposes of section 2(t) of HIPA, may have a need-to-know at least some of the personal health information to keep a patient safe and provide continuing care.

[175] My office offered the following comments on Slide #14 in my letter dated March 23, 2012:

> Slide #14 "The Circle of Care" slide persists in putting the focus on the health care worker and 'membership' in the 'club' rather than on the needs of the patient. I have yet to see any value added by using any phrase other than "need to know", which is explicitly included in HIPA. But we see plenty of confusion as a [sic] trustees and their staff fail to understand that need to know is entirely variable and will usually be different for every single health care transaction and for every different patient i.e. the specialist who say [sic] the patient for cataract surgery would not have a need to know all of the [personal health information] concerning the patient who presents with a fracture at the hospital emergency the following week. Nonetheless, we all too frequently encounter excessive sharing of [personal health information] because of confusion between need to know and circle of care.

[176] I continue to emphasize that the term need-to-know, a term explicitly used in HIPA, be used rather than circle of care. Need-to-know focuses on the need of the patient. If a health care worker has a legitimate need-to-know a patient's personal health information to fulfill a health care transaction, then he/she may view the personal health information.

[177] Slide #15 of the power point slides states as follows:

The Circle of Care "Test"

- Who **needs to know**?: The individuals providing current health services
- Why do they **need to know**?: The information is required in order for the individual to perform their function in providing services.
- What do they **need to know**?: The minimum information required in order to perform their function.[72]

[emphasis added]

[178] I informed RQRHA in my letter dated March 23, 2012 that the content of slide #15 is appropriate but I question why it is called the "Circle of Care 'Test'" rather than the "Need to Know 'Test'"? The test can be used to apply the need-to-know concept and be in compliance with HIPA.

[179] What is interesting is that the HIPA training DVD that RQRHA uses to train new employees on their privacy responsibilities, the Director, Risk Management (Director) of RQRHA cautions RQRHA employees that the circle of care map (shown in [170]) cannot always be relied upon:

> ...we need to take care when we are relying on [deemed] consent that people understand how we are using their information, how it's being collected, and how it's going to be shared. So it's safe to assume that they approve of how we are sharing information to provide services but they do have to have an understanding of how we are using it, how we are collecting it and how we are sharing it. And so we often look to the circle of care diagram...**it's not always straight forward**, it's meant to be sort of a snapshot. Within the circle, those are normally the types of individuals, types of services where we can rely on deemed consent, where we assume it's okay to share that information by the patient requesting the treatment or service, that they would understand we would share that information with those individuals to provide care to them. So those different organizations or individuals that you see outside of the circle of care, those are the situations where we would normally require express consent. An express consent can mean we need a form signed, sort of a permission slip, consent form or express consent can also mean we've had that discussion with the patient they understand how we are going to share the information and they agree to it and we document it. So either an actual form signed by the patient or documentation there has been discussion and that the patient agrees - that is what we look to for express consent.

[72] *Ibid.* at slide 15.

> Now **there are certain situations where we can't just rely on the circle of care map.** For example, if you look at the map, you can see that the police and fire department normally are considered outside the circle of care but it would be different if they were actually providing a health service. If they're actually at the scene or actually participating in the treatment, participating in care, that would make them a part of the circle of care. **And that's sort of a word of caution about using the circle of care as the gold standard rule all the time. Sometimes situations change and it doesn't describe it perfectly.** And also a person's path of care changes as they move through our system. So just because you were in the circle of care because you were the emergency room nurse looking after the patient yesterday, days later, today, two weeks later, doesn't mean it's okay for the emergency room nurse to ask how the patient is doing, what the outcome of their therapy is, just because they are curious. They're not really included in the circle of care anymore because the patient has moved on through the system.[73]
>
> [emphasis added]

[180] The emergency room nurse example discussed by the Director establishes that the circle of care concept is just an extra step that causes confusion. If she is in the circle of care one day, what is to prompt her to ask herself if she is in the circle of care the next day? The emergency room nurse should only be asking herself whether or not she has a need-to-know the patient's personal health information to fulfill her job duties. If the nurse has a need-to-know to complete a particular health transaction for the patient, then she may view the personal health information. If she does not, then she should not view the personal health information. Deciding whether or not she is in the circle of care is just an extra, unhelpful step.

[181] Further, the Director states, "a person's path of care changes as they move through our system."[74] He provides the example of an emergency room nurse may be in the circle of care initially but may not be later on as the patient moves through the system. The emergency room nurse should not be able to view information about the patient as she will no longer have a need-to-know.

[73]RQRHA, HIPA training DVD at approximately 11:02, September 22, 2010.
[74] *Ibid.* at approximately 13:01.

[182] The three cases discussed in this Report clearly indicate that training based on circle of care is ineffective. It appears Employees A, B, and C assumed they are automatically a part of the circle of care simply by virtue of the fact they are an employee of RQRHA.

[183] In addition to my above comments on the power point slides of RQRHA's formal re-education package, I also made the following recommendations in my letter dated March 23, 2012 to RQRHA as to how it may update its power point slides:

- Explain that the real reason for why HIPA exists is to enable and to facilitate the Electronic Health Record;
- Explain the difference between the terms "custody" and "control";
- Explain the different forms of consent – express, implied, and deemed;
- Explain that Acts listed in section 4 only trump three parts of HIPA; the remaining parts of HIPA continue to apply;
- Explain that all privacy laws including HIPA have a 'safety valve' which allows for the non-consented collection, use or disclosure of personal health information where there is an imminent risk to someone's health or safety; and
- Clarify when health professionals are trustees when they are not, such as when they work in a regional health authority facility; in that event, the only trustee is the regional health authority.

[184] It should be noted that these power point slides are very similar to the power point slides the Director uses in the HIPA training DVD.

[185] In response to my office's recommendations, RQRHA stated the following in its letter dated May 11, 2012:

> We are always striving to ensure the message that is presented to RQHR employees in regards to HIPA is as accurate as possible. I would like to take the opportunity to thank you for including the insightful comments from the Privacy Commissioner on the RQHR's HIPA power point presentation. We will take these comments into consideration when updating our HIPA training materials.

[186] My office asked RQRHA for a timeline as to when it would update the DVD, RQRHA responded on October 10, 2012 by stating: "We are hoping to update the DVD **based on**

> **current RQHR policies and procedures** by the end of this fiscal year." [emphasis added]

[187] As discussed earlier, RQRHA's current policies and procedures are inadequate in addressing the chronic issue of misuse of personal health information stored on the Enovation system and LIS. These three cases where employees viewing and/or altering personal health information without a legitimate need-to-know clearly demonstrates the inadequacy of the current policies and procedures. Without a firm commitment from RQRHA to review and revise its policies, procedures and training material, such cases will predictably remain a chronic issue.

[188] As noted earlier, RQRHA is not planning to remove the term and concept of circle of care from its training materials. It stated in its October 10, 2012 email:

> We continue to educate staff that the Circle of Care is intended as a visual depiction of Section 27(2) of HIPA and that "need to know" is a fundamental component of the circle of care model. While this may be considered in the future, at this time we are not planning to remove the circle of care from our training materials.

[189] Circle of care and need-to-know are two different concepts. Circle of care is a confusing and complicated concept that is not rooted in HIPA. Need-to-know is a straight-forward concept that is explicitly found in section 23 of HIPA.

[190] Given that new employees to RQRHA receive privacy training via the DVD, it is imperative that it contains accurate information about HIPA. Reviewing and revising its policies, procedures and training material would be helpful in minimizing the risk of similar privacy breaches from occurring again.

[191] However, there are commendable aspects to the power point slides and the DVD. The Director does state that employees should not be accessing information they do not require to do their job. For example, he explains that there used to be a culture within RQRHA that it would be considered acceptable to look up "cousin Fred's" chart. However, the Director states that such actions are not permissible. But again, as I stated earlier, the three cases discussed in this Report demonstrate that employees perhaps

assume they are within the circle of care just by being an employee of RQRHA. In all three cases, employees essentially looked up "cousin Fred's" chart without a legitimate need-to-know.

[192] Another administrative safeguard RQRHA has is its *Regina Laboratory Services Safety Quiz* (Quiz). In its May 11, 2012 letter to our office, RQRHA advised us that the Quiz issued to staff contains a question on confidentiality. RQRHA states in its submission to our office: "The Laboratory also has a Laboratory Services Quiz that is sent out quarterly, by alphabetical surname, to its employees which contains a question on confidentiality."

[193] Testing knowledge is an effective way for a trustee to understand if its training has been effective. However, we must note that confidentiality is not the same as privacy. My office's Glossary defines the term "confidentiality" and "privacy" as follows:

> **CONFIDENTIALITY** is the protection of [personal health information] once obtained against improper or unauthorized use or disclosure. This is just one aspect of privacy and is not synonymous with 'privacy.'
> …
>
> **PRIVACY** is a broad concept which involves the right of the individual to exercise a measure of control over his or her [personal health information]. It involves the decision of the individual about what [personal health information] will be disclosed to a trustee and for what purposes. Privacy captures both security and confidentiality which are subsets of privacy.[75]

[194] Confidentiality and privacy, although related concepts, are not the same. Answering a single question about confidentiality on a quiz would not be enough reassurance that employees understand their privacy responsibilities under HIPA. We recommended in my office's letter dated August 10, 2012 that RQRHA design a comprehensive stand-alone quiz about HIPA as part of its orientation for new employees and for any of its on-going education sessions so that RQRHA can be sure that its staff understand their responsibilities under HIPA. Such a quiz should reflect the recommendations my office has made to RQRHA.

[75] *Supra* note 26.

[195] In its September 19, 2012 letter to our office, RQRHA advised my office of the following:

> A quiz has been developed, but has not yet been circulated to RQHR staff. Logistics of how to track which staff have completed the quiz and what to do with staff who may "fail" the quiz are being looked at. There is currently no date set for the implementation of the HIPA quiz.

[196] It is certainly encouraging that a quiz has been developed. It would be a helpful tool for RQRHA to gauge its employees' knowledge of HIPA rather than simply having them passively view a DVD or sign confidentiality agreements. Such testing is necessary since RQRHA had reported that Employee C states that she thought "access without a need to know was okay as long as there was no disclosure".[76] Employee C's accessing of personal health information without a need-to-know is concerning for the following reasons:

1. She had received "confidentiality and security training numerous times and specifically upon transfer to the Lab";[77]

2. She had received HIPA training intended for Laboratory staff in January 2010, eleven months before it was reported to RQHR Privacy Officer that she had accessed personal health information without a need-to-know;

3. She had signed the former *Regina Health District Confidentiality and Security Agreement* where the employee agrees to only access confidential information when they are legally authorized or required to do so;

4. She had signed the *Laboratory Information System Security and Request for Access Form* that requires the staff member to agree "to use the computer system only to perform activities only for which I have been authorized…";[78] and

5. She stated that "everybody does it"[79] in regards to employees accessing personal health information without a need-to-know. Such a statement suggests there may be a culture of accessing personal health information without a need-to-know within the laboratory.

[76] *Supra* note 4.
[77] *Ibid.*
[78] *Ibid.*
[79] *Ibid.*

[197] I encourage RQRHA to investigate whether or not there is a culture of accessing personal health information without a need-to-know within the lab. Given that the privacy breaches involving misuse of personal health information stored in LIS by employees within the laboratory department, as well as another misuse of personal health information in the Enovation system within the HIMS department may be an indication that they are not isolated incidents.

[198] RQRHA responded in its September 19, 2012 letter stating it has started using a software program called *FairWarning* "to monitor unauthorized access of [personal health information]".[80] It advised us that the system is not fully implemented but it is producing audit logs for the RQRHA Privacy Coordinator to review. Proactive auditing, as what it appears RQRHA is doing, is a good measure to detect misuse of personal health information. However, my office was not provided any policies or procedures that guide the review of audit logs. Such a policy and related procedure should exist to guide the review of such audit logs. For example, what would be contained in an audit log that would cause the Privacy Coordinator to investigate whether a privacy breach has occurred? How often are audit logs produced and how often are they reviewed? How are employees informed there are audit logs being produced to tracks their activities and for what purposes? A policy and related procedures that clearly reflects the requirements of HIPA and guides RQRHA in monitoring its employees is of utmost importance in preventing and containing any similar privacy breaches.

[199] In my *2011-2012 Annual Report*, I stated that there is a compelling need for written materials to guide trustee organizations in complying with HIPA.[81] Such written materials include policies, procedures and training materials that accurately reflect the statutory requirements of HIPA, but should be written in such a way that this material is accessible to employees who manage personal health information.

[80]RQRHA letter dated September 19, 2012 to SK OIPC.
[81]SK OIPC *2011-2012 Annual Report* at p. 12, available at www.oipc.sk.ca/Annual%20Reports/Annual%20Report%202011-2012.pdf.

[200] RQRHA should be revising its policies, procedures, and all training materials to accurately reflect the statutory requirements of HIPA. One step towards achieving this would be to eliminate the circle of care concept and focusing on need-to-know.

[201] Finally, accurately written materials are not enough in meeting the requirements of HIPA. The trustee organizations' actual practices must be in compliance with HIPA. In a publication entitled *A Policy is Not Enough: It Must be Reflected in Concrete Practices*[82] by the Ontario Information and Privacy Commissioner, she stated that:

> A privacy policy cannot, by itself, protect personal information held by an organization. Privacy policies that are not reflected in actual practice through strong implementation, training, and auditing will fail to safeguard personal information against privacy risks. But if we return to the true meaning of "policy," we will be reminded that it was always intended to be rooted in action. *The Concise Oxford Dictionary* defines policy as: "a course, or general plan of action adopted or proposed…"[83]

b. What physical safeguards does Regina Qu'Appelle Regional Health Authority have to protect personal health information and are they adequate?

[202] In my Investigation Report H-2005-002, I discussed that appropriate safeguards may include restricted access to physical premises, alarm systems, access codes and keys to enter into buildings.[84]

[203] The power point slides RQRHA provided to my office, that I referenced earlier, *HIPA, Health Information Protection Act*[85], instructs RQRHA employees of the following:

- "Turn the computer screen away from those that do not need to see the info."
- "Place fax machines, files, charts, etc. in secure areas."
- To "dispose of paper containing [personal health information] in locked confidential shredding bins."

[82]Ontario Information and Privacy Commissioner, *A Policy is Not Enough: It Must be Reflected in Concrete Practices*, September 2012, available at www.ipc.on.ca/images/Resources/pbd-policy-not-enough.pdf.
[83]*Ibid.* at p. 1.
[84]*Supra* note 21 at p. 104.
[85]*Supra* note 68.

- To "lock file cabinets, offices and storage areas containing [personal health information]."
- To "practice the 'clean, confidential desk' policy."

[204] The above physical safeguards are important to ensure the inadvertent viewing of personal health information. However, in the case of deliberately abusing one's user privileges to the Enovation system by viewing a co-worker's personal health information within the HIMS department, physical safeguards would have played a minor role in preventing the privacy breach from occurring. For the other two cases where employees abused their user privileges to LIS, physical safeguards would have also played a minimal role in preventing such privacy breaches.

[205] Nonetheless, I recommended that RQRHA still review the adequacy of its physical safeguards. For example, RQRHA should review the role and effects of physical safeguards in the case where employees crowded around a single computer to view their coworker's personal health information. RQRHA should review measures to ensure others, including coworkers without a need-to-know cannot see the personal health information displayed on the computer screen. This can be achieved several different ways including the use of privacy screens that can be mounted onto computer monitors or physically positioning computer monitors so only the user can view the screen.

[206] RQRHA stated in its October 10, 2012 email that my recommendation "is being considered as the work plan is developed" for the RQRHA Privacy Coordinator.

c. What technical safeguards does Regina Qu'Appelle Regional Health Authority have to protect personal health information and are they adequate?

[207] In my Investigation Report H-2005-002, I provide examples of some appropriate technical safeguards:

> On October 19, 2004, our office met with the Agency's systems analyst responsible for technical security features relevant to the Program. We subsequently received a

> good deal of additional information on security features. The technical safeguards utilized by the Agency reflect industry best standards.
>
> Some general features include the following:
>
> - Firewalls.
> - Encrypted transmissions with VPN technology.
> - Use of private keys to decrypt files.
> - Individualized passwords within an inquiry based system limited by user roles.
> - Use of Oracle for backup systems.
> - No access to the server allowed except for domain administrators.
> - Data masks, and
> - Built-in ability for process audits.[86]

[208] Below is discussion of the technical safeguards RQRHA has in place to protect personal health information.

i. Auditing features of the Enovation system

[209] In its letter dated September 14, 2009, RQRHA stated the following about the Enovation system:

> The Enovation system used by the Region does not log access by individuals as is the norm for applications of this generation used in many organizations in Canada. The Region recognizes that this is a limitation of the application and this function is carefully considered when this and other existing applications are evaluated, as well as when new applications are being evaluated and implemented. To mitigate the limitations of the application, the Region has implemented access privilege and control measures as well as education and the implementation of policies and procedures to protect the personal health information of our clients.

[210] During a meeting on May 27, 2010 between RQRHA and my office, RQRHA's Director, Risk Management advised that the Enovation system is a very old system that is no longer vendor supported. However, due to costs, he did not foresee this system being replaced. He stated the system only has the ability to log changes to data but it does not log viewing of data. This, he stated, is a feature lacking in the auditing capabilities. He stated that advanced auditing functions cannot be built into the system.

[86] *Supra* note 21 at pp. 106 to 107.

[211] The efforts made by RQRHA to mitigate the risks due to the limited auditing capabilities of the Enovation system were listed in its letter dated September 14, 2009 to our office. Those included implementing access privilege and control measures, policies and procedures, and educating staff.

[212] Given the inadequacies of the Enovation system and the lack of technical safeguards, focused, accurate and granular training of staff assumes an even larger importance.

[213] My office wrote to RQRHA in a letter dated March 23, 2012 that asked if RQRHA has ever completed a Privacy Impact Assessment (PIA) to review the Enovation system.

[214] In its letter dated May 11, 2012, RQRHA states the following: "The Enovation system was implemented in 1999. A PIA has not been completed. The RQHR does not intend to complete a PIA on this system as it is a legacy system that is being reviewed for replacement."

[215] A PIA is a diagnostic tool designed to help organizations assess their compliance with the privacy requirements of Saskatchewan legislation. PIAs are a tool that is used in other provinces in Canada (and other countries) to help organizations comply with privacy legislation requirements.

[216] The process of completing a PIA requires a thorough analysis of entire systems or projects. A thorough analysis enables the organization to identify risks to privacy and reasonable mitigation measures.

[217] Generally speaking, a PIA documents the purpose of the system or project, what personal information/personal health information that is required for the system or project, the authority for the collection, use, and/or disclosure of personal information/personal health information, and how information will flow within the system or project.

[218] Ideally, PIAs should be completed after the features of the system or project has been determined in principle but before the designing and implementation of the system or project.

[219] In this case, RQRHA has been using the Enovation system since 1999. Completing a PIA at the ideal time is no longer a viable option. However, retroactively completing a PIA would enable the RQRHA to identify the privacy risks that the Enovation system presents. It will also enable RQRHA to evaluate the adequacy of the current mitigation measures it has in place for the lack of auditing capabilities.

[220] PIAs are also living documents. As systems and projects evolve, so should the PIAs. The evolution of systems and projects create new privacy challenges and risks. PIAs should be amended as new privacy challenges and risks arise to ensure that adequate mitigation strategies are put in place to meet such challenges and risks.

[221] The advantage of completing a PIA for the Enovation system, even though it is being reviewed for replacement, is that a PIA will help the design of the new replacement system. Identifying features in the Enovation system that are weak in terms of privacy can help the design in the replacement system.

[222] My office's recommendation to the RQRHA was to complete a PIA for the Enovation system.

[223] In its October 10, 2012 response to my office, RQRHA stated that the recommendation is being considered for RQRHA Privacy Coordinator's work plan that would be finalized by November 2012 but it made no firm commitment that such a PIA would be done for the Enovation system.

ii. Auditing features of LIS

[224] It appears that RQRHA has a measure of auditing capabilities for LIS based on its internal investigation report dated November 9, 2009[87] for the privacy breach involving Employee B accessing and modifying the Complainant's personal health information. It was able to conduct an audit and determine that the Complainant's personal health information was changed eight times under seven different MLA user identifications.

[225] In their internal investigation report dated November 9, 2009, RQRHA made the recommendation that: "The LIS manager will create automated audits in the LIS system (i.e. to track same name queries, etc.)."

[226] Further auditing capabilities are apparent based on the internal investigation report dated February 11, 2011[88] where Employee C viewed her own personal health information, the Complainant's personal health information and the family members' personal health information. RQRHA used its auditing capability in LIS to come to such a conclusion.

[227] One of the conclusions in RQRHA's internal investigation report dated February 11, 2011 is as follows: "Lack of proactive monitoring of employee activity in the LIS allowed the deviant activity."[89]

[228] In response to such a conclusion, RQRHA made a recommendation in its internal investigation report dated February 11, 2011 that:

> Use of the "Fair Warning" Information Technology solution (which has been purchased for use in the RQHR) will be investigated further to determine it's [sic] potential as an investigative tool as well as system of proactive monitoring of electronic systems including personal information and personal health information.[90]

[87] *Supra* note 2.
[88] *Supra* note 4.
[89] *Ibid.*
[90] *Ibid.*

[229] RQRHA provided us with an update on the status of the implementation of the *FairWarning* system in its letter to our office dated May 11, 2012. It stated:

> The RQHR Privacy Office has formed an auditing/monitoring working group of stakeholders to oversee the development and implementation of the auditing/monitoring program through use of the FairWarning system. This group will review existing auditing/monitoring capabilities of all RQHR systems, including those that will not send audit logs into the FairWarning application. The group will determine what system audit log events will be monitored and what actions will be taken based on the system audit log generated.

[230] Implementing features such as an auditing system such as the *FairWarning* system can take a considerable amount of time, especially when integrating it into already existing systems like LIS. However, considering that these two similar privacy breaches occurred within seven months of each other and that it has been nearly three years since we learned of the first privacy breach, my office asked RQRHA in a letter dated August 10, 2012 to provide us with a timeline of when we can expect the *FairWarning* system to be operational.

[231] RQRHA responded to my office in a letter dated September 19, 2012 that *FairWarning* was not implemented to its full potential yet but indicated that audit log reports were being produced by the system and reviewed by the RQRHA Privacy Coordinator.

iii. The 'time-out' feature in LIS

[232] Enclosed with its letter dated May 11, 2012, RQRHA provided my office with a draft copy of its *Information Technology Acceptable Use Procedure*[91] that states as follows:

> 1.14 Users shall lock their workstations or log off all applications and the network whenever the user leaves their workspace for an extended period of time.[92]

[233] The privacy breach involving Employee B viewing and modifying the Complainant's personal health information highlights the fact that employees were not manually logging

[91]RQRHA, *Information Technology Acceptable Use Procedure*, Procedure Reference Number: DRAFT 400.0.1.1 V 4.0. Undated.
[92]*Ibid.*

off their user profile when they left a computer unattended. They were relying on the time-out feature where the computer automatically logs off the user after a period of inactivity. However, it appears that the period of inactivity before the time-out feature activates was too long. Employee B was able to use other employees' user identifications to make changes to his co-worker's personal health information in LIS before the time-out feature logged off the user.

[234] The International Organization for Standardization (ISO) recommends that computer systems should have a session time-out feature. It states as follows:

> **11.5.5 Session time-out**
>
> Control
> Inactive sessions should shut down after a defined period of inactivity.
>
> Implementation guidance
> A time-out facility should clear the session screen and also, possibly later, close both application and network sessions after a defined period of inactivity. **The time-out delay should reflect the security risks of the area, the classification of the information being handled and the applications being used, and the risks related to the users of the equipment.**
>
> A limited form of time-out facility can be provided for some systems, which clears the screen and prevents unauthorized access but does not close down the application or network sessions.
>
> Other information
>
> This control is particularly important tin high risk locations, which include public or external areas outside the organization`s security management. The sessions should be shut down to prevent access by unauthorized persons and denial of service attacks.[93]
>
> [emphasis added]

[235] Considering that employees of trustee organizations could perhaps be the biggest threat to data security and the fact that electronic information systems within RQRHA contain

[93]ISO Standards, *Information Technology – Security Techniques – Code of practice for information security management, International Standard* ISO/IEC 17799, (2005) at p. 72.

personal health information, the time-out feature should log off the user after a very short period of inactivity.

[236] RQRHA advised us in an enclosure dated September 21, 2011 (that was sent to us in a letter dated November 3, 2011) that the manager of LIS had decreased the time it takes for the time-out feature to log off the user. Further, in its letter to us dated May 11, 2012, RQRHA advised us that it informs its employees during its lab orientation sessions, that new lab staff attend, that the preferred method is manually logging off.

[237] In our letter dated August 10, 2012 to RQRHA, we recommended that RQRHA:

1. formalize the "Information Acceptable Use Procedure";

2. that it not only informs staff to log off manually during Laboratory orientation sessions but that it remind staff on a regular basis, whether it be through staff meetings or through the on-going privacy education sessions that RQHR provides to its staff; and

3. signs be posted near computer work stations reminding staff to manually log-off their user identifications when they are not at the computer work station.

[238] In its email dated October 10, 2012, RQRHA stated the following in regards to the above recommendations:

> The Information Technology department has started the internal review and approval process with the RQHR Senior Management Team for this procedure. It is expected that approval will be granted prior to the end of this fiscal year.

[239] Further, it stated in its September 19, 2012 letter that it sent a *Privacy Alert* to LIS users about manually logging off of work stations and that it would provide such instructions as part of future privacy education sessions.

[240] In the Postscript of my Investigation Report H-2010-001, which I have already quoted earlier, employees of trustee organizations can pose a major threat to the integrity of personal health information stored in electronic information systems. Trustee organizations must have sufficient technical safeguards to protect personal health

information from reasonably anticipated threats or hazards to the security or integrity of the information.[94]

V FINDINGS

[241] I find that the viewing and modification of personal health information is a "use" of personal health information under *The Health Information Protection Act*.

[242] I find that the requirements for "use" of personal health information under *The Health Information Protection Act* were not satisfied by Regina Qu'Appelle Regional Health Authority.

[243] I find that the administrative safeguards Regina Qu'Appelle Regional Health Authority have in place are inadequate.

[244] I find that the physical safeguards Regina Qu'Appelle Regional Health Authority did not play a major role in contributing to or preventing the privacy breaches that occurred in each of the three cases.

[245] I find that the technical safeguards Regina Qu'Appelle Regional Health Authority have in place are inadequate.

VI RECOMMENDATIONS

[246] I recommend that Regina Qu'Appelle Regional Health Authority review and revise its administrative, physical and technical safeguards within 120 days in an effort to prevent similar privacy breaches from occurring in the future.

[94] *Supra* note 24.

[247] I recommend that Regina Qu'Appelle Regional Health Authority revise its *Privacy Violations – Recommended Actions for Employees Draft Jan '11* document to merge Levels II and III.

[248] I recommend that Regina Qu'Appelle Regional Health Authority completely eliminate 'circle of care' from all materials, tools and resources and substitute 'need-to-know' as the operative rule.

[249] I recommend that Regina Qu'Appelle Regional Health Authority implement a policy that addresses the issue of employees viewing and modifying their own personal health information within Regina Qu'Appelle Regional Health Authority information systems in question immediately.

[250] I recommend that Regina Qu'Appelle Regional Health Authority complete a privacy impact assessment for the Enovation system so that it may identify and address the privacy weaknesses of the system, and consider all possible mitigation strategies for the indefinite period that the system continues in use.

Dated at Regina, in the Province of Saskatchewan, this 1st day of February, 2013.

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