SASKATCHEWAN

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

INVESTIGATION REPORT H-2014-001

Dr. Gary Hunter (Lakeview Neurology), Five Hills Regional Health Authority, Prince Albert Parkland Regional Health Authority, Prairie North Regional Health Authority, Saskatoon Regional Health Authority, Heartland Regional Health Authority, Sunrise Regional Health Authority, Mamawetan Churchill Regional Health Authority, Regina Qu'Appelle Regional Health Authority, Dr. T.W. Wilson

JANUARY 9, 2014

Statutes Cited: *The Health Information Protection Act*, S.S. 1999, c. H-0.021, ss. 2(h), 2(j), 2(m), 2(m)(i), 2(m)(ii), 2(m)(iv)(A), 2(m)(v), 2(q), 2(t), 2(t)(i), 2(t)(ii), 2(t)(xii)(A), 16, 16(a), 18, 18(2), 18.1, 23, 23(2), 27, 27(1), 28, 29, 42(1)(c), 46, 52(b), 52(d), 52(e), 53; *The Freedom of Information and Protection of Privacy Act*, S.S. 1990-91, c. F-22.01, s. 2(1)(d); *The Freedom of Information and Protection of Privacy Regulations*, c. F-22.01 Reg. 1, s. 3, Part I of the Appendix; *The Medical Profession Act, 1981*, S.S. 1980-81, c. M-10.1, s. 28.

Authorities Cited: Saskatchewan OIPC Investigation Reports F-2013-003, H-2013-003, H-2013-002, H-2013-001, H-2011-001, H-2010-001, H-2005-002, *Report on Systemic Issues with Faxing Personal Health Information.*

Other Sources Cited: Saskatchewan OIPC: *Helpful Tips: Privacy Breach Guidelines, Helpful Tips: Privacy Considerations - Faxing Personal Information and Personal Health Information*; SK OIPC & Ministry of Health: *Checklist for Trustees: Misdirected Faxes*; eHealth Saskatchewan: *Empowering patients. Enabling Care*; Ministry of Health: *Enabling the Provincial Electronic Health Record (EHR) Strategy: RIS-PACS-Archive (Diagnostic Imaging), Diagnostic Imaging – Projects: Picture Archiving & Communications System (PACS)*; COACH: Canada's Health Informatics Association: *Putting it into Practice: Privacy and Security for Healthcare Providers Implementing Electronic Medical Records (2013 Guidelines for the Protection of Health Information Special Edition)*; Office of the Privacy Commissioner of Canada: *Fact Sheets: Faxing personal information*; Alberta IPC: *Guidelines on Facsimile Transmission*; British Columbia IPC: *Faxing and Emailing Personal Information*; Manitoba Ombudsman: *Manitoba Ombudsman Practice Note: Privacy Considerations for Faxing Personal and Personal Health Information*; *The Star Phoenix*, "Wrong fax numbers faulted for test mix-up" (June 28, 2012), "Pharmacists warned about faxed prescription problems" (February 28, 2011); *Lloydminster Source*, "Sask. Addressing diagnostic imaging distribution" (July 18, 2013); *Times Colonist*, "Privacy office to probe medical files breach; Patient information was faxed to roofing business" (March 3, 2011); *The Canadian Press*, "Alberta privacy commissioner calls mounting reports of lost data 'startling'" (August 24, 2011); *The Vancouver Sun*, "Private medical records faxed to auto shop; John VanVeldhuizen says his number is similar to local clinic's where the faxes are supposed to go" (January 30 2013); *Daily Mail*, "NHS loses track of 1.8m patient records in a year; Files dumped in bins and put up for sale online" (October 29, 2012); *The Telegraph Online*, "Private data fears 'hindering progress' in NHS" (April 25, 2013); *The Press*, "Medical notes sent in error; Health records faxed to wrong number" (August 1, 2011); *CBC Saskatoon* online, "Confidential medical records faxed to Sask. School" (September 16, 2013).

EXECUTIVE SUMMARY

In 2010 I learned that faxing personal health information was a particular risk area that was receiving inadequate attention from Saskatchewan trustees. I undertook a systemic investigation that reviewed the circumstances surrounding 60 misdirected faxes from 31 trustees. I was surprised to learn how poorly many of these trustees had prepared to avoid and reduce the risk of misdirected faxes which exposed individuals' personal health information to persons who had no legitimate need-to-know that information. I produced my *Report on Systemic Issues with Faxing Personal Health Information* (2010 Report) dated November 23, 2010 with the hope that all regional health authorities (RHAs), physician offices and pharmacies would take prompt action to improve their policy and procedures. In the 2010 report, I provided very detailed information on how trustees could improve their privacy compliance. The 2010 Report was posted to my office's website and through the Network of Inter-Professional Regulatory Organizations and communication with the larger health profession regulatory bodies we reinforced the need for all trustees to pay particular attention to faxing practices. Given my office's experience in 2013 with fax related privacy breaches detailed in the within the current Investigation Report, it appears that my optimism based on the 2010 Report recommendations may have been misplaced.

In discussions with trustees about our recommendations from the 2010 Report, I often heard that the problems I had identified were specific to fax machines and that as we moved to electronic medical records and the provincial electronic health record, the problem with misdirected faxes should be short lived.

This 2014 Investigation Report again takes a systematic approach in examining several privacy breaches involving misdirected faxes. In total, this investigation captures 10 different trustees, including 8 RHAs, 20 separate files and approximately 1000 affected patients. With a couple of exceptions, all of these breaches involve not a stand-alone fax machine but rather faxing features with electronic medical records and the electronic health record.

The breaches can be broken down into five categories of breaches:

> Category #1 – (338 to 922 possible affected patients, seven trustees): Outdated physician fax numbers in the Radiology Information System (RIS) caused faxes containing personal health information to be misdirected to those without a need-to-know. eHealth Saskatchewan is the Information Management Service Provider (IMSP) which provides RIS support to the trustees.
>
> Category #2 – (seven affected patients, seven trustees): A third party in Moose Jaw received several faxes for physicians no longer providing services for the organization. These breaches can be attributed to a number of different factors including out of date fax numbers in electronic medical records (EMRs); undue care and attention when entering information, choosing where to send faxes and use of an 'auto suggest function'; and reliance on outdated personal health information in a legacy system.
>
> Category #3 – (three affected patients, two trustees): An incorrect fax number in the College of Physicians and Surgeons of Saskatchewan's (CPSS) *Physicians Mailing List – January 2013* and undue attention paid to subsequent updates caused these faxes containing personal health information to be sent to a third party school. Further, in one case, highly sensitive personal health information regarding a transgendered individual was sent to the wrong recipient via this inherently insecure form of communication.

Category #4 – (Approximately 125 affected patients, three trustees): Another series of breaches involving RIS in which a configuration would not allow changes or updates to patient personal health information affecting where results were faxed.

Category #5 – (22 affected patients, one trustee): These breaches involved an incorrect fax number which was entered into RIS.

This 2014 Investigation Report examines not only the root causes of the breaches in detail, but also evaluates the responses of each trustee to the breaches and the faxing safeguards each one had in place before the breaches occurred. For these purposes, I revisited the 2010 Report.

As a result of this investigation, I identified two common themes that were consistent in these breaches: challenges with keeping fax information up-to-date and a lack of formal mechanisms to ensure that appropriate safeguards and accountability mechanisms are integrated in the RIS setup. This includes a lack of formal agreements between eHealth Saskatchewan and the seven RHAs involved in this Investigation Report that presently use RIS.

Among my 16 recommendations, I advised trustees to:

- disable 'auto-suggest' features within its electronic systems if such a technical solution is possible;
- develop consistent privacy breach investigation protocol in accordance with the Office of the Information and Privacy Commissioner's resource: *Helpful Tips: Privacy Breach Guidelines* and consistently follow such a protocol, even if its information management service provider may also be investigating the same issue;
- develop comprehensive and specific faxing policies and procedures tailored to its organization;
- develop a procedure that all copies of the College of Physicians and Surgeons of Saskatchewan physician directory be manually updated in ink immediately when monthly notifications are received;
- devise strategies and corresponding policies and procedures to audit and update all sources of fax contact information regularly;
- work with eHealth Saskatchewan to verify relevant fax numbers within the system immediately and on an annual basis;
- work with eHealth Saskatchewan and other regional health authorities to devise a strategy for updating fax information within the system. The regional health authorities must then develop internal procedures that complement the strategy;
- ensure there are adequate and up-to-date agreements in place with eHealth Saskatchewan concerning the use of RIS;
- ensure a cover sheet compliant with best practices accompanies faxes sent from this system; and
- verify that faxes sent from all machines and other sources print a fax header that is compliant with best practices.

Contrary to the suggestions in 2010 that faxing problems would be eliminated with the expanded use of electronic medical records, and the provincial electronic health record, my experience is that inadequate policy, procedures and lack of training renders even these new technologies susceptible to the same kinds of problems experienced with the more primitive fax machine.

This page left blank intentionally.

TABLE OF CONTENTS

I BACKGROUND

[1] In July of 2012, my office was advised of a problem with the Saskatchewan Radiology Information System (RIS) that resulted in a number misdirected facsimiles (misdirected faxes) originating from eight regional health authorities (RHAs). In late 2012 and over the first 7 months of 2013, my office was alerted to several more privacy breaches involving misdirected faxes containing personal health information of identifiable individuals, all constituting a contravention of *The Health Information Protection Act* (HIPA)[1]. In total, these breaches involved between 495 and 1079 patients and ten different trustees. They can be grouped into the following five categories:

- Category #1: Faxes involving RIS (2012)
- Category #2: Faxes sent to a third party in Moose Jaw
- Category #3: Faxes sent to a third party school
- Category #4: Faxes involving a configuration in RIS
- Category #5: Faxes involving an error in updating provider information in RIS

Category #1: Faxes involving RIS (2012)

039/2013-HIPA/BP	Saskatoon Regional Health Authority (SRHA)
040/2013-HIPA/BP	Prince Albert Parkland Regional Health Authority (PAPRHA)
042/2013-HIPA/BP	Five Hills Regional Health Authority (FHRHA)
043/2013-HIPA/BP	Heartland Regional Health Authority (HRHA)
044/2013-HIPA/BP	Prairie North Regional Health Authority (PNRHA)
045/2013-HIPA/BP	Sunrise Regional Health Authority (Sunrise)
046/2013-HIPA/BP	Mamawetan Churchill Regional Health Authority (MCRRHA)

[2] An article entitled "Wrong fax numbers faulted for test mix-up"[2] appearing in Saskatoon's *The Star Phoenix* on June 28, 2012 indicated eHealth Saskatchewan was investigating misdirected faxes that occurred with diagnostic imaging tests from RIS.

[3] eHealth Saskatchewan contacted my office on July 3, 2012 to alert us to the situation. It indicated that its primary focus was to ensure personal health information reached the

[1] *The Health Information Protection Act*, S.S. 1999, c. H-0.021 (hereinafter HIPA).
[2] "Wrong fax numbers faulted for test mix-up," *The Star Phoenix*, June 28, 2012 at p. A2.

appropriate providers. In due course, it would provide my office with more details about the breach.

[4] On July 5, 2013, eHealth Saskatchewan reported that eight RHAs were involved. My office opened a preliminary file to monitor the situation. My office informed eHealth Saskatchewan that once I received its report on the matter I would then decide if opening files with each of the trustees was warranted.

[5] On July 30, 2012, eHealth Saskatchewan provided me with a brief update as well as sample notification letters for affected individuals.

[6] Having not received anything more from eHealth Saskatchewan, my office asked for an update on April 29, 2013. A brief update was provided on April 30, 2013, with additional information provided on May 3, 2013 and June 21, 2013. A formal investigation report had not yet been provided by eHealth Saskatchewan.

[7] On July 3, 2013, I made the decision to open formal investigation files for this matter. As it appeared eHealth Saskatchewan's role was that of an information management service provider (IMSP), my office sent notification letters to the eight responsible trustees dated July 3, 2013. We asked for internal investigation reports from each of the RHAs no later than August 30, 2013.

[8] We received an investigation report from eHealth Saskatchewan on July 19, 2013. As of August 30, 2013, we had not received reports from SRHA, FHRHA and HRHA. Further, PAPRHA simply sent a letter referring to eHealth Saskatchewan's Investigation Report. My office sent another letter requesting a submission by September 20, 2013 from those RHAs.

[9] As a result of new information from one of the RHAs, we were able to conclude that it did not have any misdirected faxes and it will not be included in this Investigation Report. As such, only seven RHAs are involved in the Category #1 breaches.

[10] On October 18, 2013, eHealth Saskatchewan and the RHAs indicated that the following number of patients were involved per RHA in this breach:

	Number of Patients	
RHA	**Estimate of eHealth Saskatchewan**	**Estimate of RHA**
SRHA	179	679 patients were investigated but no final number of actual breaches provided.
PAPRHA	41	Reports only 20 patients affected but claims no breaches occurred as personal health information reached the correct trustee. Provided no explanation for the discrepancy in number or this conclusion.
FHRHA	4	Reports only 3 misdirected faxes sent but claims no breaches occurred as personal health information reached the correct trustee. Provided no explanation for the discrepancy in number or this conclusion. Number of affected patients unknown.
HRHA	2	Identified 4 errant faxes. Number of affected patients unknown.
PNRHA	131	Indicated 191 patients affected.
Sunrise	2	Indicated 2 patients affected.
MCRHA	1	Indicated 1 patient affected.

Total affected patients: between 338 and 922

Category #2: Faxes sent to a third party in Moose Jaw

013/2013-HIPA/BP Dr. Gary Hunter (Lakeview Neurology)
014/2013-HIPA/BP FHRHA
015/2013-HIPA/BP PAPRHA
034/2013-HIPA/BP PNRHA
057/2013-HIPA/BP PAPRHA
058/2013-HIPA/BP Anonymous Health Region
059/2013-HIPA/BP Regina Qu'Appelle Regional Health Authority (RQRHA)

[11] On October 11, 2012, my office received a phone call from a third party in Moose Jaw. This third party is an organization that provides limited health care services for a specific population and does not appear to qualify as a trustee for the purposes of section 2(t) of

HIPA. However, several physicians from Saskatchewan have provided services for this organization.

[12] The third party informed my office that it had been receiving several faxes containing personal health information for which it did not have a need-to-know. The faxes came from several trustees. It advised us that it had contacted each of the trustees to notify them of the error, but was not satisfied with their responses.

[13] My office advised the third party to send us the original faxes and not keep copies. We received the misdirected faxes in question from the third party on the following dates: October 24, 2012, November 9, 2012, December 28, 2012, May 27, 2013 and July 5, 2013. We subsequently provided to each trustee notification of an investigation by our office and asked for an internal investigation report.

Trustee	File	Date Faxes received by Third Party	Number of Affected Patients
Dr. Gary Hunter (Lakeview Neurology)	013/2013-HIPA/BP	October 22, 2012 December 12, 2012	1
FHRHA	014/2013-HIPA/BP	October 4, 2012	1
PAPRHA	015/2013-HIPA/BP	October 10, 2012	1
PNRHA	034/2013-HIPA/BP	May 6, 2013	1
PAPRHA	057/2013-HIPA/BP	June 22, 2013	1
Anonymous	058/2013-HIPA/BP	June 3, 2013	1
RQRHA	059/2013-HIPA/BP	June 26, 2013	1

Total affected patients: 7

[14] The fax in question for File 058/2013-HIPA/BP is a graph that appears to capture an identifiable individual's sinus rhythm. It is clear the graph was prepared at a certain hospital in an RHA I will not identify. However, it is unclear if the header on the document qualifies as a fax header or was simply part of the document. No fax number is listed. Finally, no cover page accompanied it. The RHA contended that it was not responsible for sending the fax. After corresponding with this RHA on this file, I came to the conclusion that there was a reasonable possibility that the fax was not sent by that

RHA. There is no other evidence to suggest who may have sent the fax to the third party in Moose Jaw.

Category #3: Faxes sent to a third party school

047/2013-HIPA/BP SRHA
060/2013-HIPA/BP Dr. T.W. Wilson

[15] On May 21, 2013, my office received a phone call from a principal at a school in Saskatchewan. The principal reported that the school fax machine had been receiving numerous faxes containing personal health information in which it did not have a need-to-know. The principal advised that the faxes were coming from several sources. My office advised the principal to contact the sender of each fax to let them know of the error. We also asked that he send us original copies of the faxes so we could launch an investigation.

[16] On May 30, 2013, my office received from the principal two of the misdirected faxes the school received on May 10, 2013 and May 22, 2013. On June 14, 2013, we received by mail another fax that the school had received on June 6, 2013.

[17] It appeared that all three of the faxes originated from SRHA. My office provided a notification letter to SRHA on June 26, 2013 with de-identified copies of the faxes asking for verification that they had been sent from the RHA.

[18] On July 8, 2013, SRHA informed my office that it was not the trustee of the personal health information in the fax dated June 6, 2013. It informed us that the personal health information originated from Dr. T. W. Wilson, a separate trustee whose office was housed at the Royal University Hospital, a facility of SRHA. We provided a notification letter to Dr. Wilson dated July 9, 2013. I note that the fax dated June 6, 2013 contained particularly sensitive personal health information as it detailed hormone therapy of a transgendered individual.

[19] We received representation from SRHA dated July 31, 2013 and from Dr. Wilson dated July 15, 2013 and July 31, 2013 respectfully.

Total affected patients: 3

Category #4: Faxes involving a configuration in RIS

072/2013-HIPA/BP PAPRHA
073/2013-HIPA/BP HRHA
075/2013-HIPA/BP SRHA

[20] My office was made aware of more disclosures of personal health information originating from RIS by an article that appeared in the *Lloydminster Source* on July 18, 2013 entitled "Sask. Addressing diagnostic imaging distribution". The article reported:

> eHealth Saskatchewan has identified and corrected a setting in an electronic distribution system in four health regions that automatically faxes diagnostic imaging results to physicians. The settings, based on regional preferences, were sending diagnostic imaging results to the original ordering physician entered and would not allow an update to redirect results if a correction was made.[3]

[21] My office contacted eHealth Saskatchewan to ask for more details about this article. On the same day, eHealth Saskatchewan provided some information and informed us that it was working with the RHAs in question to investigate the matter. It appeared that, again, these faxes originated from RIS. My office asked that it keep us updated.

[22] On August 13, 2013 my office contacted eHealth Saskatchewan for an update. eHealth Saskatchewan reported that PAPRHA, HRHA and SRHA were in fact involved. It reported the following number of misdirected faxes, however qualified that SRHA was still investigating.

[3] "Sask. Addressing diagnostic imaging distribution," *Lloydminster Source*, July 18, 2013 at p. A14.

	Number of Misdirected Faxes	
RHA	**Estimate of faxes by eHealth Saskatchewan**	**Number confirmed by RHA**
SRHA	180 potential faxes	111 faxes confirmed by SRHA. Number of affected patients unknown.
PAPRHA	12	12 faxes. Number of affected patients unknown.
HRHA	2	2 faxes. Number of affected patients unknown.

Total affected patients: Approximately 125

[23] My office sent notification letters to these three RHAs dated August 20, 2013.

[24] We received a response from each of the RHAs in question and my office also corresponded with eHealth Saskatchewan about the breach as it involved RIS.

Category #5: Faxes involving an error in updating provider information in RIS

077/2013-HIPA/BP PNRHA

[25] On September 18, 2013, I was contacted by eHealth Saskatchewan on behalf of PNRHA to report a breach involving RIS. eHealth Saskatchewan indicated that it had made an error when updating a provider fax number in RIS at the request of an RHA. This resulted in 23 misdirected faxes originated from PNRHA affecting 22 individuals.

Total affected patients: 22

2010 Report on Systemic Issues with Faxing Personal Health Information

[26] In 2010, I released a *Report on Systemic Issues with Faxing Personal Health Information* (the 2010 Report).[4] My office was alerted in April 2009 that a private business was receiving, by fax, the personal health information of a number of individuals. The faxes were sent by pharmacies, physicians, RHAs and other health care organizations in

[4]Saskatchewan Information and Privacy Commissioner (hereinafter SK OIPC), *Report on Systemic Issues with Faxing Personal Health Information* (hereinafter 2010 Report), available at www.oipc.sk.ca/resources.htm.

Saskatchewan – 60 faxes were sent by 31 trustees. Those faxes were intended for a medical clinic, the ownership of which had been dissolved. The fax number for those physicians continuing to practice together was changed. The original fax number for that medical clinic had been out of service for 17 months before it was reassigned to the private business.

[27] The 2010 Report examined each trustee's written policies and procedures regarding faxing personal health information, which is required by section 16 of HIPA. Each of the trustees' policies and procedures were graded on a score of 38.

[28] This Investigation Report will revisit these grading criteria in relation to faxing policies and procedures from the 2010 Report.

[29] In the 2010 Report, I did not identify the individual trustees involved in that investigation. I made this decision for several reasons. If it had not been for one RHA, my office may never have become aware of the problem. We do not usually issue a formal report when a trustee self-reports a breach to my office if it is given due attention by the responsible trustee. Given the scope of the identified problems related to fax transmissions, I concluded that this pointed to a much larger systemic problem than just the 31 trustees we were dealing with. Since bringing this matter to the attention of the others, many trustees had taken remedial action to help prevent a future occurrence. I was also mindful that most of the trustees in question have notified the affected individuals and my office had not received any complaints from those individuals.

[30] However, as a result of the 2010 Report, trustees in this province have been made aware of the need for effective section 16 written policies and procedures for faxing personal health information. It is disappointing that more trustees have not taken appropriate steps to prevent these kinds of breaches involving faxing personal health information.

[31] As such, in the current situation, I will identify the trustees involved in these five categories in this publically issued Report. Also, five of the RHAs that were involved in

the 2010 Report are also involved in one or more of the current breaches. At the time I issued that Report, I advised all trustees that I would approach future privacy breaches involving faxes with "more rigour". I also made the following statement in my 2010 Report:

> Furthermore, the 32 trustees are forewarned to adopt additional policies and procedures to maintain administrative, technical and physical safeguards that will meet the requirements of section 16 of HIPA. I have advised each one that these policies must be in place in the event of any future HIPA violations.[5]

[32] At this time, it is my view that discussing the specific results of the RHAs from the 2010 Report is appropriate.

Investigation Process

[33] When my office began receiving so many reports and complaints about misdirected faxes it became apparent that this was, again, a systematic issue that required attention. I made the decision early to issue this systematic Investigation Report.

[34] Each trustee received a formal notification letter advising of my office's investigation and asking for an internal investigation report. As always, my office's notification advised each trustee of resources to assist them to respond to the privacy breach and report to my office, namely *Helpful Tips: Privacy Breach Guidelines*.[6]

[35] My office completed its analysis and shared a de-identified version with each of the trustees on November 7, 2013. We asked that each trustee advise me of any factual errors and their intentions with respect to my recommendations no later than December 9, 2013.

[36] Normally, when my office reaches this point in an investigation and a trustee signals that it has taken steps to address my recommendations, I would consider the matter concluded and close the file without issuing a formal, public report. However, given the systematic

[5] *Ibid.* at p. 36.
[6] SK OIPC, *Helpful Tips: Privacy Breach Guidelines*, available at www.oipc.sk.ca/resources.htm.

nature of the faxing issues, I made the decision to issue this Investigation Report as it would be the best way to effect change. The trustees were advised of this in letters dated November 7, 2013.

[37] Appendix B provides a brief snapshot of the responses of the trustees with respect to my recommendations. We did not receive a response from FHRHA. Further, Dr. Gary Hunter's (Lakeview Neurology) response was dated November 12, 2013, but was not received by my office until December 19, 2013. It did not contain many details.

II ISSUES

1. Do the misdirected faxes constitute privacy breaches?

2. What circumstances led to each of the breaches?

3. Did each of the trustees involved have written policies and procedures as required by section 16 of *The Health Information Protection Act* and follow best practices for both sending the faxes in question and responding to the breaches?

4. Tying it together: Do common root causes reflect systematic failures on the well established practice of faxing personal health information?

III DISCUSSION OF THE ISSUES

[38] My authority for investigating these matters is found in the following sections 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.
>
> …

46(1) Notwithstanding any other Act or any privilege that is available at law, the commissioner may, in a review, require to be produced and examine any personal health information that is in the custody or control of a trustee.
(2) For the purposes of conducting a review, the commissioner may summon and enforce the appearance of persons before the commissioner and compel them to give oral or written evidence on oath or affirmation and to produce any documents or things that the commissioner considers necessary for a full review, in the same manner and to the same extent as the court.

(3) For the purposes of subsection (2), the commissioner may administer an oath or affirmation.

…

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;

…

(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.

53 The commissioner may:

(a) engage in or commission research into matters affecting the carrying out of the purposes of this Act;

(b) conduct public education programs and provide information concerning this Act and the commissioner's role and activities;

(c) receive representations concerning the operation of this Act.

1. Do the misdirected faxes constitute privacy breaches?

a. Do they contain personal health information?

[39] For the purposes of this investigation, first, I must establish that each of the misdirected faxes qualify as or contain personal health information. 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;
>
> (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;
>
> ...
>
> (q) **"registration information"** means information about an individual that is collected for the purpose of registering the individual for the provision of health services, and includes the individual's health services number and any other number assigned to the individual as part of a system of unique identifying numbers that is prescribed in the regulations

i. Categories #1, #4 and #5

[40] The misdirected faxes in question in all of these categories originated from RIS, an electronic medical record (EMR) that, together with the Picture Archiving and Communications System (PACS), houses data about diagnostic imaging tests and results of patients. These systems are both managed by eHealth Saskatchewan. The Government of Saskatchewan, Ministry of Health's website describes these systems as follows:

> The PACS component is a computer system that interfaces with the medical imaging device (i.e., X-Ray, CT Scan, MRI, ultrasound, etc.) to capture the image in a digital format. Once captured, the image can be stored, manipulated and transmitted over a computer network.
>
> The RIS component interfaces with the existing hospital information systems to capture patient demographic and study (digital exams) orders. Once the information is captured, authorized health care providers in Medical Imaging departments use the information to schedule and complete the exam. As exams are completed they are interpreted by an authorized radiologist and the results are recorded in the RIS. The RIS interfaces with the PACS component to link images from the study and the interpreted results making them available to authorized users – typically referring physicians.[7]

[41] Another webpage of the Ministry of Health provides more detail about the types of images found in PACS:

> The Saskatchewan Picture Archiving and Communication System (PACS) is a secure computer system designed for the storage, retrieval and display of diagnostic images by authorized health care providers.
>
> The kind of images managed include:
>
> - general x-ray;
> - ultrasound;
> - computed tomography (CT);
> - magnetic resonance imaging (MRI);
> - nuclear medicine; bone density;

[7]Ministry of Health, *Enabling the Provincial Electronic Health Record (EHR) Strategy: RIS-PACS-Archive (Diagnostic Imaging)*, available at www.health.gov.sk.ca/ris-pacs-archive.

- lithotripsy (non-invasive treatment of kidney stones and stones in the gallbladder or in the liver);
- angio/interventional (use of x-rays and contrast dyes to diagnose); and
- diagnostic mammography at selected sites.[8]

[42] My office has not collected any of the misdirected faxes or asked for copies of them. However, we have been told that all of the misdirected faxes contained diagnostic imaging information. This could include details of those diagnostic imaging exams and diagnostic interpretations of radiologists.

[43] The investigation report of eHealth Saskatchewan covering all files in Category #1 stated the following:

> From April 26th to June 25th, 2012, **copies of diagnostic imaging results** from the Saskatchewan Radiology Imaging [sic] System ("RIS"), supported by eHealth Saskatchewan ("eHealth"), were inadvertently faxed to incorrect numbers within the Saskatchewan healthcare system.
>
> [emphasis added]

[44] With respect to Category #4, the PAPRHA stated in its letter dated September 9, 2013 (File 072/2013) that:

> As a result of a configuration setting with the Radiology Information System (RIS), twelve (12) **radiology reports** originating in the PAPHR were sent to the wrong physician clinic from 2010 to June 18, 2013.
>
> [emphasis added]

[45] HRHA's investigation report (File 073/2013) did not specifically address that personal health information had been disclosed by fax; however, my knowledge of the circumstances allows me to conclude that the faxes sent from RIS would qualify as personal health information.

[8]Ministry of Health, *Diagnostic Imaging – Projects: Picture Archiving & Communications System (PACS)*, available at www.health.gov.sk.ca/pacs.

[46] SRHA's investigation report (File 075/2013) of September 2013 stated:

> Given that configuration setting in an electronic distribution system for the Saskatoon Health Region was not correct – eHealth automatically faxed **diagnostic imaging results** to the wrong trustees.
>
> [emphasis added]

[47] Finally, the investigation report from PNRHA (File 077/2013) stated the following:

> September 16/13: Medical transcription at Lloydminster Hospital received a call from a person in Spiritwood who wanted to let PNHR know that she was receiving **faxed radiology reports** at her private home.
>
> [emphasis added]

[48] As such, it appears that these faxes would qualify as personal health information pursuant to sections 2(m)(i) of HIPA as it would contain information with respect to the physical health of the individual; 2(m)(ii) of HIPA as it would contain information about a diagnostic imaging test of an individual which is a health service; and 2(m)(iv)(A) of HIPA as the information would have been collected in the course of providing health services to the individual.

[49] None of the above trustees have informed me that the personal health information contained in the faxes in question was de-identified.

ii. Categories #2 and #3

[50] The third parties in these two cases forwarded the misdirected faxes in question to my office for the purpose of containment and this investigation. As such, my office was able to examine each of the misdirected faxes. The faxes included physicians' referrals and reports; confirmations of appointments; radiology, microbiology, laboratory and catheterization reports; a graph depicting an individual's sinus rhythm; inpatient admission records; and a cardiology discharge letter to a family practitioner.

[51] Upon review of these documents, each one would qualify as personal health information pursuant to sections 2(m)(i) of HIPA as it would contain information with respect to the physical health of the subject individual; 2(m)(ii) of HIPA as it would contain information about medical testing of the subject individual which is a health service; and 2(m)(iv)(A) of HIPA as the information would have been collected in the course of providing health services to the subject individual. Further, each fax appears to contain registration information of the subject individual pursuant to sections 2(m)(v) and 2(q) of HIPA.

b. Were they under the custody or control of a particular trustee?

[52] Section 2(t) of HIPA defines trustee. The relevant portions are as follows:

> 2 In this Act:
>
> ...
>
> (t) **"trustee"** means any of the following that have **custody or control of personal health information**:
>
> (i) a government institution;
>
> (ii) a regional health authority or a health care organization;
>
> …
>
> (xii) a person, other than an employee of a trustee, who is:
>
> (A) a health professional licensed or registered pursuant to an Act for which the minister is responsible; or
>
> (B) a member of a class of persons designated as health professionals in the regulations;
>
> [emphasis added]

[53] FHRHA, PAPRHA, PNRHA, SRHA, HRHA, Sunrise, MCRRHA and RQRHA all qualify as trustees pursuant to section 2(t)(ii) of HIPA as they are all RHAs.

[54] Lakeview Neurology is operated by two physicians: Dr. Paul Masiowski and Dr. Gary Hunter. Dr. T.W. Wilson operates his practice on his own.

[55] It is my understanding that these physicians are licensed pursuant to section 28 of *The Medical Profession Act, 1981*.[9] This is an Act for which the Minister of Health is responsible.

[56] As such it appears that Dr. T. W. Wilson is a trustee pursuant to section 2(t)(xii)(A) of HIPA.

[57] However, it is unclear who is the responsible trustee in the case of Lakeview Neurology. In a conversation between a Portfolio Officer in my office and Dr. Masiowski on September 6, 2013, Dr. Masiowski informed our office that Lakeview Neurology was a venture and if the two physicians separated, each one would retain custody or control of their own patients' personal health information. He also confirmed that the affected individual for File 013/2013-HIPA/BP is his patient. This indicates that Dr. Masiowski is the responsible trustee. However, he also provided our office with a copy of Lakeview Neurology's Privacy Policy. It states:

> This policy applies to all personal health information (PHI) as defined under *The Health Information Protection Act of Saskatchewan* [sic] (HIPA), **and is under the trusteeship of Gary Hunter (Privacy Officer for Lakeview Neurology)**.
>
> [emphasis added]

[58] This passage indicates that Dr. Hunter is the trustee. As Lakeview Neurology has provided nothing further in writing, and no supporting evidence, on a balance of probabilities, I conclude Dr. Gary Hunter is the responsible trustee pursuant to section 2(t)(xii)(A) of HIPA.

[59] Now that I have determined that each of the above named entities is a trustee, I must determine which trustee has custody or control of the personal health information for

[9] *The Medical Profession Act, 1981*, S.S. 1980-81, c. M-10.1 at section 28.

each case at the material time. In other words, I must determine who was ultimately accountable for the personal health information at the time it was sent by fax.

[60] In my 2010 Report, I found that the responsible trustee was the health care provider who sent the fax:

> The 31 trustees that sent the faxes to the third party business had custody or control of the personal health information when the unauthorized disclosures took place. These trustees had a duty to protect the personal health information within their custody or control. Section 16 of HIPA requires that trustees have policies and procedures to protect against any reasonably anticipated unauthorized access to or use, disclosure or modification of personal health information.[10]

[61] To make the decision to communicate personal health information by fax, the sender trustee would need to have custody or control to do so. A trustee who is an intended recipient of a fax containing personal health information would not necessarily know that personal health information is being conveyed to them or have a say in how the personal health information is communicated. The trustee who is the intended recipient would only have custody or control over the personal health information once it has been received and accepted (i.e. collected).

[62] Categories #2 and #3 appear to be straightforward cases of sender trustees sending faxes astray. As such the trustees listed in the Background Section appear to be the trustees with custody or control of the personal health information in question for each case, not the recipient trustees.

[63] However, I must consider what roles both the RHAs and eHealth Saskatchewan played in Categories #1, #4 and #5 as all appear to qualify as trustees.

[64] eHealth Saskatchewan would also qualify as a trustee pursuant to section 2(t)(i) of HIPA as it is a government institution for the following reasons. Section 2(h) of HIPA defines "government institution" as follows:

[10] *Supra* note 4 at p. 16.

> 2 In this Act:
>
> …
>
> (h) **"government institution"** means a government institution as defined in *The Freedom of Information and Protection of Privacy Act*;

[65] Section 2(1)(d) of *The Freedom of Information and Protection of Privacy Act* (FOIP)[11] defines government institution as follows:

> 2(1) In this Act:
>
> …
>
> (d) **"government institution"** means, subject to subsection (2):
>
> (i) the office of Executive Council or any department, secretariat or other similar agency of the executive government of Saskatchewan; or
>
> (ii) any prescribed board, commission, Crown corporation or other body, or any prescribed portion of a board, commission, Crown corporation or other body, whose members or directors are appointed, in whole or in part:
>
> (A) by the Lieutenant Governor in Council;
>
> (B) by a member of the Executive Council; or
>
> (C) in the case of:
>
> (I) a board, commission or other body, by a Crown corporation; or
>
> (II) a Crown corporation, by another Crown corporation;

[66] Finally, section 3 of *The Freedom of Information and Protection of Privacy Regulations*[12] states:

> 3 For the purposes of subclause 2(1)(d)(ii) of the Act:
>
> (a) the bodies set out in Part I of the Appendix; and
>
> (b) subsidiaries of government institutions that are Crown corporations;

[11] *The Freedom of Information and Protection of Privacy Act*, S.S. 1990-91, c. F-22.01.
[12] *The Freedom of Information and Protection of Privacy Regulations*, c. F-22.01 Reg. 1.

are prescribed as government institutions.

[67] eHealth Saskatchewan is listed in Part I of the FOIP Regulations' Appendix and therefore qualifies as a trustee pursuant to section 2(t)(i) of HIPA provided it has custody or control of personal health information.

[68] The homepage of eHealth Saskatchewan's website explains the following:

> eHealth Saskatchewan is responsible for developing and implementing the Electronic Health Record (EHR) for Saskatchewan. The EHR makes important information available to support improved patient care. eHealth also coordinates, implements and maintains key electronic health information systems in many public health care organizations.[13]

[69] As will be discussed later in this Investigation Report, the root cause of the breaches in Categories #1, #4 and #5 related to problems with RIS, which has been developed and is maintained by eHealth Saskatchewan. However, eHealth Saskatchewan appears to have been operating as an IMSP to each of the RHAs involved in Categories #1, #4 and #5 so would not be a trustee in its own right in these situations.

[70] IMSP is defined in section 2(j) of HIPA as follows:

> 2 In this Act:
>
> …
>
> (j) **"information management service provider"** means a person who or body that processes, stores, archives or destroys records of a trustee containing personal health information or that provides information management or information technology services to a trustee with respect to records of the trustee containing personal health information, and includes a trustee that carries out any of those activities on behalf of another trustee, but does not include a trustee that carries out any of those activities on its own behalf;

[71] eHealth Saskatchewan is providing the use of RIS as an "information management or information technology service" to the RHAs. However, information management or information technology services are provided for the personal health information within

[13] eHealth Saskatchewan, *Empowering patients. Enabling Care.*, available at www.ehealthsask.ca.

the RHAs' custody or control; in other words, RHAs are trustees of the personal health information in these systems.

[72] As such, all of the listed health care providers are the responsible trustees for each of the respective files.

c. Were there unauthorized disclosure(s) and use(s) of the personal health information?

i. Disclosure(s)

[73] Section 27(1) of HIPA states:

> 27(1) A trustee shall not disclose personal health information in the custody or control of the trustee except with the consent of the subject individual or in accordance with this section, section 28 or section 29.

[74] None of the trustees have brought forward arguments that the misdirected faxes were sent in accordance with sections 27, 28 or 29 of HIPA. Further, none of the trustees have indicated that the subject individuals in question provided consent for disclosure before these faxes were disclosed.

[75] However, some of the trustees involved in Categories #1 and #4 have alleged that because some faxes were misdirected to *other trustees* it does not qualify as a privacy breach.

[76] In its investigation report of July 19, 2013, eHealth Saskatchewan stated:

> It is important to note that the faxed documents that were sent to the incorrect fax numbers were still sent to healthcare organizations or professionals.
>
> …
>
> - Each contact with healthcare providers was recorded in a detailed spreadsheet, ensuring an accurate record of how the misdirected faxes were handled and confirming that no faxes went outside the Saskatchewan healthcare system.

[77] It does not matter if personal health information is disclosed to another trustee; without authorization from sections 27, 28 or 29 of HIPA or consent from the subject individual, it is considered a privacy breach. For the purposes of HIPA, if another trustee receives a misdirected fax in which it has no legitimate need-to-know, that action is treated no differently than a disclosure to a non-trustee. To conclude otherwise would abrogate section 23 of HIPA.

[78] I acknowledge that the current Director, Privacy and Access Services and Chief Privacy Officer of eHealth Saskatchewan has diligently been sending the message to other trustees that unless a misdirected fax is received by the intended recipient, it constitutes a breach. Nonetheless, the above quotations in eHealth Saskatchewan's report, which was circulated to all of the involved trustees, sent a confusing message.

ii. Use(s)

[79] Other trustees reported faxes that were misdirected to their own organization, in other words, within the RHA.

[80] In its letter of September 20, 2013 dealing with File 042/2013-HIPA/BP, FHRHA stated:

> This, along with the challenge of ensuring physician fax numbers were accurate in the system, resulted in 3 faxes affecting 3 patients related to diagnostic imaging events going to the wrong fax numbers within the Five Hills Health Region, (FHHR).

[81] In the investigation report provided by MCRRHA, it stated:

> MCRHR had only 2 results affected (one patient), and this fax was sent to a number within the region.
>
> …
>
> In 2012, when eHealth contacted the La Ronge Medical Clinic, they were informed that the third physician no longer worked in MCRHR and in fact she had moved to an out of region community and was employed at a different clinic.
>
> Although it had been determined that there had not been harm to the patient due to delay in transmittal of faxes in 2012 & assurances from eHelath [sic] that the breach

had been contained, MCRHR decided to revisit this event upon receipt of the letter from the information and Privacy Commissioner dated July 3, 2013.

[82] Section 23(2) of HIPA states:

> 23(2) A trustee must establish policies and procedures to restrict access by the trustee's employees to an individual's personal health information that is not required by the employee to carry out the purpose for which the information was collected or to carry out a purpose authorized pursuant to this Act.

[83] I commented on section 23(2) of HIPA in my Investigation Report H-2013-003 as follows:

> [90] This section of HIPA embodies both the data minimization and need-to-know principles. I have previously defined these principles in my Investigation Report F-2012-005 as follows:
>
> > [65] For both the personal information and personal health information involved in the injury claim and [return-to-work] planning it appears that there are issues related to the 'need-to-know' and 'data minimization' principles.
> >
> > [66] These two principles underlie section 28 of FOIP and sections 23 and 26 of HIPA. The need-to-know principle means that SGI should collect, use and disclose only on a need-to-know basis. As well, data minimization means that SGI should collect, use or disclose the least amount of identifying information necessary for the purpose.

[84] Section 23(2) requires that trustees restrict its employees' access to personal health information requiring a need-to-know.

[85] In some cases in Categories #1 and #4, even though some misdirected faxes ended up in the wrong place of a large trustee organization, it still constitutes a breach of privacy.

[86] In all cases, unauthorized uses and disclosures of personal health information occurred when the faxes in question were sent to the incorrect recipients.

2. What circumstances led to each of the breaches?

a. Category #1

[87] My office encountered difficulty in understanding the causes of the RIS breaches captured by Category #1. The *Investigation Report 2012-029 RIS Faxing Review* provided by eHealth Saskatchewan on July 19, 2013 explains the breach as resulting from two separate incidents. These incidents are explained in rather technical terms. For the most part, the investigation reports of the RHAs simply relied on eHealth Saskatchewan's *Investigation Report 2012-029 RIS Faxing Review* and did not provide any extra analysis or explanation (as described in the evaluation portion of this Investigation Report).

[88] eHealth Saskatchewan's *Investigation Report 2012-029 RIS Faxing Review* provides the following explanation of the two incidents:

> **Details preceding the misdirected faxes (1st incident)**
>
> …
>
> Before April 2012, there were seven RHAs that were using the RIS system – Prince Albert Parkland, Cypress, Five Hills, Heartland, Prairie North, Sunrise and Mamawetan Churchill River. Saskatoon Health Region ("SktnHR") became a part of this system on May 28th, 2012.
>
> The RIS system is configured to accept only one programmed fax contact number per healthcare provider (regardless of the number of RHAs associated to that provider). When an RHA goes live, the system administrator working on the project worksheets is given a list of providers currently in the RIS. They identify and verify the provider's information (address, fax number, and alias) required in their RHA. These changes would be included in an updated Provider "Master Spreadsheet or List".[14]

[14]Footnote found in eHealth Saskatchewan's investigation report as follows: "The Provider 'Master Spreadsheet or List' (named 'Physician and Provider Group Deliverables') was a master list of all RIS Providers and their address, phone, fax and regional identifier information. The spreadsheet was initially populated from the Provider Registry System ('PRS') at the beginning of the RIS project and was used to do the initial population of RIS provider information. During subsequent RHA implementations it had been used as a base for configuring and validating regional provider information. It was also updated regularly by RHAs using RIS to request changes to provider information in RIS."

Prior to the misdirected faxes, there was a technical incident which directly affected this course of events. A technical description of the circumstances leading up to the faxing incident includes:

- SktnHR radiology information was being built and validated by eHealth based upon the requirements identified by the SktnHR.

- In preparation for the SktnHR RIS go–live, the information was promoted from the BUILD[15] environment to PRODUCTION ("PROD")[16] environment in RIS using RDDS in two stages – one on April 26th and one just prior to the SktnHR go-live on May 28th. The tool used to transfer the configuration from the BUILD to the PROD environments resulted in configuration issues of some of the provider fax information.

- When SktnHR was being implemented, they were given the Provider Master Spreadsheet to review and identify what providers required SktnHR aliases and to ensure that the data was current. SktnHR said that the list was too difficult to go through and that there were many discrepancies. Cerner, the vendor for the RIS, was involved to compare what was in the current RIS production environment to their QuadRIS[17] system. The records that matched were given SktnHR aliases. The unmatched records were identified and sent to SktnHR to review and verify the provider's information (address, fax number, and alias). The verified information from SktnHR was updated in the BUILD environment.

- When a result is finalized, the following are possibilities that could occur based on the provider copy distribution set-up:
  - If the fax number is blank it will be printed on the RHA's default printer.
  - If an error occurs while faxing, the report will be displayed in the RRDS Report Queue as an error.
  - If the fax successfully sends, the fax cover sheet identifies any information going to the wrong location should be reported back.

- The primary cause of this technical issue was the result of a missed configuration step in the BUILD where some physician information in a tool called Health Network Architectures ("HNA") was not correctly cross referenced with physician information in a fax configuration tool called Remote Report Distribution ("RRD").

[15]Footnote found in eHealth Saskatchewan's investigation report as follows: "The BUILD environment is considered a development type of IT environment. It is used by the project team to create the new sites and is also used for the user acceptance testing prior to deploying it to PROD environment."
[16]Footnote found in eHealth Saskatchewan's investigation report as follows: "The PROD environment is the environment used to store confidential patient test and result information. It is accessed by all RHAs using RIS."
[17]Footnote found in eHealth Saskatchewan's investigation report as follows: "QuadRIS was SktnHR's regional RIS system prior to moving over to the provincial RIS system."

- Shortly after the SktnHR RIS implementation, SktnHR identified the issue that faxes were not being distributed as expected. On June 4th, 2012 it was also confirrmed that this had occurred in seven other RHAs.

…

Details regarding the misdirected faxes (2nd incident)

- June 22nd: A conference call had been set up to discuss the lessons learned from the first incident. At this meeting a representative from SktnHR identified that there may be an additional issue, that some RIS faxes were being sent to incorrect numbers.

    - While there had been a few reports of faxing errors preceding this meeting, this had not been identified as a global issue due to the minimal number of reports that had been received (four in total) for the other 7 health regions during this time frame. SktnHR had identified this number was more significant, and the issue was escalated.
    - SktnHR indicated that their acting privacy officer had been notified earlier that week of their misdirected faxes.

- June 25th: The eHealth Privacy and Access Unit was debriefed on the second incident. An eHealth Privacy and Security Incident Report was created and the eHealth Standards Unit (who is responsible for patient safety incidents) was notified. As well, the Ministry of Health Chief Privacy Officer and Communications Branch were advised. RIS is a provincial system but the responsibility of the data is that of each RHA (8 regions in total at that time). Because this issue occurred during the SktnHR RIS implementation and involved eHealth, it was determined that eHealth would take the lead on the incident review and communication (in order to ensure coordination of the incident). By doing so, this in no way removed the responsibility for each trustee to review their policies and procedures for this situation.

- June 26th: The Office of the Information and Privacy Commissioner was notified, and contact was made with the RHA privacy officers advising them of the situation.

…

- June 27th: A faxed memo was sent to physicians advising that RIS faxes may have been misdirected and that diagnostic imaging results were (and had always been) available in the Picture Archiving and Communications System ("PACS").

…

- July 16th: Although the investigation was still proceeding, a decision was made by eHealth executive management to issue letters advising of both the privacy and

critical incident potential. As final containment results had not yet been completed, it was decided to proactively inform any patients who could have been **potentially** affected by the incident. The exception to this decision was that no letters were to be issued to patients who had passed away during this timeframe (pending final containment results).

- July 20th: Based on new available data, the RIS Applications Support Team reported that the number of incorrect faxes had changed to 1,031 and involved a potential 845 patients. Notification letters were sent to the 845 patients thought to be potentially affected.

- August 22nd: Final containment was completed. There were 362 confirmed misdirected faxes, 304 patients involved, 38 ordering care providers, and 1 deceased patient.

[89] This account by eHealth Saskatchewan did not identify root causes of the incident and raised more questions than it answered. A Portfolio Officer from my office met with the Director, Privacy and Access Services and Chief Privacy Officer of eHealth Saskatchewan on October 9, 2013 to have our questions clarified. This meeting proved to be very helpful. As a result, the following is my office's understanding of this breach.

[90] Both Incidents #1 and #2, described above by eHealth Saskatchewan, stemmed from problems after SRHA 'went live' on RIS.

[91] Before an RHA is able to begin using RIS, eHealth Saskatchewan provides the RHA with a master list of fax numbers that it would potentially fax personal health information to through RIS. The master list was taken from a provincial Provider Registry System (PRS). The purpose of the PRS is to identify physicians and assign a unique identifier for the purposes of the EMRs managed by eHealth Saskatchewan. The PRS is built from the college directories and the Medical Services Branch in the Ministry of Health. It is our understanding that this system is simply meant to uniquely identify providers for EMRs; it is not intended as a source of up-to-date contact information.

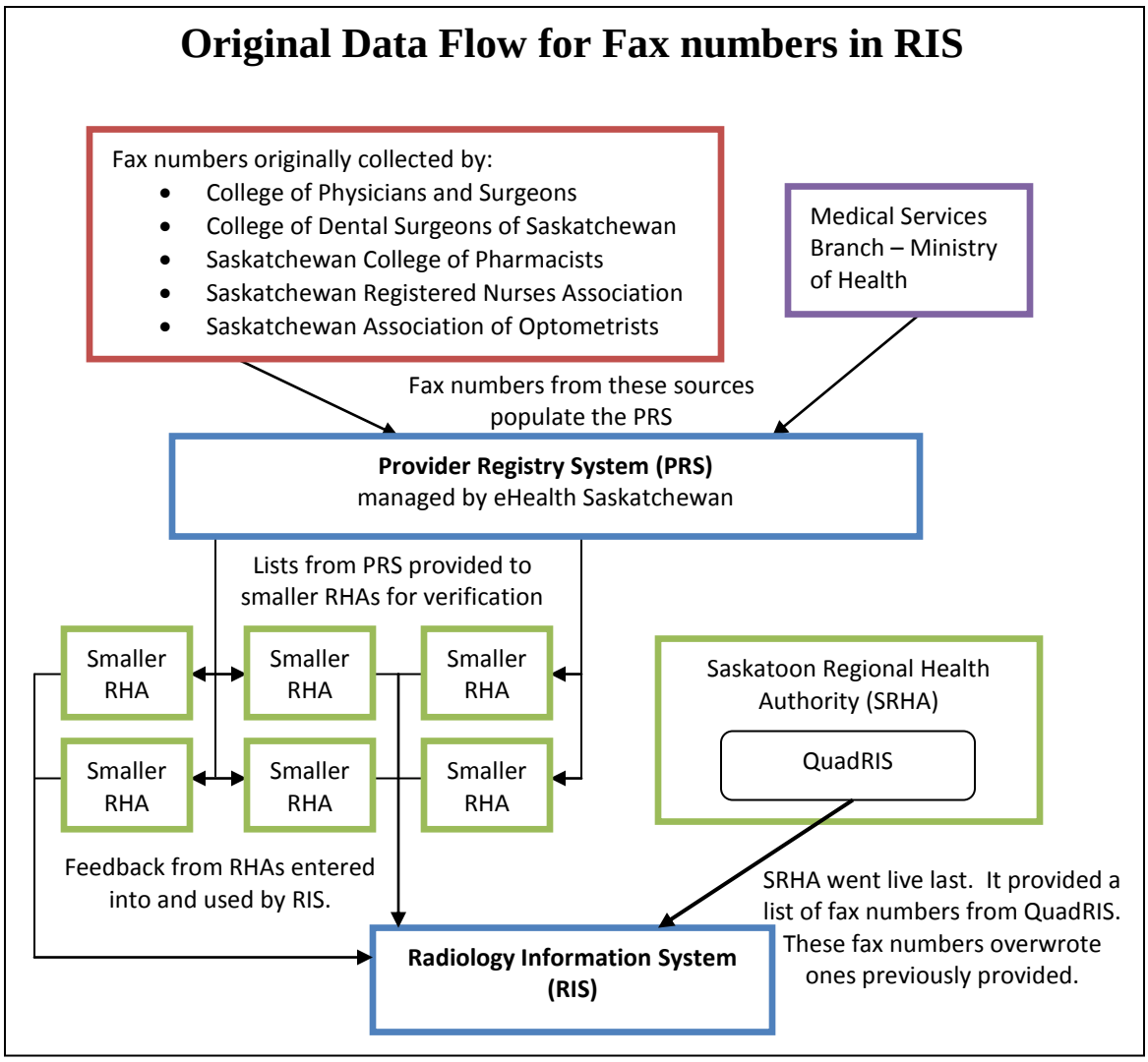
[92] Before SRHA 'went live', eHealth Saskatchewan supplied it with such a master list. eHealth Saskatchewan requested that SRHA verify each fax number to which it would be faxing on the master list provided.

[93] SRHA was resistant to completing this task as the list was complex and there were many discrepancies. Instead, SRHA provided eHealth Saskatchewan with a list from its existing radiology information system – QuadRIS. eHealth Saskatchewan accepted this list and loaded it into RIS.

[94] When this occurred, as fax numbers from the QuadRIS were in a different format, there was a computer glitch where the system put zeros in front of each fax numbers. As a result, no faxes for these numbers were able to be sent as the numbers were invalid. This is described as Incident #1 in eHealth Saskatchewan's report.

[95] Incident #2 flowed from Incident #1. When eHealth Saskatchewan entered the list of unverified fax numbers provided by SRHA, common fax numbers already provided by the other RHAs using RIS were overwritten. Steps taken by eHealth Saskatchewan to correct Incident #1 revealed incorrect fax numbers, presumably provided by SRHA. This caused all of the misdirected faxes in question in the Category #1 breach for all RHAs.

[96] The following diagram depicts the original flow of fax numbers into RIS.



[97] eHealth Saskatchewan alleges SRHA is partly at fault for not doing its due diligence in verifying the master list from eHealth Saskatchewan or by verifying that the fax numbers provided from the QuadRIS system were correct. However, eHealth Saskatchewan also acknowledges that it should not have deviated from the already established practice.

[98] eHealth Saskatchewan has indicated that it plans to ensure that the next large RHA to start using RIS is diligent in verifying fax numbers before it is able to fax from RIS. RQRHA is currently scheduled to begin using RIS in the second quarter of 2014.

b. Category #2

[99] My office's assumption at the beginning of this investigation was that there may be one root cause for multiple faxes to be misdirected from multiple trustees to the same third party in Moose Jaw. However, once I heard from the relevant trustees, I concluded that multiple problems could be attributed to these faxing errors.

[100] However, there does appear to be one common thread throughout these six files: problems related to an automated EMR system.

[101] It is important to note when considering Category #2 that many physicians work or worked for the third party in Moose Jaw, however five physicians in particular are relevant in this Investigation Report. Coincidentally, it is also important that the last names of Physician #1, Physician #3 and Physician #5 described in Category #2 begin with the same first four letters as this proved to be a factor.

i. File 013/2013-HIPA/BP – Lakeview Neurology

[102] In its letter of July 21, 2013, Lakeview Neurology described the following error that occurred from human interfacing with the EMR Accuro involving Physician #1:

> All three letters should have been sent to Dr [same last name of Physician #1]…. My office staff create profiles for any new patient in my electronic medical records, including the name of the referring physician. Mistakenly, they added Dr [last name of Physician #1], practicing [for the third party], as the referring physician for [the affected individual], instead of Dr [same last name as Physician #1].
>
> **My EMR system, Accuro, allows us to search a database of physicians in the province by typing part of the physician's name and then selecting from an alphabetical list of matches.** For instance, searching for "Morri" calls up a list of physicians including a Dr Morris, Dr Morrison and Dr Morrissette. As far as I can tell, **my staff would have typed part or all of [of Physician #1's last name] in the search box, hit enter, and seen a list of options including Dr [same as Physician #1's last name] and Dr [last name of Physician #1]. They then clicked on the wrong name on that list.**

> Once Dr [last name of Physician #1] was listed as the patient's referring physician, all correspondence from my EMR system, including appointment letters and my clinic notes, would automatically be directed to him.
>
> [emphasis added]

[103] It appears that the root cause of this breach was an entry of inaccurate information into the EMR. This was enabled by the use of an 'auto suggest' feature in the EMR. I also note however, that the third party in Moose Jaw has informed me that Physician #1 has not worked with them for over ten years. This is an indication that the contact information for physicians in Lakeview Neurology's Accuro system is also long out of date.

ii. File 014/2013-HIPA/BP – Five Hills Regional Health Authority

[104] In its letter of June 20, 2013, FHRHA explained that it was the interface between its EMRs, WinCIS and RIS, as well as outdated patient information that caused the misdirected fax in this case:

> **It was explained to us that our FHHR RIS accepts certain elements of information from our hospital admitting/discharge/transfer system (called WinCIS).** One key element is the name of a patient's family doctor. That information from WinCIS is provided to RIS when it's ready to auto-generate a faxed results report. In this breach allegation, the FHHR RIS auto-faxed [the affected individual's] report to [Physician #2] – as he was the doctor listed in WinCIS as [the affected individual's] family doctor.
>
> ...
>
> In our breach allegation, our RIS auto-faxed [Physician #2] as he was listed as the patient's family doctor.
>
> ...
>
> At this point, we contacted [the affected individual] himself and explained to him the alleged breach details. [The affected individual] confirmed with us that [Physician #2] is not his family doctor - and in fact he stated he does not have a family doctor at the present time. …
>
> Upon further investigation, the best we could determine is that at some point in the past 20 years or so, [the affected individual] probably came to Moose Jaw Union

> Hospital, presented to our Admitting/Registration area, and likely was seen by [Physician #2] for some type of treatment. **At that point, [Physician #2's] name would have been entered into the WinCIS as [the affected individual's] family doctor. It is feasible that [the affected individual] has not visited MJUH for service since that initial encounter where [Physician #2] was added as his family doctor. Therefore, his information was never updated.**
>
> We have since discovered that the family doctor field in WinCIS is only updated when the patients themselves present for medical treatment at regional facilities that have WinCIS capability. It was discovered by us, that Central Butte Primary Health Care clinic did not have WinCIS capability. We are happy to report that since this breach allegation, we have set in motion the required steps to have Central Butte PHC Clinic obtain permission to access WinCIS, and to edit the family doctor field to accurately reflect their patient's family doctor (if they have one) to avoid similar problems in the future with diagnostic imaging reports faxed out of RIS in the future from this location.
>
> [emphasis added]

[105] As noted, outdated information in one system interfacing with RIS caused this misdirected fax. However, in this case the outdated information appears to be that of the affected individual, and not physician contact information within RIS.

iii. Files 015/2013-HIPA/BP and 057/2013-HIPA/BP – Prince Albert Parkland Regional Health Authority

[106] PAPRHA sent two misdirected faxes to the third party in Moose Jaw. I note the second incident occurred on June 22, 2013 which was a month after I received the internal investigation report of PAPRHA dated May 6, 2013. This internal report for the first misdirected fax was short on detail and simply stated the following:

> Thank you for confirming that the facsimile in question was received by the [third party]. **It is unclear as to who the ordering physician was, as lab staff can no longer refer to the original requisition.** As per Lab Quality Assurance Program guidelines, original requisitions are only kept for three months. There are two factors that may have contributed to the misdirected fax:
>
> 1. In the old Laboratory Information System (LIS) the physician identification [first 4 letters] belonged to [Physician #1]. In the new lab system, it belongs to [Physician #3]. Staff may have picked the wrong physician identifier.

2. If [Physician #3] was the doctor on the requisition, staff were unaware that she no longer practiced [with the third party]. They only became aware of this fact after the report was released.

Lab employees take great care when faxing personal health information, and all faxes are sent with a fax cover sheet.

[emphasis added]

[107] It appears that PAPRHA may have simply chosen the wrong physician. However, the lack of detail provided by PAPRHA leaves us asking many questions such as what is a "physician identification"? Is it the same as an 'auto suggest function'? How are different physicians with similar last names differentiated within the Laboratory Information System (LIS)?

[108] Again, I note that the third party indicated that Physician #1 had not practiced with it for approximately ten years. It also advised that Physician #3 had not practiced there for approximately four years. Either way, contact information for both physicians was out of date in PAPRHA's LIS system.

[109] Further, our office provided the name of the affected individual to PAPRHA for the purposes of this investigation. It is disappointing it did not investigate further to find the identity of the ordering physician to both ensure continuity of care and help determine the cause of the breach.

[110] Also, the statement about staff taking "great care" when faxing personal health information is questionable as there was a similar occurrence. In its letter dated July 29, 2013, PAPRHA provided the following limited information:

> In response to your letter dated July 9, 2013, the misdirected fax in question did originate from the Prince Albert Parkland Health Region. The ordering physician was listed as "Dr. [name of Physician #4]". The employee inadvertently chose "[Physician #4]", resulting in the report being sent to the wrong [party] in error.

[111] For both files, preventable human error and outdated contact information were root causes of the breach.

iv. File 034/2013-HIPA/BP – Prairie North Regional Health Authority

[112] PNRHA also explained that outdated information played a role in its misdirected fax in its letter dated August 19, 2013 as follows:

> This report was faxed from [Battlefords Union Hospital] Lab LIS fax server. From my investigation the technologist accessioned [Physician #3] into our LIS. The LIS had an old fax number in the system for [Physician #3]. We did not have a fax number on the requisition to verify the fax number that was in our LIS. The completed report was then faxed to her old fax number on May 6... Once we received notification that [Physician #3] had moved and had a new fax number the LIS fax number was changed and confirmed on May 15 and a report was faxed to her.
>
> **As part of my investigation I had the original requisition retrieved and I have also noted that [Physician #3] was not the [sic] on the original requisition order**. I have contacted [Physician #3's] new office to notify her that she should not have received a report on the patient. The office already destroyed the report since it was not her patient. The report should have gone to Dr. R. [same last name as Physician #1] who is a resident with [another physician – Physician X]. I have made a corrected report and faxed the lab results from May to the patients' family physicians as listed in WinCis; [names of two other physicians]. No copy to Dr. R. [same last name as Physician #1] as I do not have a validated fax number for her. It has been mailed to [Physician X's] office. I have asked [an individual] to provide me with his/her information so it can be inputted into the LIS.
>
> [emphasis added]

[113] Again, dual root causes led to this misdirected fax breach.

v. File 059/2013-HIPA/BP – Regina Qu'Appelle Regional Health Authority

[114] The September 2013 investigation report from RQRHA indicated that the two faxes in question were sent from the Accuro EMR and drew the following conclusions:

July 29, 2013
- Saskatchewan College of Physicians and Surgeons was contacted to determine if [Physician #5] was a practicing physician in Saskatchewan.
    - [Physician #5] is retired but did practice [with the third party] that uses [fax number] as the fax number.

July 29, 2013
- [RQRHA Privacy Officer] contacted the WRC Physiatry Clinic again to ensure that [Physician #5] is the physician on file for [the affected individual].
    - Physician on file for [the affected individual] is [Physician with the same last name as Physician #5] in Regina, Saskatchewan.

…

Conclusion:

1. A breach of [the affected individual's] privacy has been substantiated.
2. The breach primarily occurred as a result of human error in which a WRC Physiatry Clinic staff member selected the wrong [physician] to send [the affected individual's] results out.
3. On August 27, 2013 [the affected individual] was sent a notification letter describing the privacy breach that occurred.

Incidental Findings:

1. **There are two [physicians with the same last name] who had contact information within the Provider Address Book in the Accuro EMR.**
    - **[Physician #5] was retired, but when practicing did provide healthcare services [for the third party].**

[emphasis added]

[115] It appears that the individual in charge of sending the fax chose the wrong physician. RQRHA's report also focuses on difficulties updating contact information in the EMR, but did not identify this as a root cause.

c. Category #3

[116] The misdirected faxes involved in this category are unique in this Investigation Report as they do not involve an EMR. All faxes in this category appear to have been sent manually. Both of the trustees involved report the same root cause – an error printed in

the College of Physicians and Surgeons of Saskatchewan's (CPSS) *Physicians Mailing List – January 2013* for the intended recipient physician.

[117] Dr. T.W. Wilson's letter to our office dated July 15, 2013 stated:

- We also attempted to fax the consultation and covering letter to [the intended physician], Family Physician of record. I had checked with the patient. I always recommend Family Physicians be informed. UNFORTUNATELY, THE FAX NUMBER LISTED FOR [the intended physician] IN THE CPSS PHYSICIANS MAILING LIST OF JANUARY 2013 WAS IN ERROR (copy enclosed; the "correction" was made by us, today).
- The [fax number] Fax number was a school. A representative of the school contacted our office on June 6th or 7, 2013, notifying us of the error. We advised that person to shred the fax. We refaxed the package to [the intended physician].

[118] SRHA's Privacy Incident Overview dated July 29, 2013 stated:

> Given the evidence noted above the privacy concern raised with the Privacy and Access Department have been substantiated. The personal health information faxed to the [the third party school] was done so in error as a result of the wrong fax number listed in the January 28, 2013 Directory of the College of Physicians and Surgeons. Additionally the revised information sent from the College of Physician and Surgeons on February 21, 2013 was not updated into the Unit 6000 Directory.
>
> Unit 6000 Cardiology have now created a process whereby the monthly revisions for the directory will be updated directly into the directory rather than tucking the revisions into the front cover.

[119] I have reviewed CPSS' *Physicians Mailing List – January 2013* and the fax number for the intended physician in these two cases does appear to be incorrect.

[120] My understanding is that CPSS produces a "Physicians Mailing List" twice a year. Organizations and individuals can subscribe to this directory for a fee. It is also my understanding that each month, CPSS sends a document which lists changes to the directory (eg. additions, changes, corrections, etc.) to each organization or individual that has a subscription to the directory once a month (with the exception of December and June). However, CPSS also sells individual copies of the "Physicians Mailing List".

Those who purchase individual copies would not receive the updates. This understanding has been confirmed by CPSS on October 9, 2013.

[121] CPSS issued a change notification in January 2013, February 2013, March 2013, April 2013 and May 2013. Each of these notifications, except for January 2013, provided the correct fax for the intended physician in this case. The correction to this physician's fax number was highlighted in bold and/or increased font size in both the March 2013 and May 2013 notifications.

[122] I note that the fax sent by Dr. T. W. Wilson was sent on June 6, 2013 and the two faxes sent from SRHA were sent on May 17, 2013 and May 22, 2013. As such, both trustees should have received multiple notices that the fax number for the intended physician in the CPSS Mailing List – January 2013 was incorrect and advised of the correct number. Neither of the trustees had reported that they did not receive the monthly updates from CPSS.

[123] After receiving a draft copy of this Investigation Report on or about November 7, 2013, Dr. Wilson indicated to our office that he did not receive the CPSS updates. He noted that he relies upon the College of Medicine at the University of Saskatchewan for such updates. He did not expand on this matter such as whether he subscribes himself to the CPSS "Physicians Mailing List" and whether or not he was aware of the long standing practice of CPSS issuing updates.

[124] As such, the root cause of these breaches was undue care and attention when sending these faxes.

[125] Also, as noted in the Background Section, the fax sent by Dr. T. W. Wilson appeared to contain highly sensitive personal health information of the affected individual in question. It discusses hormonal treatment with respect to a transgendered individual. The fax also discusses some of the individual's sexual habits as well as other personal health information. As will be discussed later in this Investigation Report, best practise is

to use discretion when faxing sensitive personal health information as it is clearly an insecure form of communication. As this fax contained highly sensitive personal health information, it should not have been sent by fax. As such, I also find this to be a contributing factor in this breach.

d. Category #4

[126] This breach, involving the use of RIS in three RHAs resulted in 125 misdirected faxes. It occurred as a result of a configuration setting that the RHAs made when RIS was first set up with each of the RHAs.

[127] From time to time, the physician who orders a diagnostic imaging test may not be the physician who should receive the results (eg. locum, retirement of physician, etc.). Changes may occur before the results have been prepared. At the time of set up with each RHA, RIS can be configured to send results to either the original ordering physician or the current physician. The three involved RHAs had the configurations set to original ordering physician so any changes that had to be made in terms of where results should be directed were not able to be made.

[128] SRHA noted the following in its investigation report of September 2013:

> eHealth Saskatchewan identified and corrected a configuration setting in an electronic distribution system in four health regions … that automatically faxes diagnostic imaging results to physicians. According to eHealth the configuration settings were based on regional preferences, and were to send diagnostic imaging results to the original ordering physician entered the configuration settings were not allowing this setting to be updated should a change in physician been made.

[129] HRHA made the following explanation in its investigation report of September 27, 2013:

> ... (in the RIS there is a distribution setting that each region selects. This will send results to the original ordering provider or the current ordering provider. The distinction is when care of the patient may have been transferred (e.g., ER physician to the family physician) or if a correction has been made. Your regions apparently

> had the distribution setting set to original ordering provider so results were sent to that provider and not the current ordering provider (where such a change was made).

[130] HRHA also stated:

> The information identified in the second reported breach [Category #4] is two of the seven breaches that were investigated and reported on by eHealth entitled ***Investigation Report 2012-029 RIS Faxing Review*** (Investigation Report) attached as Appendix A.

[131] HRHA did not provide any further explanation as to how the Category #1 and Category #4 breaches were related.

[132] PAPRHA's letter of September 9, 2013 provided no details and simply stated:

> In regards to your letter dated August 20, 2013 regarding misdirected faxes, Prince Albert Parkland Health Region (PAPHR) has been working with eHealth Saskatchewan regarding this breach of privacy. As a result of a configuration setting with the Radiology Information System (RIS), twelve (12) radiology reports originating in the PAPHR were sent to the wrong physician clinic from 2010 to June 18, 2013.

[133] eHealth Saskatchewan confirmed that this understanding of this category's breaches was correct.

e. Category #5

[134] This breach involved only PNRHA (File 077/2013-HIPA/BP). Twenty-three faxes affecting 22 patients were misdirected.

[135] On September 16, 2013, a hospital in PNRHA received a call from an individual advising that she had been receiving radiology reports on her fax machine in her private home.

[136] As it appeared the faxes were being generated from RIS, PNRHA consulted its IMSP, eHealth Saskatchewan. Upon request from PNRHA, eHealth Saskatchewan provided the following details to my office on September 18, 2013:

> On June 25th, [an RHA other than PNRHA] called the eHealth Service Desk to add a provider to the Radiology Information System (RIS) faxing tool. The information provided by [the RHA] was correct. An employee of eHealth Saskatchewan incorrectly entered the fax number; "883" was entered instead of "833".

[137] In its investigation report of September 27, 2013, PNRHA also identified the following root cause:

- … Further detail included that this was a fax number for a locum physician up in La Loche.
- [A PNRHA employee] indicated that PNHR practice is not to add locum physicians (who are often very short term) into the RIS because the locums are covering for a regular physician who is temporarily absent and thus felt to be better to send to the location of the permanent physician. The PNHR protocol for this is on the RIS/PACS Sharepoint site … It would not have been a PNHR request to have [the other RHA] add the locum physician; this was likely an SHR practice.

[138] Both human error when entering the fax number into RIS and apparent confusion regarding locum information in RIS appear to be root causes in this breach.

f. Summary of common root causes for all five breaches

[139] The following list recaptures root causes identified for all five categories of breaches involving misdirected faxes:

- Category #1 – The root cause of the biggest of the breaches involving RIS appears to have been incorrect fax numbers in RIS when each RHA came online.
- Category #2 – Several root causes can be attributed to this category of breaches which includes: out of date fax numbers in EMRs; undue care and attention when entering information, choosing where to send faxes and use of an 'auto suggest function'; and reliance on outdated personal health information in a legacy system.
- Category #3 – An incorrect fax number in the CPSS *Physicians Mailing List – January 2013* and undue attention paid to subsequent updates. Further, in one case, highly sensitive personal health information should not have been sent by fax.

- Category #4 – A configuration in RIS would not allow changes or updates to patient personal health information affecting where results should be sent.

- Category #5 – An incorrect fax number change was made in RIS.

3. Did each of the trustees involved have written policies and procedures as required by section 16 of *The Health Information Protection Act* and follow best practices for both sending the faxes in question and responding to the breaches?

a. Were such breaches reasonably anticipated?

[140] Fax machines are widely used in the health care field in this province. As such, the potential for misdirected faxes is not new. The incident described in my 2010 Report was covered in the media and involved five of the trustees named in this Investigation Report. It has been publically available on our website since December 6, 2010. In the 2010 Report, I listed several different breaches involving faxing personal information and personal health information that had been reported in the media.

[141] We also note the following non-exhaustive list of incidents that were reported in the media since 2010:

- On February 28, 2011, *The Star Phoenix* published an article entitled "Pharmacists warned about faxed prescription problems" which raised concerns about the authenticity of faxed prescriptions.[18]

- It was reported in the *Times Colonist* in Victoria on March 3, 2011 that the Office of the Information and Privacy Commissioner of British Columbia was investigating medical files being sent to a Langford roofing company in an article entitled: "Privacy office to probe medical files breach; Patient information was faxed to roofing business".[19]

- *The Canadian Press* published a story on August 24, 2011 detailing how T-4 slips and personal information were being faxed to wrong numbers from various

[18]Hannah Scissons, "Pharmacists warned about faxed prescription problems," *The Star Phoenix*, February 28, 2011 at p. A3.
[19]Richard Watts, "Privacy office to probe medical files breach; Patient information was faxed to roofing business," *Times Colonist*, March 3, 2011 at p. A4.

organizations in Alberta. The article was entitled "Alberta privacy commissioner calls mounting reports of lost data 'startling'".[20]

- On January 30, 2013, *The Vancouver Sun* published an article entitled "Private medical records faxed to auto shop"; John VanVeldhuizen says his number is similar to local clinic's, where the faxes are supposed to go" describing an auto body shop who kept receiving personal health information from various health care providers.[21]

- Problems with faxing in the health care sector even surface in the international media. The *Daily Mail* reported on October 29, 2012 that personal health information was routinely being faxed to the wrong number.[22] *The Telegraph* online reported on April 8, 2012 about misdirected faxes[23] and reported April 25, 2013 that "at least 1.8 million sensitive papers were lost by the NHS in the space of 12 months – a rate of 5,000 a day" partly due to misdirected faxes.[24] In August 2011, *The Press*, a New Zealand news publication, reported that a senior had been receiving 50 to 100 medical files on his personal fax machine in his home in a six month period.[25]

- Finally, CBC Saskatoon's website reported on September 16, 2013 that a Clearwater Dene Nation School in Saskatchewan was receiving faxes containing personal health information in an article entitled "Confidential medical records faxed to Sask. school".[26]

[142] Given all of the media reports over the years, as well as OIPC Reports and resources, misdirected faxes can be reasonably anticipated and trustees should have policies and procedures in place to safeguard personal health information when faxing it.

[20]*The Canadian Press*, "Alberta privacy commissioner calls mounting reports of lost data 'startling'," August 24, 2011.
[21]Brian Morton, "Private medical records faxed to auto shop; John VanVeldhuizen says his number is similar to local clinic's where the faxes are supposed to go," *The Vancouver Sun,* January 30 2013 at p. A11.
[22]Jack Doyle, "NHS loses track of 1.8m patient records in a year; Files dumped in bins and put up for sale online," *Daily Mail,* October 29, 2012 at p. 2.
[23]Laura Donnelly and James Clayton, "Cancer diagnosis among catalogue of NHS fax blunders," *The Telegraph* online, April 8, 2012.
[24]Nick Collins, "Private data fears 'hindering progress' in NHS," *The Telegraph* online, April 25, 2013.
[25]Amy Glass, "Medical notes sent in error; Health records faxed to wrong number," *The Press*, August 1, 2011 at p. A1.
[26]Jennifer Quesnel, "Confidential medical records faxed to Sask. School," *CBC Saskatoon* online, September 16, 2013.

b. What is required by *The Health Information Protection Act*?

[143] Even if there were not so many media reports and regular occurrences of misdirected faxes, trustees are still legally bound to protect against unauthorized disclosures of personal health information through the use of fax machines. One way in which HIPA imposes this duty is through section 16 of HIPA which states as follows:

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

[144] I have emphasized the significance of section 16 of HIPA and have called it "the spine to the HIPA skeleton as it is linked to every other provision in HIPA".[27]

[145] In various Investigation Reports, I have also made the following comments about section 16 of HIPA:

> [40] Section 16 is one of the most important features of HIPA. Without comprehensive written policies and procedures, the risk that a trustee will fall short of its many statutory responsibilities is dramatically increased. We have attempted to underscore this feature in a number of our publications including Review Report H-2008-002 and Investigation Reports H-2007-001, H-2005-002 and H-2004-001.[28]
>
> [91] HIPA prescribes that the trustee must establish policies and procedures to maintain administrative, technical and physical safeguards. These safeguards must

[27]SK OIPC, Investigation Report H-2013-002 at [47], available at www.oipc.sk.ca/reviews.htm.
[28]SK OIPC, Investigation Report H-2010-001 at [40]; also quoted in Investigation Report H-2013-002 at [46], both available at www.oipc.sk.ca/reviews.htm.

> protect the integrity, accuracy and confidentiality of the information. They must also protect against any reasonably anticipated threat or hazard to the security or integrity of the information; and the loss of, unauthorized access to, use or disclosure of the information.[29]

[146] I also stated:

> [93] If a trustee fails to achieve satisfactory compliance with HIPA requirements, there is a greatly increased risk that patients' [personal health information] will fail to be protected from exposure to others who would have no legitimate need-to-know that [personal health information] without the consent of the patients. There is also a heightened risk that patient confidence in their health providers will be undermined and that this will negatively impact health outcomes. Such a lack of confidence could compromise the effectiveness of the electronic health record system now being rolled out in this province. These risks are a concern to the Canadian Medical Association (CMA). The CMA underscores the importance of privacy when it states:
>
> 1. Privacy, confidentiality and trust are cornerstones of the patient-doctor relationship.
>
> Health information is highly sensitive and is confided or collected under circumstances of vulnerability and trust. Trust plays a central role in the provision of health care and treatment; fulfillment of physicians' fiduciary obligations enables open and honest communications and fosters patients' willingness to share personal health information.[30]

[147] Written policies and procedures are essential for all aspects of the protection of personal health information. As faxing is very common in the health care field, all trustees who fax must have appropriate written policies and procedures in place.

[148] As part of this investigation, I will be examining the policies and procedures that the trustees in question had in place at the time the misdirected faxes were sent.

[149] Before examining the trustees' policies, I will discuss faxing best practices and the methodology for scoring the trustees' policies, procedures and responses to the breaches.

[29]SK OIPC, Investigation Report H-2011-001 at [91]; also quoted in Investigation Reports H-2013-002 at [45] and H-2013-003 at [49], all available at www.oipc.sk.ca/reviews.htm.
[30]SK OIPC, Investigation Report H-2011-001 at [93]; also quoted in Investigation Report H-2013-003 at [49], both available at www.oipc.sk.ca/reviews.htm.

c. Where do we find best practices for faxing and responding to breaches?

[150] In addition to my 2010 Report, there are many resources available to trustees in Saskatchewan to assist in creating and strengthening fax policies and procedures.

[151] In April 2009, in response to the events detailed in the 2010 Report, my office created a resource entitled *Helpful Tips – Privacy Considerations: Faxing Personal Information and Personal Health Information*.[31] It was revised in October 2010. The advice and tips presented in this document are consistent with other resources on faxing such as:

- COACH, *Putting it into Practice: Privacy and Security for Healthcare Providers Implementing Electronic Medical Records* (2013)[32]
- Office of the Privacy Commissioner of Canada, *Fact Sheets: Faxing personal information*[33]
- Alberta Office of the Information and Privacy Commissioner, *Guidelines on Facsimile Transmission*[34]
- British Columbia Office of the Information and Privacy Commissioner, *Faxing and Emailing Personal Information*[35]
- Manitoba Ombudsman, *Manitoba Ombudsman Practice Note: Privacy Considerations for Faxing Personal and Personal Health Information*[36]

[152] In terms of privacy breaches, when this office begins any privacy breach investigation, we advise public bodies and trustees to consult our resource *Helpful Tips: Privacy Breach*

[31]SK OIPC, *Helpful Tips – Privacy Considerations: Faxing Personal Information and Personal Health Information*, available at www.oipc.sk.ca/resources.htm.
[32]COACH: Canada's Health Informatics Association, *Putting it into Practice: Privacy and Security for Healthcare Providers Implementing Electronic Medical Records – 2012 (Guidelines for the Protection of Health Information Special Edition)* at pp. 62-63.
[33]Office of the Privacy Commissioner of Canada, *Fact Sheets: Faxing personal information*, available at www.priv.gc.ca/resource/fs-fi/02_05_d_04_e.asp.
[34]Alberta Office of the Information and Privacy Commissioner, *Guidelines on Facsimile Transmission*, available at www.oipc.ab.ca/ims/client/upload/Guidelines_on_Facsimile_Transmission.pdf.
[35]British Columbia Office of the Information and Privacy Commissioner, *Faxing and Emailing Personal Information*, available at www.oipc.bc.ca/guidance-documents/1446.
[36]Manitoba Ombudsman, *Manitoba Ombudsman Practice Note: Privacy Considerations for Faxing Personal and Personal Health Information*, available at www.ombudsman.mb.ca/documents_and_files/practice-notes-1.html.

Guidelines.[37] This resource is one of many that can assist trustees in responding to any kind of privacy breach, including those involving misdirected faxes.

[153] All of the resources mentioned above were available for trustees in terms of preventing misdirected faxes with written policies and procedures and responding to breaches prior to the earliest of the breaches in question in this Investigation Report.

[154] In October 2013, following continued reports of misdirected faxes, our office also produced a resource jointly with the Ministry of Health entitled *Checklist for Trustees: Misdirected Faxes*.[38] This resource provides a checklist for trustees who receive misdirected faxes, send misdirected faxes and are involved in an OIPC investigation for sending misdirected faxes.

d. What is the methodology for evaluation of the individual trustees faxing policies and procedures and responses to the breaches?

[155] In the 2010 Report, I devised the following methodology for evaluating the policies and procedures and responses of the trustees involved. With slight modifications, I will use the same methodology for the purposes of this Investigation Report.

[156] The criteria for evaluating the responses to the breaches in the 2010 Report were as follows:

- 1 point – A summary of the incident and immediate response to contain the breach and reduce harm.
- 1 point – Steps taken to contain the breach.
- 1 point – Background of the incident:
  - Include timelines and a chronology of events.

[37]SK OIPC, *Helpful Tips: Privacy Breach Guidelines,* available at www.oipc.sk.ca/resources.htm.
[38]SK OIPC & Ministry of Health, *Checklist for Trustees: Misdirected Faxes,* available at www.oipc.sk.ca/resources.htm.

- Personal Information (PI) or Personal Health Information (PHI) involved (data elements and sensitivity of; number of individuals affected; etc).

- 1 point – A description of the investigative process.
  - Include the cause of the incident (root and contributing).
- 1 point – A summary of interviews held (complainant, internal, external).
- 1 point – A review of safeguards and protocols that were in place at the time of the breach.
- 1 point – A summary of possible solutions and recommendations.
- 1 point – A description of necessary remedial actions, including short and long-term strategies to correct the situation (staff training, rework policies/procedures, etc).
- 1 point – A detailed description of what the next steps will be.
- 1 point – Responsibility for implementation and monitoring, including timelines.
  - May also include the names and positions of individuals responsible for implementation.

...

I then gave one point to each trustee that has provided notification to the affected individual or has taken reasonable measures to do so.[39]

[157] I will use this methodology for evaluating responses of the trustees in question for the purposes of these breaches, however, I will make the following change. Trustees will receive one extra point for identifying the root cause and contributing causes of the breach. Without identifying this, no meaningful mitigation strategies or change can occur. As such the responses of the trustees for the purposes of this Investigation Report will be scored out of 12 points.

[158] Also, for the purposes of this Investigation Report, several of the trustees have more than one misdirected fax incident or file to be evaluated. In these cases, the response to each incident will be evaluated individually and then averaged into one score.

[39] *Supra* note 4 at p. 18.

[159] The written fax policies and procedures of the trustees will also be evaluated in the same manner as the 2010 Report. That evaluation criterion was outlined as follows:

a. Policy and Procedures

- 4 points – Adopt a written policy on faxing personal information and personal health information and ensure that employees, including all new employees, are trained and regularly reminded of the policy. This policy should include the types of information that can be faxed by or to your organization.
  - 1 point for having a written policy or procedure.
  - 1 point for mention of training of new employees and regular reminders for staff.
  - 1 point is awarded if the policy referenced HIPA as the applicable law and a further point is awarded for consistent use of the term "personal health information".

- 1 point – If possible, designate one employee to be responsible for sending and receiving personal information and personal health information by fax. Train that employee in proper procedures and ensure they are aware of the legal duty to protect the information.

b. Tips for Sending Faxes

- 1 point – Determine if there is an immediate time requirement that necessitates faxing the personal information or personal health information. Is there a quick and more secure way to forward the information to the recipient?

- 1 point – If a client requests that you fax their personal information or personal health information, first explain the risk of accidental disclosure or the possibility that the information may be deliberately intercepted by people other than the intended recipient and seek their consent before faxing.

- 1 point – Remove all personal identifiers and confidential information before faxing the information, wherever possible.

- 1 point – Before faxing personal information or personal health information, confirm that you have the correct fax number for the intended recipient and confirm with the recipient (or another employee in the office) the right number before sending.

- 1 point – When faxing personal information and personal health information, confirm that the recipient has taken appropriate precautions to prevent those without the requisite need-to-know from viewing the faxed document.

- 5 points – Always use a fax cover sheet clearly identifying the sender, the contact information for the sender, the intended recipient, the recipient's fax number and the total number of pages sent. Include a confidentiality clause that specifies that the faxed material is confidential, is intended only for the stated recipient, and is not to be used or disclosed by any other individual. The confidentiality clause should ask the individual in receipt of a fax received in error to immediately notify the sender and then return or securely destroy the personal information or personal health information (as requested by the sender).
    - 1 point – Requires use of cover sheet.
    - 1 point – Requires sender information be on the cover sheet.
    - 1 point – Requires recipient information be on the cover sheet.
    - 1 point – Requires that the number of pages sent be on the cover sheet.
    - 1 point – Requires a confidentiality notice.

- 1 point – After you have dialed a fax number carefully check the number before hitting "send".

- 1 point – Check the fax confirmation report to be certain that the fax went to the right place – check the number on the report against the confirmed recipient's number. Also check the number of pages actually transmitted and received. If you have designated one employee for faxing, that individual should check each day's fax history reports for errors or unauthorized faxes.

- 1 point – Retrieve all materials that have been faxed from the fax machine immediately. Do not leave faxes sitting on or near the fax machine. When faxing personal information or personal health information, stay by the machine to ensure that all materials were transmitted correctly.

- 1 point – Security precautions should be taken for faxes received after normal business hours.

c. Tips for Fax Equipment

- 1 point – If you have a need to continually fax personal information or personal health information, look into acquiring a fax machine that has enhanced security features such as encryption or other heightened security measures.

- 1 point – Fax machines should be physically located in an area of the office that prevents unauthorized individuals from viewing/retrieving faxed personal information and personal health information. Make sure to control access to the machine.

- 1 point – Be aware that your fax number likely will be reassigned once you have given up the number. If you require the number not to be used while you advise clients that the organization is moving or closing, check with your telephone service provider about options to rent the number for a period of time to ensure all clients have been contacted and have had the opportunity to update their contact information.

- 1 point – Safeguarding faxes not only applies to fax equipment. If you re-locate or if your contact information is changed, ensure that you update your fax number with all of your contacts and directories that included the previous number. Don't forget to destroy pre-printed forms, fax cover sheets and correspondence that refer to your previous number. This would include such items as letterhead, business cards, prescription forms, etc – all of which need to be replaced with updated information.

- 1 point – If you have pre-programmed a fax header into your fax machine that automatically prints the fax number on the recipient copy, update that information if your fax number or office contact information changes.

- 1 point – Be aware that fax machines now have hard drive and/or memories that store and retain information. When disposing of or selling a fax machine, ensure that the hard drive has been properly scrubbed to remove all information that was stored on the hard drive or memory.

- 2 points – Pre-program commonly used fax numbers and be sure to check those numbers regularly to ensure accuracy.
    - In order to get a mark for using pre-programmed numbers, there must also be a detailed plan for checking the accuracy of numbers on a regular basis.

Fax policies were scored on a total of 27 points.

The fax policies of several trustees also included other practices that are helpful for protecting personal health information. Bonus points were awarded for additional good practices.[40]

[160] One important safeguard overlooked in the evaluation system from the 2010 Report was the fax header. It is important that each fax containing personal health information sent from a trustee be printed with an accurate header giving the date of the fax transmittal, page number and number of pages as well as the outgoing fax number and trustee name. This will be added to our evaluation. Policies and procedures will therefore be evaluated on a score of 28 points.

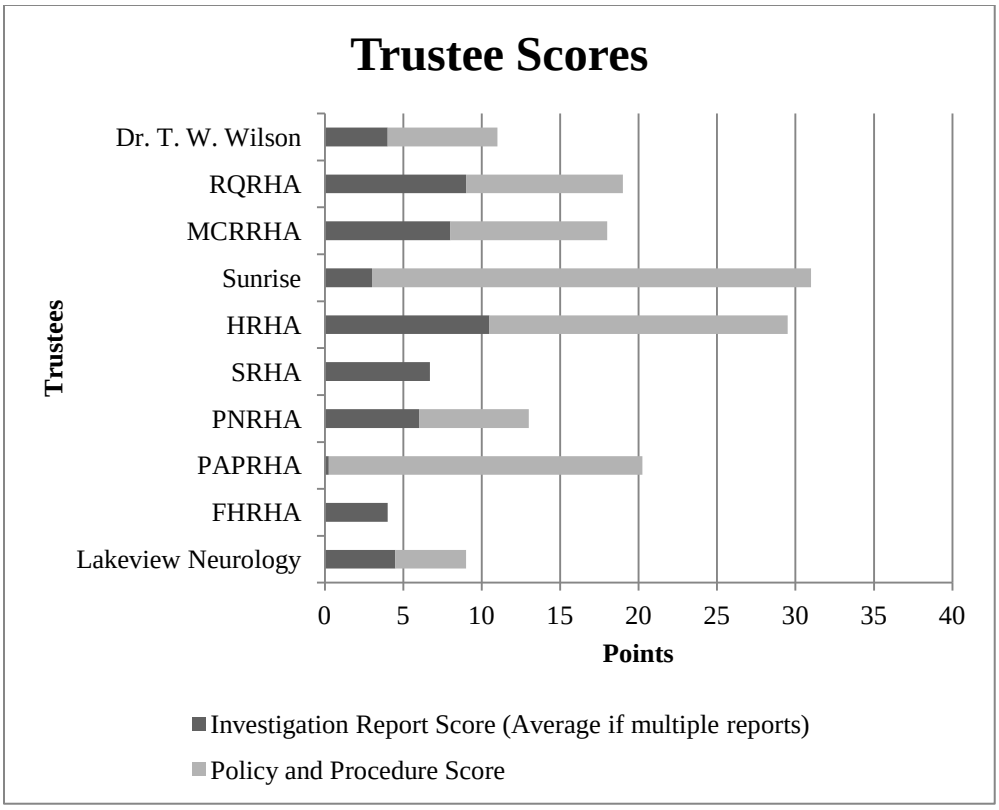
[40] *Supra* note 4 at pp. 19-22.

e. Commentary on the responses of trustees

[161] The full evaluation of each trustee, including comments, is appended at the end of this Investigation Report (Appendix A).

Trustee Scores

Trustee	Files	Investigation Report Score (Average if multiple reports)		Policy and Procedures Score		Total	
		Out of 12	%	Out of 28	%	Out of 40	%
Lakeview Neurology	013/2013	4.5	37.5%	4.5	16.1%	9	22.5%
FHRHA	014/2013 042/2013	4	33.3%	0	0.0%	4	10.0%
PAPRHA	015/2013 040/2013 057/2013 072/2013	0.25	2.1%	20	71.4%	20.25	50.6%
PNRHA	034/2013 044/2013 077/2013	6	50.0%	7	25.0%	11	32.5%
SRHA	039/2013 047/2013 075/2013	6.7	55.8%	0	0.0%	6.7	16.8%
HRHA	043/2013 073/2013	10.5	87.5%	19	67.9%	29.5	73.8%
Sunrise	045/2013	3	25.0%	28	100%	31	77.5%
MCRRHA	046/2013	8	66.7%	10	35.7%	18	45.0%
RQRHA	059/2013	9	75.0%	10	35.7%	19	47.5%
Dr. T. W. Wilson	060/2013	4	33.3%	7	25.0%	11	27.5%
Overall Average:		**5.6**	**46.6%**	**10.6**	**37.7%**	**16.1**	**40.4%**
Overall Average (RHAs only):		5.9	49.4%	11.8	42.0%	17.7	44.2%
Overall Average (Other Trustees):		4.3	35.4%	5.8	20.5%	10.0	25.0%



[162] Firstly, in the 2010 Report, I noted the disparity between the scores of RHAs and other trustees. In the present case, the same trend is clear. The average score for RHAs' investigation report was 49.4% while the average of the two physician trustees was 35.4%. More significantly, the averages of scores between the policies and procedures of the RHAs and the non-RHA trustees varied even more: 42.0% for RHAs compared to 20.5% for non-trustees. In the 2010 Report, I stated:

> HIPA has been in force since September 1, 2003. HIPA does not have different standards for different sized trustee organizations. All trustees are expected to have written policies and procedures to protect personal health information pursuant to section 16. Those policies should be appropriate for the particular trustee but all of them should address certain common elements. More importantly, patients in Saskatchewan should be able to expect the same level of protection of personal health information from all health care organizations no matter its size.
>
> The disparity between the quality of policies and procedures of RHAs and physicians offices and pharmacies is unacceptable. I encourage physician offices, pharmacies and other health care organizations to look to their regulatory bodies and professional

> associations for support in implementing robust privacy regimes within their organizations.[41]

[163] It is still my view that all trustees must have adequate written section 16 policies and procedures.

i. Investigation reports

[164] The overall percentage for the scores for trustee responses is most troubling for me. The overall average for all trustees was 46.6%. This suggests that trustees are not taking these misdirected fax breaches seriously. It may be understandable that if one or two faxes are sent astray, there is no need for a full scale investigation, so long as immediate, remedial action is taken. However, as the breaches described in this Investigation Report demonstrate, misdirected fax breaches occur regularly and begin to add up. This suggests a systematic problem that has not been addressed. The lack of detail found in the trustees' reports and the rate of reoccurrence gives little confidence that immediate remedial action is being undertaken when misdirected faxes occur.

[165] Most important is the lack of emphasis that the trustees have placed on devising meaningful processes to investigate, recommendations and solutions that address the root causes of the breaches. Most of the trustees described remedial actions that were taken such as speaking to its employees or making changes to the information of one patient or physician. However, out of the 20 breach files from the responsible trustees, only six of the investigation reports make effective recommendations for preventing future breaches (SRHA Files 039/2013-HIPA/BP and 047/2013-HIPA/BP, HRHA Files 043/2013-HIPA/BP and 073/2013-HIPA/BP, MCRRHA File 046/2013-HIPA/BP and RQRHA File 059/2013-HIPA/BP). These recommendations include developing awareness strategies regarding faxing personal health information and using cover sheets, strategies for ensuring patient information is correct when entered into EMRs, audit schedules for fax contact information in an EMR, moving from a faxing regime to a retrieval regime and even suggesting a provincial strategy for updating physician information in all EMRs.

[41] *Supra* note 4 at p. 24.

[166] I am not satisfied, however, that any of these trustees have taken enough steps to address all root causes effectively. Many of the recommendations are simply ideas and are unaccompanied by explanations as to how they will be executed.

[167] Further, with respect to the Category #1 breaches, many of those trustees have simply referred to eHealth Saskatchewan's investigation report on the matter. eHealth Saskatchewan's report makes many recommendations, however, they are all specific to eHealth Saskatchewan. With respect, none of them adequately address the matter of ensuring physician contact information is up-to-date because the involved RHAs themselves have a major role to play in this endeavour. As such, the RHAs cannot simply rely on eHealth Saskatchewan's recommendations.

[168] As will be discussed in the *Clear Accountability for RIS* portion of the next issue, I partly attribute the low scores to the involvement of eHealth Saskatchewan in the Category #1 breaches involving RIS. The RHAs relied too heavily on their IMSP to ensure the matter was properly investigated.

[169] I expect all trustees to fully investigate breaches of privacy brought to their attention, regardless of whether it involves a formal investigation from this office. Without complete investigations, I cannot be assured that root causes have been identified and addressed effectively.

ii. Notice to affected individuals

[170] In the 2010 Report, I made the following comments on notifying affected individuals:

> One of the best practices when responding to a privacy breach involving sensitive or prejudicial personal health information is to provide notification to the affected individual that the incident has occurred. My office's *Guidelines* document details when such notification is appropriate. Each fax in question contained personal health information which is inherently sensitive information and trustees were informed that this would be part of the evaluation.[42]

[42] *Supra* note 4 at p. 24.

[171] In the 20 relevant files in question in this Investigation Report, I received confirmation from the trustees that the affected individuals were notified for 14 of the files.

[172] PAPRHA did not confirm that any of the affected individuals were notified in any of the four files involving this RHA. This represents 55 individuals. Sunrise did not confirm whether the two affected individuals involved in its file had been notified either. The report from eHealth Saskatchewan from the Category #1 breach indicated that the affected individuals had been notified, however, PAPRHA and Sunrise did not confirm such as the other involved trustees did. Further, PNRHA did not confirm that the affected individual involved in its Category #2 breach was notified.

[173] As such, it appears that in 70% of the current files, the affected individuals were notified. This is an increase when compared with only 64.5% of trustees involved in the 2010 Report who provided notification. I applaud the trustees for this effort.

iii. Written policies and procedures

[174] The overall average of the trustees' scores for their written policies and procedures are also disappointing at only 37.7%. I note two of the RHAs did not have any such written policies and procedures.

[175] My office was generous in awarding points for the written policies and procedures. It was obvious that many of the policies and procedures were adapted from our *Helpful Tips – Privacy Considerations: Faxing Personal Information and Personal Health Information* resource. I encourage trustees to use this as a guide in developing their own section 16 policies and procedures; as clearly I use it as a basis for evaluation. However, trustees must tailor this guidance to their own specific needs and situations. For RHAs, there may be a need for different procedures in different business units within the organization.

[176] In evaluating the policies and procedures, all too often we encountered statements such as "Determine if there is an immediate time requirement that necessitates faxing the personal information or personal health information. Is there a quick and more secure way to forward the information to the recipient?" It is the hope, however, that a trustee's policies and procedures would provide more direction, such as defining parameters of the time requirement and listing alternative and more secure methods of communicating personal health information. I awarded a point each to four RHAs (PAPRHA, PNRHA, HRHA and Sunrise) for mentioning alternatives in its faxing policies and procedures because at least it prompts its employees to consider alternatives. However, more detail is required. I also question the enforcement of this policy as faxes are automatically generated from EMRs such as RIS and LIS.

[177] The preceding example was just one found when reviewing the policies and procedures. It is not enough that trustees' faxing policies and procedures simply mimic resources that are available for guidance. Policies and procedures must provide specific and tailored guidance for the specific needs of its staff.

[178] What is most disheartening is the lack of policies and procedures for ensuring fax numbers were up-to-date. Out-of-date fax numbers was one of the root causes in four of the five categories of breaches. Only one of the involved trustees' policies and procedures provided any mention of the crucial process of ensuring fax numbers are up-to-date – MCRRHA. However, we did not award a point to MCRRHA for this as the policy simply stated: "Each program that has a fax machine in their area, shall designate a staff member to annually confirm speed dial numbers of that machine." This is not enough detail for the effective management of preprogrammed fax numbers. Trustees were warned about this important safeguard in the 2010 Report where I stated the following:

> To their credit, many trustees indicated to my office that it is their policy to use preprogrammed numbers for frequently used faxed numbers. However, this would only be a best practice if there were policies and procedures in place to ensure that the numbers are kept up to date. As such, the trustees were not awarded a point for using

> preprogrammed numbers without adequate policies and procedures for updating the numbers.
>
> Many trustees had, within their policies or correspondence, statements such as "Preprogrammed fax numbers should be checked regularly." However, I do not consider this to be adequate for employees tasked with the responsibility for ensuring preprogrammed numbers are up-to-date. As indicated, only 5 trustees were awarded a point for updating policies and procedures. An adequate policy or procedure would give direction as to who must update the numbers, how often they are to be updated and what sources are used to verify them.[43]

[179] In the evaluations, I also chose not to award a point to trustees using RIS and having a policy or procedure that indicated that a fax cover sheet must contain the sender's contact information. This included PAPRHA, HRHA, Sunrise and MCRRHA. During this investigation, eHealth Saskatchewan provided us with a sample cover sheet that accompanies all faxes from RIS. The following is a reproduction of the coversheet:

[43] *Supra* note 4 at p. 29.

Saskatchewan Health
Confidential
Medical Imaging Results

Cypress Regional Hospital (306) 778-9457

Lloydminster Hospital (306) 820-5971

Victoria Hospital (306) 765-6076
786-0423

La Ronge Health Centre (306) 425-2422
882-2672 ext202

Outlook and District Health Centre
(306) 867-8676 ext242

Kindersley and District Health Centre
(306) 463-1000 ext214

Royal University Hospital (306) 655-2375

St. Paul's Hospital (306) 655-5149

Battlefords Union Hospital (306) 446-6475

Moose Jaw Union Hospital (306) 694-0381

Yorkton Regional Health Centre (306)

Rosetown Health Centre (306)

Biggar Union Hospital (306) 948-3323 ext228

Unity and District Health Centre
(306) 228-2666 ext283

Saskatoon City Hospital (306) 655-8600

Humboldt Hospital (306) 682-8127

To: [name removed]

Pages: [information removed]

Date/Time: [information removed]

Note:

This cover sheet is used by multiple medical imaging departments. **Please refer to the attached report for the name and phone number of the sending station.**

Confidential Notice: This material is intended for the individual or entity to which it is addressed. If you are not the intended recipient, any use, disclosure, copying or communication of the contents of this transmission is strictly prohibited. If you have received this communication in error, please notify the Medical Imaging department immediately by telephone and return this material (and all copies) to us by mail.

[emphasis added]

[180] A fax cover sheet cannot prevent a misdirected fax. However, it is meant to act as protection when a fax has gone astray. The coversheet is meant to prevent an unintended recipient from looking at the personal health information attached to it. All the pertinent details should be on the coversheet so the recipient can take appropriate action without looking at the attached personal health information. The RIS 'common' coversheet really serves no purpose if an unintended recipient must examine the attached personal health information for sender information. Further, the best practice would be to advise an unintended recipient to contact the sender trustee and then choose the most appropriate course of action with respect to copies of the personal health information. The confidentiality notice above is vague and unclear as to which "medical imaging department" and what is meant by "us".

[181] Another important safeguard in mitigating harm when faxes have been misdirected is the fax header. Fax headers are generally programmed in the sender's fax machine or system and then printed on the receiver's copy. A fax header should include the sender trustee's name and fax number, page number and number of pages in the fax as well as date and time of the fax transmittal. This is an important safeguard as it is automatic and does not rely on an individual or system to complete an accurate cover sheet.

[182] Each fax machine can be individually programmed. However, there is no standard for headers on faxes sent from EMRs. It appears that RIS only prints the date and time of transmission as well as page information. eHealth Saskatchewan was unable to confirm this. Further, the fax headers sent from LIS provides counterintuitive information. It appears that the general fax header from LIS appears as follows:

> [Date and time of transmission] Saskatchewan Health via VSI-FAX Page [x] of [x] [Unknown number]

[183] In one of the files involving misdirected faxes from LIS (PAPRHA File 015/2013-HIPA/BP, Category #2), we had trouble identifying the sender trustee due to the fax header. The fax header did not match the information on the fax. It is conceivable that a trustee might have faxed personal health information originally produced by another

trustee. We asked both the Ministry of Health and eHealth Saskatchewan about this fax header in December 2012. They were unable to provide any information about this header. We then approached PAPRHA which confirmed the fax was sent from its LIS. In our notification letter of March 14, 2013, we specifically asked PAPRHA to address this issue. It did not.

[184] In the Background Section, I referenced File 058/2013-HIPA/BP that my office had opened with an RHA which will remain anonymous. The personal health information faxed to the third party in Moose Jaw appeared to be a graph that captures an identifiable individual's sinus rhythm which was prepared at a certain hospital in the RHA. The personal health information was not accompanied by a cover sheet nor does it have a fax header. There is no way to identify the sender trustee to advise of the mistake to either address privacy concerns or ensure continuity of care. The RHA has provided arguments indicating the fax was not sent from one of its machines. We cannot make a determination one way or the other.

[185] Without the necessary information, recipients will not be able to report misdirected faxes to the sender trustees. An effective safeguard would make it easy for the recipient to know who sent the fax and what to do with the personal health information.

[186] When the 2010 Report and the resources referenced were written, they did not address a faxing feature within the EMR. The introduction of this technology brings a whole new dimension to the practice of faxing personal health information. Most EMRs are designed to automatically communicate personal health information with other trustees by means of faxing. Every EMR is different with respect to how contact information is uploaded, managed and updated. Yet not one of the involved trustees' faxing policies and procedures address these new challenges.

[187] Finally, policies and procedures need to be communicated to staff effectively. This includes timely reminders to exercise due care and caution when faxing, whether it be

faxing manually or using an auto-suggest feature. Only two of the ten policies and procedures of the trustees addressed this issue.

[188] Going forward, trustees must do better with faxing policies and procedures. It is expected that the policies and procedures will not simply mimic available resources, but be tailored to the organization – and individual units within the organization if necessary. They must be specific enough to provide real guidance to trustees. The policies and procedures should also cover what to do if misdirected faxes are sent or received. Processes should be added to audit the sources of contact information. Finally, they should include strategies to ensure employees understand and are regularly reminded of the importance of following the procedures.

4. Tying it together: Do common root causes reflect systematic failures on the well established practice of faxing personal health information?

[189] Faxing is a well established practise for the communication of personal health information in the health care field in Saskatchewan. This Investigation Report accounts for between 495 and 1079 patients that have had their privacy breached as a result of misdirected faxes.

[190] The majority of these misdirected faxes were proactively reported to this office by the IMSP in question, eHealth Saskatchewan. The breaches in Categories #1 and #5 were reported on behalf of the responsible trustees, accounting for 382 of the breaches.

[191] However, my office was alerted to the other breaches through the media and third parties. I do not know how many misdirected faxes are received by unintended recipients each day who do not report it to our office, or to anyone at all.

[192] It is easy to write off a misdirected fax as an unfortunate accident. However, by examining these breaches and the 2010 Report, two clear systematic failures become

evident: the challenge of ensuring information is up-to-date and the lack of clear accountability for breaches involving RIS.

a. Keeping information up-to-date

[193] The 2010 Report concluded that the following three factors contributed to the misdirected faxing breach discussed in that document:

> As listed above, the three key factors that caused these privacy breaches are as follows:
>
> - a change of fax number;
> - use of outdated pre-programmed fax numbers; and
> - carelessness of employees due to lack of training.[44]

[194] Many of the trustees involved in the 2010 Report pointed to pre-programmed numbers that were not updated in individual fax machines as the culprit for their misdirected faxes.

[195] As noted earlier, a root cause for four of the five Categories of breaches with respect to this Investigation Report also stemmed from incorrect or outdated fax numbers either in traditional directories or in electronic systems.

[196] In the breaches of Categories #1 and #5, incorrect fax numbers were entered into RIS, an EMR utilized by several trustees.

[197] Incorrect or outdated fax numbers are to blame in several of the Category #2 breaches. This includes outdated information in EMRs such as RIS, LIS and Accuro. Incorrect patient information also contributed to one of the faxes of Category #2 as well.

[198] Category #4 breaches were attributed to the inability to update patient and provider information.

[44] *Supra* note 4 at p. 27.

[199] Finally, the root cause of the Category #3 misdirected faxes was a low-tech error in a paper directory.

[200] The problem of outdated information covers all of these breaches whether an electronic system was used or not. As such, I must take a closer look at how fax contact information and patient information is updated and changed by trustees.

[201] First, I will consider traditional paper directories such as the CPSS *Physicians Mailing List – January 2013*. CPSS produces a directory of physicians for the province twice a year – January and July. Organizations and individuals can subscribe to this directory for a fee. However, single issues of the directory can also be purchased for a fee. For those with a subscription, notices advising of updates, changes and corrections are produced once a month except for June and December as the updates for these months are included in July and January when the full directories are published.

[202] The CPSS directory may be the most up-to-date source of physician contact information as updates are requested at the time of annual renewal for licenses. Physicians are also expected to notify CPSS of a change in office address and/or telephone numbers; however the College has no bylaw or policy mandating such notification. Nonetheless, notifications of January 2013, February 2013, March 2013, April 2013 and May 2013 to subscribers corrected a total of 11 fax numbers and advised of six other fax number changes with respect to the CPSS *Physicians Mailing List – January 2013.*

[203] Many trustees simply tuck the updates loosely into the directory when they are received. This is not a secure practice as the updates could fall out and get lost or be ignored when faxing. It is best practice for trustees to go through the directory manually and note updates in ink.

[204] CPSS has indicated that it is considering eliminating the paper directory altogether in favour of an electronic version that can be updated in real time. This would be a major improvement. Further, after being alerted to my investigation in this matter, CPSS has

made some helpful changes to its process. Individual "Physicians Mailing Lists" can no longer be purchased. A subscription must be obtained so that updates will be received. Also, with each update, CPSS will attach a page long disclaimer discussing the need to make immediate changes to contact information in electronic systems, preprogrammed systems and paper copies of the directory. I applaud CPSS for these actions.

[205] Although the CPSS physician directory appears to be a dependable source for physician contact information, it is fallible. Other professional colleges for the health care field also maintain directories such as this. As depicted in the first diagram, this information is what was originally loaded into EMRs such as RIS. Therefore, mistakes in these directories can have a trickledown effect.

[206] Next, I must consider electronic systems and the accuracy of contact information used for faxing within them.

[207] As explained earlier in this Investigation Report, it is the responsibility of the trustee sending the personal health information to ensure that it is kept secure until it reaches whoever it is being communicated to. As such, it is the sender trustee's responsibility to ensure that a fax number is correct before a fax is transmitted. When using an electronic system, such as an EMR which sends faxes automatically, the trustee must ensure the fax numbers and other relevant information are constantly up-to-date to avoid breaches.

[208] eHealth Saskatchewan acts as an IMSP managing several of the EMRs which several trustees in the province use. eHealth Saskatchewan had explained that the contact information in some of these systems such as LIS is managed and updated by trustees themselves. In other words, contact information for a particular physician may be updated in one trustee's LIS, while it is out of date in another's.

[209] An example of this is illustrated in the Category #2 breaches. The LIS of each trustee is not interoperable with that of another; as such, trustees must update contact information within its own LIS. Physician #3, referenced in these breaches, at one time worked for

the third party in Moose Jaw. She now practices elsewhere. PAPRHA (File 015/2013-HIPA/BP) sent a fax from its LIS to Physician #3 on October 10, 2012 which ended up with the third party in Moose Jaw. PAPRHA was apparently alerted to the mistake by the third party shortly after the incident and by this office on or about March 14, 2013. Although PAPRHA has never indicated if it had updated Physician #3's information in LIS, it is our expectation that it did so immediately. Then PNRHA sent a fax to Physician #3 from its LIS on June 6, 2013. Even if PAPRHA had updated Physician #3's contact information in its LIS prior to this date, the change would not have affected PNRHA's LIS.

[210] By contrast, the contact information of some of the EMRs, such as RIS, are managed centrally by the IMSP, even though ultimate responsibility rests with the trustees. I refer to the first diagram in this Investigation Report which explains how contact information in RIS was originally populated. eHealth Saskatchewan has implemented an internal procedure for updating fax numbers which it has shared with the applicable trustees. The procedure (effective October 5, 2012) is as follows:

> In order to effectively and efficiently update Provider information the following process is being implemented. Providers may include physicians, nurse practitioners, chiropractors, etc.
>
> The most current version of the RIS Request – Provider form is located in the RIS-PACS SharePoint site under the Provincial RIS Documents\ RIS Support – RIS Request Forms.
>
> 1) New Provider:
>
> b) Verify the Provider first/last names with Provider Registry.
>
> c) Obtain the Person ID from your regional WinCIS administrator.
>
> d) Download the RIS Request – Provider form from the RIS-PACS SharePoint Site.
>
> e) Fill in all required fields in the RIS Request – Provider:
>
> i) Request Type is "New" (select from dropdown)
>
> ii) Region is your region (select from dropdown)
>
> iii) "I have checked for aliases and, where applicable, confirmed these changes with affected regions" – select "Yes" from the dropdown. The

field will change from Red to Green. Note you will be notified by Apps support that your request will not proceed until you have selected "Yes".

f) Email the request to the eHS Service Desk. The email's Subject line should be "RIS Provider Request – Add <provider name>. Attach the Request form to the email prior to sending.

2) Update Provider:

a) Download the RIS Request – Provider form from the RIS-PACS SharePoint Site.

b) Fill in all required fields in the RIS Request – Provider form:

i) Request Type is "Update" (select from dropdown)

ii) Region is your region (select from dropdown)

iii) "I have checked for aliases and, where applicable, confirmed these changes with affected regions" – select "Yes" from the dropdown. The field will change from Red to Green. Note you will be notified by Apps support that your request will not proceed until you have selected "Yes".

c) Fill in the information being updated. Include both the Current and the New information.

d) Email the request to the eHS Service Desk. The email's Subject line should be "RIS Provider Request – Update <provider name>. Attach the Request form to the email prior to sending.

3) Inactivate Provider:

a) Download the RIS Request – Provider form from the RIS-PACS SharePoint Site.

b) Fill in all required fields in the RIS Request – Provider form:

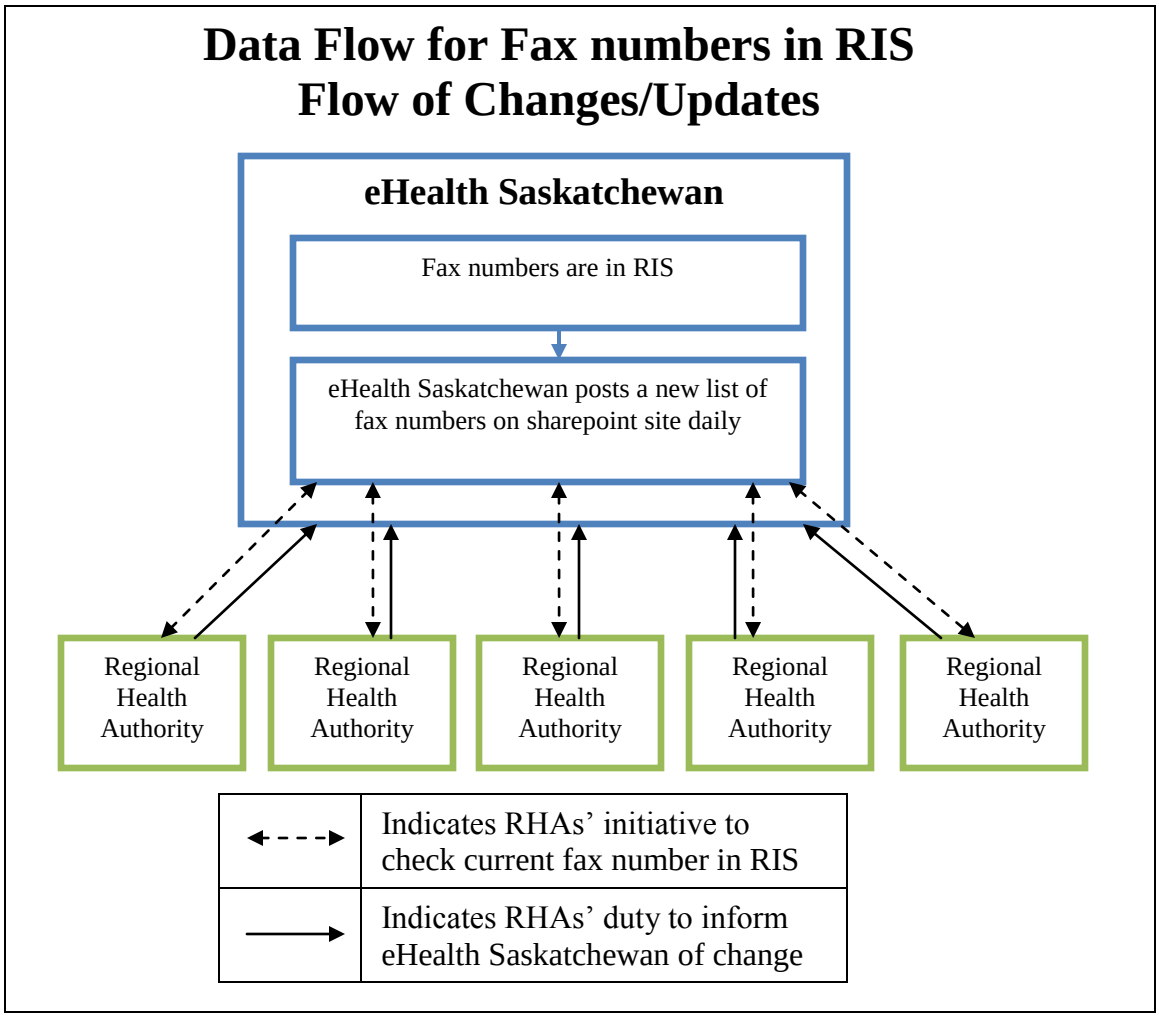
i) Request Type is "Inactivate" (select from dropdown)

ii) Region is your region (select from dropdown)

iii) "I have checked for aliases and, where applicable, confirmed these changes with affected regions" – select "Yes" from the dropdown. The field will change from Red to Green. Note you will be notified by Apps support that your request will not proceed until you have selected "Yes".

c) Email the request to the eHS Service Desk. The email's Subject line should be "RIS Provider Request – Inactivate <provider name>. Attach the Request form to the email prior to sending.

[211] This procedure is more simply described by the following diagram designed by my office:



[212] eHealth Saskatchewan has informed my office that RHAs must confer with each other if there is a disagreement regarding a physician's information. This is partly reflected in the policy/procedure. Although there appears to be instructions to advise other RHAs that a change has even been made, it is unclear to me as to how this occurs and who in an RHA must be notified.

[213] It is encouraging that eHealth Saskatchewan has taken this initiative. However, this procedure is entirely dependent on the participation of the trustees. It is disappointing that none of the RHAs involved with RIS have demonstrated that they have responded to this procedure by developing their own policies and procedures for compliance.

[214] To complicate matters further, there are circumstances which make it difficult to keep physician contact information up-to-date. For instance, locums are physicians that travel from community to community to relieve permanent physicians who need to take time off or to fill other needs on a temporary basis. As such, there are conflicting views among RHAs and eHealth Saskatchewan about whether they should be even entered into RIS. There is no official policy on the subject which may create inconsistencies and the potential for breaches.

[215] Another example of a challenge to maintain current contact information in EMRs is a configuration in the system that allows only one assigned fax number per physician. For example, a physician may have their own solo-practice and also pick up shifts in a department in a hospital. The physician would be the trustee of the personal health information involved in his or her solo practice, but the RHA would be the trustee of the personal health information involved at the hospital. We queried this practice of eHealth Saskatchewan and whether it presents a problem. It provided us with the following response on October 23, 2013:

> Back in the early days of eHealth implementing the Cerner RIS a decision was made with the members of the Clinical Working Group (CWG) that each Provider would only exist in the RIS once. With that decision, we are constrained to only having one fax number to fax reports to a provider. However, technically if we were to set multiple instances of a provider up in RIS (i.e. John Smith – Lloydminster, John Smith – North Battleford), we could have separate fax numbers for each of them. However, this creates further complications in that our RIS providers generally need to match up (i.e. they have an alias) with a provider from the ADT system. If we wanted 2 providers in RIS, we would need to have 2 providers in the ADT system that would correspond to them (if we wanted those providers to automatically appear on the RIS order).
>
> In today's world, I think there may be different practices happening in different RHAs when physicians work in more than one location. Sometimes, the reports are simply sent to whatever fax number is set up for that provider in RIS. Sometimes, the location where the provider is working (i.e. 123 Medical Imaging Services) is setup as a Provider (so, the facility or location is the provider in this case, not the actual person) in the RIS and then the workflow is that this Provider is added as a consulting physician so that the report will actually go to wherever this provider is working. Sometimes, the reports are delivered to our System Administrators printer in the RHA and they are responsible for ensuring the report gets to the provider.

[216] Taking into account the issue detailed in the quote above, it is unclear what is being done to resolve the issue. RIS's original design of one fax number per health care provider does not reflect the reality of locums or physicians working for multiple trustee organizations. eHealth states, in the above quote, that the location's fax number instead of a health care provider's one of many fax numbers is what should be inputted into RIS. If this is a solution, then the misdirected faxes discussed in this Investigation Report is evidence that this solution has not been implemented successfully or that it is not the solution to resolve this issue.

[217] We cannot continue down the path where RIS's design of one fax number per health care provider is a stumbling block and a reason for misdirected faxes that results in violations of Health. Either RIS is re-designed to reflect real word needs or RIS, as it is currently designed, is used in a way that will be in compliance with HIPA.

[218] Further, it is unclear how and when physicians are removed from these systems once they have left the province or retired, as this also appeared to be a problem in the Category #2 breaches.

[219] However, provider contact information is not the only information that must be kept up-to-date in these systems to prevent misdirected faxes. As we have seen, patient personal health information must also be accurate.

[220] Pursuant to section 16(a) of HIPA, trustees have a duty to maintain the accuracy of personal health information as follows:

> 16 Subject to the regulations, a trustee that has custody or control of personal health information must establish policies and procedures to maintain administrative, technical and physical safeguards that will:
>
> (a) protect the **integrity, accuracy** and confidentiality of the information;
>
> [emphasis added]

[221] In File 014/2013-HIPA/BP, the personal health information of a patient of FHRHA was faxed by RIS to the third party in Moose Jaw as a result of incorrect information in another EMR, WinCIS. The two EMRs communicate with each other.

[222] Further, as demonstrated in the Category #4 breaches, patient information can change before a fax is to be sent. A configuration setting in RIS for those trustees would not allow such changes to be made in RIS. EMRs must have the capability to adapt to changes to prevent misdirected faxes.

[223] As I have seen, there are many challenges to ensuring that trustee contact information is kept up-to-date, both in electronic and non-electronic systems, for the purposes of preventing privacy breaches caused by misdirected faxes. It is easy to see, yet deeply troubling, that the faxing policies and procedures of the involved trustees cannot be fully effective in remedying these problems.

[224] Trustees must devise strategies to audit and update all sources of fax contact information regularly. This includes fax information in all EMRs and EHRs, preprogrammed features on individual fax machines and traditional paper directories. Once a year is insufficient. Further, those trustees using RIS must work with eHealth Saskatchewan and other RHAs to devise a strategy for updating contact information that is fair to all those accountable.

b. Clear accountability for RIS

[225] RIS was a central issue in the Categories #1, #4 and #5 breaches. As such, it was a major focus of this investigation. It became clear that confusion over ultimate accountability for personal health information contained in RIS is a factor in both the breaches and the disappointing responses thereto.

[226] Clearly distinguishing trustee and IMSP roles is important. In my Investigation Report H-2005-002, I stated:

> The question of an information management services provider is important since the scheme of HIPA is to vest in a given trustee clear responsibility for protecting the privacy of [an individual] and the confidentiality of [his/her] personal health information.[45]

[227] Accountability for EHRs and EMRs is a very complex issue.

[228] One example of the complexity from this investigation is how physician contact information was originally loaded into RIS. As trustees have ultimate responsibility for the faxes sent from RIS, eHealth Saskatchewan attempts to ensure each trustee RHA reviewed fax numbers it would be using before they were loaded into RIS. However, as each subsequent RHA began to use RIS and submitted their fax numbers, it is unclear whether the first RHAs had any knowledge as to any changes being made to the fax numbers they had already submitted and were accountable for. This certainly became an issue when SRHA began to use RIS and several fax numbers were changed to incorrect numbers. A decision made by SRHA and eHealth Saskatchewan to break from the established procedure and load unverified fax numbers into RIS affected the other RHAs. Those RHAs were nonetheless accountable for their breaches.

[229] The Category #1 breaches were first reported to my office by eHealth Saskatchewan, the IMSP for the responsible trustees. At that time, it was my understanding that eHealth Saskatchewan was working with the trustees to deal with this breach. My office opened a preliminary file with eHealth Saskatchewan, which means, when breaches are proactively reported, we monitor the situation to ensure it was dealt with appropriately without a full investigative effort from our office. For reasons outlined earlier, it became necessary for my office to open formal investigation files – one with each of the responsible RHAs. In our notification letter, my office asked that each RHA provide us with a copy of its own investigation report as well as section 16 faxing policies and procedures. We asked that they provide this material no later than August 30, 2013.

[45]SK OIPC, Investigation Report H-2005-002 at p. 141, available at www.oipc.sk.ca/reviews.htm.

[230] Shortly after opening the files with each of the trustees involved, eHealth Saskatchewan provided us with a copy of its final investigation report. As a result, we did not receive reports from three of the trustees. Further, most RHAs' reports simply referred to eHealth Saskatchewan's report and did not provide information specific to its own organization. The average score for investigation reports for Category #1 breaches was 4.9 out of 12, lower than the overall average of 5.6. Further, my office noticed a general lack of comprehension of the events that contributed to this breach. None of the RHAs explained with sufficient detail what had occurred.

[231] I have previously commented on the importance of the responsible trustee, or public body, responding to privacy breaches. My Investigation Report F-2013-003 discussed a situation where a Ministry of Highways and Infrastructure employee accessed and used personal information in a Saskatchewan Government Insurance (SGI) database without authority. SGI took the lead in responding to the breach. However, as the employee was under the supervision and control of the Ministry, I found it should have responded as it needed to ensure the affected individual that there were safeguards in place to prevent other employees from taking similar actions.[46] The same principles apply in this situation.

[232] Further, in its joint investigation report for Files 043/2013-HIPA/BP (Category #1) and 073/2013-HIPA/BP (Category #4), HRHA raises the possibility that these two categories of breaches are indistinguishable, one from the other. In other words, some of the breaches identified in Category #1 were in fact caused by the issues arising in Category #4. HRHA stated:

> The information identified in the second reported breach is two of the seven breaches that were investigated and reported on by eHealth entitled ***Investigation Report 2012-029 RIS Faxing Review*** (Investigation Report) attached as Appendix A. As a result, this report will address both requests from the OIPC for an investigation and report.

[233] HRHA did not elaborate on this point. Neither eHealth Saskatchewan nor any of the other RHAs involved in both Categories #1 and #4 addressed this possibility. Given the

[46]SK OIPC, Investigation Report H-2013-003 at [85] to [90], available at www.oipc.sk.ca/reviews.htm.

low investigation scores by the RHAs and this revelation by one RHA, this also raises concern that the RHAs were not fully invested in investigating these breaches.

[234] The underwhelming response caused my office to probe deeper into this accountability issue. We asked the RHAs in question to provide us with copies of IMSP agreements between themselves and eHealth Saskatchewan for the use of RIS. The response we got from the RHAs was perplexing.

[235] Not every RHA provided the same documents or any documents at all. The documents that were provided are as follows:

- *RIS Provider Update Process* (October 5, 2012),
- A RIS Fax Cover Sheet,
- *Saskatchewan Health Information Network – Confidentiality Agreement* (May 2004),
- *Saskatchewan Health Information Network – Master Services Agreement* (May 2004),
- *PACS Joint Services/Access Policy* (January 24, 2012 – Version 6.0),
- *Minimum Standards For Participation In The Provincial PACS* (April 2009), and
- *PACS Source Trustee Committee Terms of Reference* (November 30, 2010).

[236] The only two documents provided that reference RIS are not agreements. One is a process for which contact information of health care providers are updated in RIS. The other is a sample of the coversheets that accompany all faxes from RIS.

[237] The *Saskatchewan Health Information Network – Master Service Agreement* and *Saskatchewan Health Information Network – Confidentiality Agreement* referenced above are between Saskatchewan Health Information Network (SHIN) and the RHA that provided it to our office. From discussions with eHealth Saskatchewan, it is my understanding that each of the RHAs in question would have signed the same documents around 2004. SHIN is the predecessor to eHealth Saskatchewan. It appears that these

documents are almost ten years old and outdated. They make no reference to RIS and do not appear to be applicable in this case.

[238] It is also my understanding that although RIS and PACS, both managed by eHealth Saskatchewan, work together to manage diagnostic imaging images, results and other related information, both are distinct electronic systems. Most significantly, all of the trustees using PACS have the ability to view all personal health information within this system. However, RIS is unique to each trustee so trustees do not have access to each other's RIS system.

[239] As such, the PACS related documents are not applicable to RIS.

[240] eHealth Saskatchewan has confirmed that no written agreements currently exist between itself and the RHAs for the purpose of RIS.

[241] Written agreements are absolutely essential between a trustee and an IMSP. I discussed the importance of having written agreements with IMSPs in my Investigation Report H-2011-001.[47]

[242] For the purposes of this investigation, I reviewed the *PACS Joint Services/Access Policy* (January 24, 2012 – Version 6.0) document. Although it is outdated and applies to PACS, such a document would have been helpful in this situation in assisting all of the parties understanding the accountability structure for RIS in this case. The PACS agreement confirms that RHAs are the responsible trustee of the personal health information within PACS as follows:

> **5.1 <u>Accountability.</u>**
>
> Each Diagnostic Image and Result will be associated with the RHA ("Source Trustee") that provided the diagnostic imaging service.
>
> **<u>The Source Trustee will be considered the "trustee" for the purposes of HIPA for the Diagnostic Image Data related to its Diagnostic Images and Results.</u>**

[47] SK OIPC, Investigation Report H-2011-001 at [142] to [147], available at www.oipc.sk.ca/reviews.htm.

...

It is the responsibility of each Source Trustee and Accessing Trustee to ensure they have appropriate safeguards in place and are otherwise in compliance with HIPA and other applicable laws.

It is eHS's responsibility to ensure it has appropriate safeguards in place and is otherwise in compliance with HIPA and other applicable laws.

...

5.6 Safeguards.

Each Source Trustee and Accessing Trustee agrees that appropriate physical, organizational and technological measures as outlined in section 5.1 will be put in place within their organization to protect the security and confidentiality of the Diagnostic Imaging Data and to ensure that this data is only used on a need to know basis for the Authorized Health Purposes.

Each Source Trustee and Accessing Trustee agrees to follow any security procedures approved by all of the Source Trustees and delivered to the Accessing Trustee from time to time.

...

5.9 Complaints.

All complaints relating to PACS received by the Centralized Privacy Service will be referred to the Lead Source Trustee. The Lead Source Trustee will refer, coordinate or address issues as appropriate depending on the nature of the complaint.

All Source Trustees agree to have appropriate and reasonable policies, procedures and forms to address privacy concerns or complaints raised by patients/clients. To the extent that a privacy concern or complaint involves multiple Source Trustees (RHAs), the Source Trustees will work together to address the patient/client's concerns.

Any unresolved complaints may be forwarded by the patient/client to the Office of the Information and Privacy Commissioner (Sask).

…

7. Termination

(a) eHS may terminate a Source Trustee's or Accessing Trustee's access to the eHS Services:

(i) without cause upon 60 days prior written notice; or

(ii) immediately upon material breach of this Schedule or the Policy by the Source Trustee or Accessing Trustee;

(b) The Source Trustees or Accessing Trustees may terminate the eHS Services:

(i) without cause upon 60 days prior written notice; or

(ii) immediately upon material breach of this Schedule or the Policy by eHS;

(c) Upon termination of a Source Trustee's access to PACS, the patient/client data for that Source Trustee will be transferred to the Source Trustee. The Source Trustee will be responsible for all reasonable costs associated with such transfer.

[emphasis added]

[243] With respect to PACS, this agreement confirms the following views:

- Under HIPA, the RHAs would be the responsible trustee for its personal health information, and subsequently, for what it faxes.
- The RHAs must have appropriate safeguards in place.
- That the RHAs would have ultimate responsibility for responding to privacy breaches.
- eHealth Saskatchewan, as the IMSP, is responsible to the RHAs for any role it played in privacy breaches. RHAs would be able to terminate its use of eHealth Saskatchewan's services if it did not support those RHAs' compliance with HIPA.

[244] Unfortunately for RIS, no such document exists. There is nothing for either party to rely on for guidance when dealing with breaches or determining accountability.

[245] This may be the reason for the skeletal responses from the RHAs and the lack of effective strategy proposed thus far to ensure faxing information in RIS is up-to-date.

[246] In the absence of written agreements in regards to the RHAs involved in Categories #1, #4 and #5, I must look to HIPA for guidance. However, HIPA itself is not complete. The relevant sections are as follows:

18(1) A trustee may provide personal health information to an information management service provider:

(a) for the purpose of having the information management service provider process, store, archive or destroy the personal health information for the trustee;

(b) to enable the information management service provider to provide the trustee with information management or information technology services;

(c) for the purpose of having the information management service provider take custody and control of the personal health information pursuant to section 22 when the trustee ceases to be a trustee; or

(d) for the purpose of combining records containing personal health information.

(2) Not yet proclaimed.

(3) An information management service provider shall not use, disclose, obtain access to, process, store, archive, modify or destroy personal health information received from a trustee except for the purposes set out in subsection (1).

(4) Not yet proclaimed.

(5) If a trustee is also an information management service provider and has received personal health information from another trustee in accordance with subsection (1), the trustee receiving the information is deemed to be an information management service provider for the purposes of that personal health information and does not have any of the rights and duties of a trustee with respect to that information.

18.1(1) **Subject to the terms of any agreements made pursuant to subsection 18(2), the Saskatchewan Health Information Network** or a prescribed person may create comprehensive health records with respect to individuals.

(2) A comprehensive health record with respect to an individual:

(a) consists of records containing the individual's personal health information that are provided by two or more trustees;

(b) is created for the purposes of:

(i) compiling a complete health history of the individual; and

(ii) providing access to that history to any trustee; and

(c) is stored and controlled by the Saskatchewan Health Information Network or the prescribed person that created it.

(3) The Saskatchewan Health Information Network or a prescribed person shall provide a trustee with access to a comprehensive health record only if:

> (a) access is authorized by each trustee whose records were used to compile the comprehensive health record; and
>
> (b) either:
>
> (i) the subject individual has provided consent in writing authorizing the trustee to have access; or
>
> (ii) one of the purposes or circumstances set out in subsection 27(2) or (4) exists and the subject individual has not made a direction pursuant to subsection 8(2) or (3).
>
> (4) Nothing in this section prevents the combining of records of personal health information where the combination is not for the purpose of creating a comprehensive health record.
>
> [emphasis added]

[247] Although I cannot be sure, it appears that section 18(2) of HIPA is meant to require some sort of agreement between a trustee and an IMSP. However, section 18(2) of HIPA has not yet been proclaimed even 10 years after the Act was enacted. Further, as noted above, HIPA has not been updated to reflect the change in SHIN.

[248] As it appears to be incomplete and out-of-date, HIPA does not provide guidance on accountability with respect to the EMRs that eHealth Saskatchewan manage.

[249] The lack of clear formal accountability rules is evident in the RIS breaches and the responses by the trustees.

[250] As previously noted, the trustees involved in this Investigation Report were given draft copies on or about November 7, 2013. My office asked if each one would notify us of any factual inaccuracies and if they would indicate which of my recommendations it would be complying with. We also asked for some sort of timeline or plan if those details were available. My general observation is that the trustees' responses to those recommendations that require the involvement of eHealth Saskatchewan were not as decisive and lacked any meaningful detail (see Appendix B). My feeling is that these

trustees are still placing eHealth Saskatchewan, the IMSP, in the driver's seat with respect to these decisions.

c. The future

[251] Faxing is an antiquated technology. It is inherently insecure as many faxes are not encrypted and it is easy to fax to an incorrect number, either manually or through lack of updates to relied upon directories.

[252] The EHR is being built so that healthcare providers have timely access to relevant information. In other words, the ultimate goal would be for a trustee with a need-to-know to be able to access relevant personal health information of a patient at a click of a button. The question then becomes: will healthcare professionals no longer have a need for faxing?

[253] eHealth Saskatchewan has made the following comment: "It is eHealth Saskatchewan's goal to eliminate faxing once all required information is available to all providers electronically."

[254] Our observation is that quite apart from any particular technology, privacy risks will continue to exist. Faxing may be a particularly vulnerable and high-risk-to-privacy technology but as this Investigation Report documents, more sophisticated computer technology may well eliminate or at least minimize certain risks but may also create or expand new and other risks. Auto-dialing and stored memory of contact information may mean that instead of one misdirected fax there may be hundreds all sent to the incorrect address because there was a lack of care in inputting data. Many of the misdirected faxes discussed in this Investigation Report reflect inadequacies in policy, procedure, and training. It would be a serious error to expect that inappropriate use or disclosure of personal health information will cease to be a problem for public confidence in our health care system once fax machines are displaced by more sophisticated computer equipment.

[255] In any event, this province is not in a position to eliminate faxing yet. Not all trustees use an EMR. Further, many providers prefer to have personal health information 'fed' to them such as an automatic fax update, rather than retrieving information themselves in an EMR.

IV FINDINGS

[256] I find:

[257] That all faxes in question contain personal health information of an identifiable individual pursuant to section 2(m) of *The Health Information Protection Act.*

[258] That in all relevant files in this Investigation Report, eHealth Saskatchewan qualifies as an information management service provider pursuant to section 2(j) of *The Health Information Protection Act.*

[259] That there is no responsible trustee for File No. 058/2013-HIPA/BP.

[260] That pursuant to section 2(t) of *The Health Information Protection Act*, the following health care providers qualify as the responsible trustee for the following files:

013/2013-HIPA/BP	Dr. Gary Hunter (Lakeview Neurology)
014/2013-HIPA/BP	Five Hills Regional Health Authority
015/2013-HIPA/BP	Prince Albert Parkland Regional Health Authority
034/2013-HIPA/BP	Prairie North Regional Health Authority
039/2013-HIPA/BP	Saskatoon Regional Health Authority
040/2013-HIPA/BP	Prince Albert Parkland Regional Health Authority
042/2013-HIPA/BP	Five Hills Regional Health Authority
043/2013-HIPA/BP	Heartland Regional Health Authority
044/2013-HIPA/BP	Prairie North Regional Health Authority
045/2013-HIPA/BP	Sunrise Regional Health Authority
046/2013-HIPA/BP	Mamawetan Churchill Regional Health Authority

047/2013-HIPA/BP	Saskatoon Regional Health Authority
057/2013-HIPA/BP	Prince Albert Parkland Regional Health Authority
059/2013-HIPA/BP	Regina Qu'Appelle Regional Health Authority
060/2013-HIPA/BP	Dr. T.W. Wilson
072/2013-HIPA/BP	Prince Albert Parkland Regional Health Authority
073/2013-HIPA/BP	Heartland Regional Health Authority
075/2013-HIPA/BP	Saskatoon Regional Health Authority
077/2013-HIPA/BP	Prairie North Regional Health Authority

[261] That all misdirected faxes in question resulted in unauthorized disclosures of personal health information pursuant to section 27(1) of *The Health Information Protection Act* or were sent to those without a need-to-know pursuant to section 23(2) of *The Health Information Protection Act*.

[262] That incorrect physician contact information in the Radiology Information System was the root cause of the Category #1 breaches.

[263] That incorrect physician contact information combined with undue care and attention were the root causes in Files 015/2013-HIPA/BP, 034/2013-HIPA/BP, 057/2013-HIPA/BP and 059/2013-HIPA/BP.

[264] That outdated patient information in an electronic medical record was the root cause in File 014/2013-HIPA/BP.

[265] That undue care and attention when faxing was the root cause for the Category #3 breaches.

[266] That decision to fax highly sensitive personal health information was also a root cause for File 060/2013-HIPA/BP.

[267] That a configuration setting rendering it impossible to make changes to personal health information of patients was the root cause of the Category #4 breaches.

[268] That incorrect physician contact information in the Radiology Information System was the root cause of the Category #5 breach.

[269] That the average score of trustee's investigation reports was 46.6%.

[270] That the average score of trustee's faxing policies and procedures was 37.7%.

[271] That fax headers on faxes sent from the laboratory information systems of Prince Albert Parkland Regional Health Authority constitutes an inadequate safeguard.

[272] That the cover sheet automatically generated by the Radiology Information System is an inadequate safeguard.

[273] That trustees have a duty to keep patient personal health information stored in an electronic medical record up-to-date pursuant to section 16(1)(a) of *The Health Information Protection Act.*

[274] That none of the regional health authorities using the Radiology Information System have an agreement in place with eHealth Saskatchewan addressing the use of this electronic medical record.

V RECOMMENDATIONS

[275] I recommend:

[276] That all trustees disable 'auto-suggest' features within its electronic systems if such a technical solution is possible.

[277] That all trustees develop consistent privacy breach investigation protocol in accordance with *Helpful Tips: Privacy Breach Guidelines*.

[278] That all trustees consistently follow privacy breach investigation protocol when a privacy breach occurs, even if its information management service provider is also investigating the same issue.

[279] That all trustees develop comprehensive and specific faxing policies and procedures tailored to its organization as detailed on page 55 of this Investigation Report.

[280] That all trustees that purchase the College of Physicians and Surgeons of Saskatchewan physician directory subscribe so that it will also receive the monthly notifications.

[281] That all trustees with subscriptions to the College of Physicians and Surgeons of Saskatchewan physician directory develop a procedure that all copies be manually updated in ink when monthly notifications are received rather than keeping the notifications in the book.

[282] That all trustees devise strategies and corresponding policies and procedures to audit and update all sources of fax contact information regularly. This includes fax information in electronic medical records and electronic health records, preprogrammed features on individual fax machines and traditional paper directories

[283] That all trustees using the Radiology Information System work with eHealth Saskatchewan to verify relevant fax numbers within the system immediately and on an annual basis.

[284] That trustees using the Radiology Information System work with eHealth Saskatchewan and other regional health authorities to devise a strategy for updating fax information within the system. The regional health authorities must then develop internal procedures that complement the strategy.

[285] That trustees using the Radiology Information System configure the Radiology Information System so that faxes are allowed to be sent to the appropriate physician.

[286] That trustees using the Radiology Information System ensure there are adequate and up-to-date agreements in place with eHealth Saskatchewan concerning its use.

[287] That all trustees using the Radiology Information System ensure a cover sheet compliant with best practices accompanies faxes sent from this system.

[288] That all trustees verify that faxes sent from all machines and other sources print a fax header that is compliant with best practices.

[289] That all trustees using the Radiology Information System should work with eHealth Saskatchewan to develop a solution so that the Radiology Information System's current design of one fax number per health care provider is not a reason for misdirected faxes.

[290] That the Minister of Health consider updating sections 18 and 18.1 of *The Health Information Protection Act* on an expedited basis.

[291] That all trustees ensure all misdirected faxes have been retrieved and securely destroyed.

Dated at Regina, in the Province of Saskatchewan, this 9th day of January, 2014.

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

APPENDIX A

Trustee Evaluations

Trustee: Dr. Gary Hunter (Lakeview Neurology)
File(s): 013/2013–HIPA/BP

Evaluation of Investigation Report: 013/2013–HIPA/BP Category #2	**Evidence**	**PT**
Summary of incident	Yes	1
Steps taken to contain breach	No	0
Background of incident (eg. chronology, description of personal health information, etc.)	Yes	1
Description of investigative process	No	0
Identified root and contributing causes	Yes*	0.5
Summary of interviews held	No	0
Review of existing safeguards and protocols	No	0
Summary of possible solutions and recommendations	No	0
Summary of remedial actions	Yes	1
Description of next steps / Timeline	No	0
Responsibility for implementation and monitoring	No	0
Affected individuals notified	Yes	1
	Total Points:	**4.5**

***** I note that this trustee did identify one of the root causes of the breach; that a mistake was made when entering affected individual's referring physician in to the EMR. However, the trustee did not identify another apparent contributing cause, that the contact information to which the fax was sent was out of date. This indicates the information within his EMR is out of date.

I also note that the recipient third party had indicated that it notified this trustee of one misdirected fax and another was subsequently sent. This is confirmed by the trustee's report. The trustee took no steps after the first breach to remedy the situation.

Evaluation of Fax Policy/Procedures – Dr. Gary Hunter (Lakeview Neurology)	**Evidence**	**PT**
Policy and Procedures		
Trustee has a written policy or procedure	Yes*	0.5
Policy details training of new employees and regular reminders for staff	Yes	1
Policy mentions *The Health Information Protection Act* (HIPA)	Yes	1
Policy uses "personal health information" consistently	Yes	1
Policy requires one person to be designated to send faxes	No	0
Sending Faxes		
Policy details when personal health information may be faxed and alternatives	No	0
Policy requires employees to explain risks to clients that request that their personal health information be faxed	Yes	1
Policy instructs employees to remove all personal identifiers wherever possible	No	0
Policy instructs employees to confirm the correct fax number	No	0
Policy instructs employees to confirm that the recipient has appropriate safeguards in place	No	0
Policy requires a cover sheet to be used. Cover sheet should include:	No	0
- Sender information	No	0
- Recipient information	No	0
- Number of pages sent	No	0
- Confidentiality notice	No	0
Policy requires a fax header to display sender information, date and page numbers	No	0
Policy requires employees to carefully check the number before hitting "send"	No	0
Policy requires employees to check the fax confirmation report	No	0
Policy cautions employees not to leave personal health information on fax machine	No	0
Policy details security precautions taken after normal business hours	No	0
Tips for Fax Equipment		
Policy requires fax machines to have enhanced security features	No	0
Policy requires fax machines to be located in secure area	No	0
Policy details measures to be taken when changing fax numbers such as:		
- Renting the fax number for a few extra months	No	0
- destroy pre-printed forms, fax cover sheets and correspondence that refer to your previous number	No	0
- change pre-programmed a fax header	No	0
- ensure that the hard drive has been properly scrubbed to remove all information that was stored on the hard drive or memory	No	0
Policy instructs employees to use pre-programmed commonly used fax numbers	No	0
Policy details how and when pre-programmed numbers should be verified and updated	No	0
	Total points:	**4.5**

Additional Comments:

*This trustee does have a written general privacy policy procedure, but only one statement is specific to faxing.

TOTAL SCORE: 9/40

Trustee: Five Hills Regional Health Authority
File(s): 014/2013-HIPA/BP, 042/2013-HIPA/BP

Evaluation of Investigation Report: 014/2013-HIPA/BP Category #2	**Evidence**	**PT**
Summary of incident	Yes	1
Steps taken to contain breach	No	0
Background of incident (eg. chronology, description of personal health information, etc.)	Yes	1
Description of investigative process	No	0
Identified root and contributing causes	Yes	1
Summary of interviews held	No	0
Review of existing safeguards and protocols	No	0
Summary of possible solutions and recommendations	No	0
Summary of remedial actions	Yes	1
Description of next steps / Timeline	No	0
Responsibility for implementation and monitoring	No	0
Affected individuals notified	Yes	1
	Total Points:	**5**

We note that the remedial actions taken by this trustee – manually updating the affected individuals' information in WinCIS – will only prevent future similar breaches for this one individual. Further, it ensured that one facility without the capability to update patient information in WinCIS would have such capability. It is our understanding that others do not have this capability. As such, we are concerned that the trustee has not taken adequate steps to prevent similar occurrences.

Evaluation of Investigation Report: 043/2013-HIPA/BP Category #1	**Evidence**	**PT**
Summary of incident	No	0
Steps taken to contain breach	Yes	1
Background of incident (eg. chronology, description of personal health information, etc.)	No	0
Description of investigative process	No	0
Identified root and contributing causes	No	0
Summary of interviews held	No	0
Review of existing safeguards and protocols	Yes	1
Summary of possible solutions and recommendations	No	0
Summary of remedial actions	No	0
Description of next steps / Timeline	No	0
Responsibility for implementation and monitoring	No	0
Affected individuals notified	Yes	1
	Total Points:	**3**

eHealth Saskatchewan indicated that there were 4 affected individuals as a result of misdirected faxes sent from FHRHA. FHRHA'S letter of September 20, 2013 stated: "We can confirm that the three faxes in question that were identified that related to FHHR Clients sent from our Moose Jaw Union Hospital Diagnostic Imaging Department were forwarded to the correct provider, see the attached list." The attached list did not provide any relevant detail. FHRHA did not provide anything further to support its claim or explain this discrepancy.

Average of Investigation Report Scores: 4

Evaluation of Fax Policy and Procedures – Five Hills Regional Health Authority	**Evidence**	**PT**
Policy and Procedures		
Trustee has a written policy or procedure	No	0
Policy details training of new employees and regular reminders for staff	No	0
Policy mentions *The Health Information Protection Act* (HIPA)	No	0
Policy uses "personal health information" consistently	No	0
Policy requires one person to be designated to send faxes	No	0
Sending Faxes		
Policy details when personal health information may be faxed and alternatives	No	0
Policy requires employees to explain risks to clients that request that their personal health information be faxed	No	0
Policy instructs employees to remove all personal identifiers wherever possible	No	0
Policy instructs employees to confirm the correct fax number	No	0
Policy instructs employees to confirm that the recipient has appropriate safeguards in place	No	0
Policy requires a cover sheet to be used. Cover sheet should include:	No	0
- Sender information	No	0
- Recipient information	No	0
- Number of pages sent	No	0
- Confidentiality notice	No	0
Policy requires a fax header to display sender information, date and page numbers	No	0
Policy requires employees to carefully check the number before hitting "send"	No	0
Policy requires employees to check the fax confirmation report	No	0
Policy cautions employees not to leave personal health information on fax machine	No	0
Policy details security precautions taken after normal business hours	No	0
Tips for Fax Equipment		
Policy requires fax machines to have enhanced security features	No	0
Policy requires fax machines to be located in secure area	No	0
Policy details measures to be taken when changing fax numbers such as:		
- Renting the fax number for a few extra months	No	0
- destroy pre-printed forms, fax cover sheets and correspondence that refer to your previous number	No	0
- change pre-programmed a fax header	No	0
- ensure that the hard drive has been properly scrubbed to remove all information that was stored on the hard drive or memory	No	0
Policy instructs employees to use pre-programmed commonly used fax numbers	No	0
Policy details how and when pre-programmed numbers should be verified and updated	No	0
	Total points:	**0**

Additional Comments:

This trustee does not have specific faxing policies and procedures as required by section 16 of HIPA.

TOTAL SCORE: 4/40

Trustee: Prince Albert Parkland Regional Health Authority
File(s): 015/2013-HIPA/BP, 040/2013-HIPA/BP, 057/2013-HIPA/BP, 072/2013-HIPA/BP

Evaluation of Investigation Report: 015/2013-HIPA/BP Category #2	**Evidence**	**PT**
Summary of incident	No	0
Steps taken to contain breach	No	0
Background of incident (eg. chronology, description of personal health information, etc.)	No	0
Description of investigative process	No	0
Identified root and contributing causes	No	0
Summary of interviews held	No	0
Review of existing safeguards and protocols	Yes*	0.5
Summary of possible solutions and recommendations	No	0
Summary of remedial actions	No	0
Description of next steps / Timeline	No	0
Responsibility for implementation and monitoring	No	0
Affected individuals notified	No	0
	Total Points:	**0.5**

Evaluation of Investigation Report: 040/2013-HIPA/BP Category #1	**Evidence**	**PT**
Summary of incident	No	0
Steps taken to contain breach	No	0
Background of incident (eg. chronology, description of personal health information, etc.)	No	0
Description of investigative process	No	0
Identified root and contributing causes	No	0
Summary of interviews held	No	0
Review of existing safeguards and protocols	No	0
Summary of possible solutions and recommendations	No	0
Summary of remedial actions	No	0
Description of next steps / Timeline	No	0
Responsibility for implementation and monitoring	No	0
Affected individuals notified	No	0
	Total Points:	**0**

Evaluation of Investigation Report: 057/2013-HIPA/BP Category #2	**Evidence**	**PT**
Summary of incident	No	0
Steps taken to contain breach	No	0
Background of incident (eg. chronology, description of personal health information, etc.)	No	0
Description of investigative process	No	0
Identified root and contributing causes	Yes*	0.5
Summary of interviews held	No	0
Review of existing safeguards and protocols	No	0
Summary of possible solutions and recommendations	No	0
Summary of remedial actions	No	0
Description of next steps / Timeline	No	0
Responsibility for implementation and monitoring	No	0
Affected individuals notified	No	0
	Total Points:	**0.5**

Evaluation of Investigation Report: 072/2013-HIPA/BP Category #4	**Evidence**	**PT**
Summary of incident	No	0
Steps taken to contain breach	No	0
Background of incident (eg. chronology, description of personal health information, etc.)	No	0
Description of investigative process	No	0
Identified root and contributing causes	No	0
Summary of interviews held	No	0
Review of existing safeguards and protocols	No	0
Summary of possible solutions and recommendations	No	0
Summary of remedial actions	No	0
Description of next steps / Timeline	No	0
Responsibility for implementation and monitoring	No	0
Affected individuals notified	No	0
	Total Points:	**0**

In all four cases, PAPRHA provided very little detail in describing the breach or its response. All that was provided was a short one page letter for each breach.

* For File 015/2013-HIPA/BP (Category #2), PAPRHA identified two possible causes, but did not appear to put in extra effort to determine the exact cause. Further, the lack of detail with respect to the investigation does not instill confidence that a proper investigation took place and root causes were properly identified. Further, a similar breach reoccurred (File 057/2013-HIPA/BP (Category #2)) and PAPRHA provided no further detail.

In its letter of May 6, 2013 for 015/2013-HIPA/BP, PAPRHA stated: "Lab employees take great care when faxing personal health information, and all faxes were sent with a cover sheet." This statement is questionable as a similar breach reoccurred months later. Further, the third party did not send a cover sheet with the faxes in question for either Category #2 files from PAPRHA – if they existed. The fax header for these faxes also read: "[Date and time of transmission] Saskatchewan Health via VSI-FAX Page [x] of [x] [Unknown number]". This made it difficult to determine which trustee sent the faxes.

With respect to File 040/2013-HIPA/BP (Category #1), PAPRHA's letter of August 20, 2013 simply referred to the report from eHealth Saskatchewan, its IMSP. It did not offer a summary, the root cause, remedial actions or confirm the affected individuals had been notified.

eHealth Saskatchewan had informed us there were 41 affected individuals as a result of misdirected faxes sent from PAPRHA. On October 15, 2013 our office received a letter from PAPRHA dated October 7, 2013 that stated:

> Upon further review of the incident regarding the above noted file, I have determined that I was incorrect when I identified that there were twenty (20) patients who were affected by a breach of privacy. In fact, there was no actual privacy breach. The twenty faxes in question were not sent to the wrong physician clinic, they were in fact not sent out at all. There was no privacy breach from PAPHR as a result of this incident with the RIS.

I note that PAPRHA's letter of August 20, 2013 did not identify that there were 20 affected individuals. It did not explain how it arrived at this conclusion.

Finally, with respect to File 072/2013-HIPA/BP, PAPRHA simply stated:

> In regards to your letter dated August 20, 2013 regarding misdirected faxes, Prince Albert Parkland Health Region (PAPHR) has been working with eHealth Saskatchewan regarding this breach of privacy. As a result of a configuration setting with the Radiology Information System (RIS), twelve (12) radiology reports originating in the PAPHR were sent to the wrong physician clinic from 2010 to June 18, 2013.

PAPRHA did not elaborate further on this breach. Further, my office did not benefit from a report from the IMSP leaving us with virtually no details with respect to this breach. As a result we had to contact the IMSP, eHealth Saskatchewan, to receive a meaningful account of the breach.

The lack of detail provided and apparent lack of rigour to which PAPRHA has responded to these breaches demonstrates that PAPRHA has not taken these incidents seriously.

Average of Investigation Report Scores: 0.25

Evaluation of Fax Policy and Procedures – Prince Albert Parkland Regional Health Authority	**Evidence**	**PT**
Policy and Procedures		
Trustee has a written policy or procedure	Yes	1
Policy details training of new employees and regular reminders for staff	No	0
Policy mentions *The Health Information Protection Act* (HIPA)	Yes	1
Policy uses "personal health information" consistently	Yes	1
Policy requires one person to be designated to send faxes	No	0
Sending Faxes		
Policy details when personal health information may be faxed and alternatives	Yes	1
Policy requires employees to explain risks to clients that request that their personal health information be faxed	No	0
Policy instructs employees to remove all personal identifiers wherever possible	Yes	1
Policy instructs employees to confirm the correct fax number	No	0
Policy instructs employees to confirm that the recipient has appropriate safeguards in place	Yes	1
Policy requires a cover sheet to be used. Cover sheet should include:	Yes	1
- Sender information	Yes*	0
- Recipient information	Yes	1
- Number of pages sent	Yes	1
- Confidentiality notice	Yes	1
Policy requires a fax header to display sender information, date and page numbers	No	0
Policy requires employees to carefully check the number before hitting "send"	Yes	1
Policy requires employees to check the fax confirmation report	Yes	1
Policy cautions employees not to leave personal health information on fax machine	Yes	1
Policy details security precautions taken after normal business hours	No	0
Tips for Fax Equipment		
Policy requires fax machines to have enhanced security features	No	0
Policy requires fax machines to be located in secure area	Yes	1
Policy details measures to be taken when changing fax numbers such as:		
- Renting the fax number for a few extra months	No	0
- destroy pre-printed forms, fax cover sheets and correspondence that refer to your previous number	Yes	1
- change pre-programmed a fax header	Yes	1
- ensure that the hard drive has been properly scrubbed to remove all information that was stored on the hard drive or memory	Yes	1
Policy instructs employees to use pre-programmed commonly used fax numbers	Yes	1
Policy details how and when pre-programmed numbers should be verified and updated	No	0
Bonus points (described below)	Yes	2
	Total points:	**20**

Additional Comments:

We note PAPRHA revised its faxing policies and procedures following these breaches. It did not provide a copy of what was in place at the time of the breaches. However, the document provided to our office appears to 'track changes' in red font. As such we will assume that what is in black ink was in place at the time of the breaches. It appeared it added policies for faxing from automated systems. It is our understanding that PAPRHA is waiting for feedback before making this new policy official.

We awarded the following bonus points to PAPRHA:

- Instructions to document that personal health information transmittal by fax of patient's chart (1pt)
- Instructions for when a misdirected fax is sent (1 pt)

* As discussed elsewhere in this analysis, we did not award a point for sender information on a fax cover sheet even if the policy/procedure asked for one as RIS cover sheets name all RIS trustees.

PAPRHA has one of the strongest fax policies among the trustees in this Report, and yet misdirected faxes still occurred. It is disappointing that PAPRHA did not more fully investigate to determine with more certainty the true causes of the breaches and ways to prevent them.

PAPRHA was one of the trustees involved in the 2010 Report (File 092/2009-HIPA/BP). At that time, PAPRHA scored 9/11 for its investigative report and 14/27 for its policies and procedures. While it appears that it has enhanced its faxing policy and procedure, it has not gone to as much effort as it did for investigating the faxing breach in 2009.

TOTAL SCORE: 20.25/40

Trustee: Prairie North Regional Health Authority
File(s): 034/2013–HIPA/BP, 044/2013–HIPA/BP, 077/2013–HIPA/BP

Evaluation of Investigation Report: 034/2013-HIPA/BP Category #2	**Evidence**	**PT**
Summary of incident	Yes	1
Steps taken to contain breach	Yes	1
Background of incident (eg. chronology, description of personal health information, etc.)	Yes	1
Description of investigative process	Yes	1
Identified root and contributing causes	Yes	1
Summary of interviews held	No	0
Review of existing safeguards and protocols	Yes	1
Summary of possible solutions and recommendations	No	0
Summary of remedial actions	Yes	1
Description of next steps / Timeline	No	0
Responsibility for implementation and monitoring	No	0
Affected individuals notified	No	0
	Total Points:	**7**

Evaluation of Investigation Report: 044/2013-HIPA/BP Category #1	**Evidence**	**PT**
Summary of incident	No	0
Steps taken to contain breach	Yes	1
Background of incident (eg. chronology, description of personal health information, etc.)	No	0
Description of investigative process	No	0
Identified root and contributing causes	No	0
Summary of interviews held	No	0
Review of existing safeguards and protocols	Yes	1
Summary of possible solutions and recommendations	No	0
Summary of remedial actions	No	0
Description of next steps / Timeline	No	0
Responsibility for implementation and monitoring	No	0
Affected individuals notified	Yes	1
	Total Points:	**3**

Evaluation of Investigation Report: 077/2013-HIPA/BP Category #5	**Evidence**	**PT**
Summary of incident	No	0
Steps taken to contain breach	Yes	1
Background of incident (eg. chronology, description of personal health information, etc.)	Yes	1
Description of investigative process	Yes	1
Identified root and contributing causes	Yes	1
Summary of interviews held	Yes	1
Review of existing safeguards and protocols	Yes	1
Summary of possible solutions and recommendations	No	0
Summary of remedial actions	Yes	1
Description of next steps / Timeline	No	0
Responsibility for implementation and monitoring	No	0
Affected individuals notified	Yes	1
	Total Points:	**8**

With respect to File 034/2013-HIPA/BP (Category #2), PNRHA identified that one of the factors was that a physician's contact information was out of date on the RIS system. Yet, none of the actions or recommendations of PNRHA's report addresses the need to update contact information in the LIS system. It did not address the other root cause either which was choosing the wrong physician. Its report did not indicate if it had notified affected individuals or explained why or why not.

Not much detail was provided with respect to File 044/2013-HIPA/BP (Category #1).

Average of Investigation Report Scores: 6

Evaluation of Fax Policy and Procedures – Prairie North Regional Health Authority	**Evidence**	**PT**
Policy and Procedures		
Trustee has a written policy or procedure	Yes	1
Policy details training of new employees and regular reminders for staff	No	0
Policy mentions *The Health Information Protection Act* (HIPA)	Yes	1
Policy uses "personal health information" consistently	Yes	1
Policy requires one person to be designated to send faxes	No	0
Sending Faxes		
Policy details when personal health information may be faxed and alternatives	Yes	1
Policy requires employees to explain risks to clients that request that their personal health information be faxed	No	0
Policy instructs employees to remove all personal identifiers wherever possible	No	0
Policy instructs employees to confirm the correct fax number	No	0
Policy instructs employees to confirm that the recipient has appropriate safeguards in place	No	0
Policy requires a cover sheet to be used. Cover sheet should include:	No	0
- Sender information	No	0
- Recipient information	No	0
- Number of pages sent	No	0
- Confidentiality notice	No	0
Policy requires a fax header to display sender information, date and page numbers	No	0
Policy requires employees to carefully check the number before hitting "send"	No	0
Policy requires employees to check the fax confirmation report	No	0
Policy cautions employees not to leave personal health information on fax machine	No	0
Policy details security precautions taken after normal business hours	No	0
Tips for Fax Equipment		
Policy requires fax machines to have enhanced security features	No	0
Policy requires fax machines to be located in secure area	No	0
Policy details measures to be taken when changing fax numbers such as:		
- Renting the fax number for a few extra months	No	0
- destroy pre-printed forms, fax cover sheets and correspondence that refer to your previous number	No	0
- change pre-programmed a fax header	No	0
- ensure that the hard drive has been properly scrubbed to remove all information that was stored on the hard drive or memory	No	0
Policy instructs employees to use pre-programmed commonly used fax numbers	No	0
Policy details how and when pre-programmed numbers should be verified and updated	No	0
Bonus points (described below)	Yes	3
	Total points:	**7**

Additional Comments:

In response to these breaches PNRHA revised its faxing policies and procedures. Our understanding is the new policies and procedures are in draft form and awaiting feedback before implementation.

I awarded three extra bonus points to the old policy and procedure for listing what needs to be done when a misdirected fax is received (1pt notifying sender, 1pt deciding with sender what to do with the personal health information, 1pt for advising not to send personal health information on). The total score for the old policy and procedure is five.

I awarded three extra bonus points to the new policy and procedure for listing what needs to be done when a misdirected fax is received. We also awarded two extra points for describing what to do if a misdirected fax has been sent. The new policy indicates that faxes should be sent with a cover sheet; however, it also states "When the standardized cover sheet is unable to be sent with the fax…" giving employees permission not to use a cover sheet.

As such, a point would not have been awarded for the use of cover sheets. PNRHA also uses RIS. Therefore, as discussed elsewhere in this analysis, we would not have awarded a point for sender information on a fax cover sheet even if the policy/procedure asked for one as RIS cover sheets name all RIS trustees. The score for the new policy/procedure would be 19.

I encourage PNRHA to replace "circle of care" with "need-to-know" within its policy as per my comments in my Investigation Report H-2013-001 starting at [59].

PNRHA was one of the trustees involved in the 2010 Report (File 093/2009-HIPA/BP). At that time, PNRHA scored 5/11 for its investigative report and 16/27 for its policies and procedures. PNRHA has not improved its investigative efforts for faxing breaches. Further, it is unclear why there is a discrepancy between the policy and procedures provided for the 2010 Report and those provided for the purposes of this analysis. The policy and procedures provided in 2010 were more fulsome than what PNRHA claims were in place at the time of the breaches in question. Nonetheless, the new draft policies and procedures of PNRHA show improvement.

TOTAL SCORE: 11/40

Trustee: Saskatoon Regional Health Authority
File(s): 039/2013-HIPA/BP, 047/2013-HIPA/BP, 075/2013-HIPA/BP

Evaluation of Investigation Report: 039/2013-HIPA/BP Category #1	**Evidence**	**PT**
Summary of incident	Yes	1
Steps taken to contain breach	No	0
Background of incident (eg. chronology, description of personal health information, etc.)	Yes	1
Description of investigative process	No	0
Identified root and contributing causes	Yes	1
Summary of interviews held	No	0
Review of existing safeguards and protocols	No	0
Summary of possible solutions and recommendations	Yes	1
Summary of remedial actions	Yes	1
Description of next steps / Timeline	No	0
Responsibility for implementation and monitoring	No	0
Affected individuals notified	Yes	1
	Total Points:	**6**

Evaluation of Investigation Report: 047/2013-HIPA/BP Category #3	**Evidence**	**PT**
Summary of incident	Yes	1
Steps taken to contain breach	No	0
Background of incident (eg. chronology, description of personal health information, etc.)	Yes	1
Description of investigative process	No	0
Identified root and contributing causes	Yes	1
Summary of interviews held	Yes	1
Review of existing safeguards and protocols	No	0
Summary of possible solutions and recommendations	Yes	1
Summary of remedial actions	Yes	1
Description of next steps / Timeline	No	0
Responsibility for implementation and monitoring	No	0
Affected individuals notified	Yes	1
	Total Points:	**7**

Evaluation of Investigation Report: 075/2013-HIPA/BP Category #4	**Evidence**	**PT**
Summary of incident	Yes	1
Steps taken to contain breach	Yes	1
Background of incident (eg. chronology, description of personal health information, etc.)	Yes	1
Description of investigative process	Yes	1
Identified root and contributing causes	No	0
Summary of interviews held	Yes	1
Review of existing safeguards and protocols	Yes	1
Summary of possible solutions and recommendations	No	0
Summary of remedial actions	No	0
Description of next steps / Timeline	No	0
Responsibility for implementation and monitoring	No	0
Affected individuals notified	Yes	1
	Total Points:	**7**

The recommendations from the investigation report for File 039/2013 are as follows:

- SHR Medical Imaging Department works closely with eHealth to ensure physician fax numbers are validated before changed in the RIS/PAC system.

- eHealth is working with the Saskatchewan Medical Association to ensure physicians update they [sic] fax numbers should any changes occur.

- RIS/PAC move towards a system whereas referring physicians retrieve the medical image rather than RIS faxing the reports.

It is unclear how SRHA will implement these recommendations and what timeframe is expected. Further, it is unclear as to how and why the Saskatchewan Medical Association is involved.

SRHA solutions for File 047/2013-HIPA/BP (Category #3), ensuring directories for faxing on unit 6000 are up-to-date, does not appear to prevent potential breaches in the rest of the RHA. A policy that incorporates the whole region would be more effective.

For File 076/2013-HIPA/BP (Category #4), SRHA did identify root causes or make recommendations for preventing future breaches.

Average of Investigation Report Scores: 6.7

Evaluation of Fax Policy and Procedures – Saskatoon Regional Health Authority	**Evidence**	**PT**
Policy and Procedures		
Trustee has a written policy or procedure	No	0
Policy details training of new employees and regular reminders for staff	No	0
Policy mentions *The Health Information Protection Act* (HIPA)	No	0
Policy uses "personal health information" consistently	No	0
Policy requires one person to be designated to send faxes	No	0
Sending Faxes		
Policy details when personal health information may be faxed and alternatives	No	0
Policy requires employees to explain risks to clients that request that their personal health information be faxed	No	0
Policy instructs employees to remove all personal identifiers wherever possible	No	0
Policy instructs employees to confirm the correct fax number	No	0
Policy instructs employees to confirm that the recipient has appropriate safeguards in place	No	0
Policy requires a cover sheet to be used. Cover sheet should include:	No	0
- Sender information	No	0
- Recipient information	No	0
- Number of pages sent	No	0
- Confidentiality notice	No	0
Policy requires a fax header to display sender information, date and page numbers	No	0
Policy requires employees to carefully check the number before hitting "send"	No	0
Policy requires employees to check the fax confirmation report	No	0
Policy cautions employees not to leave personal health information on fax machine	No	0
Policy details security precautions taken after normal business hours	No	0
Tips for Fax Equipment		
Policy requires fax machines to have enhanced security features	No	0
Policy requires fax machines to be located in secure area	No	0
Policy details measures to be taken when changing fax numbers such as:		
- Renting the fax number for a few extra months	No	0
- destroy pre-printed forms, fax cover sheets and correspondence that refer to your previous number	No	0
- change pre-programmed a fax header	No	0
- ensure that the hard drive has been properly scrubbed to remove all information that was stored on the hard drive or memory	No	0
Policy instructs employees to use pre-programmed commonly used fax numbers	No	0
Policy details how and when pre-programmed numbers should be verified and updated	No	0
	Total points:	**0**

Additional Comments:

We did not give credit to SRHA for faxing policies and procedures. Within its "Privacy and Confidentiality" procedure it states:

> 2.3.1 Faxing of PHI and/or confidential information must only take place with appropriate safeguards in place and in accordance with "SHR Faxing Guidelines" (Appendix C).

Appendix C of SRHA's "Privacy and Confidentiality" policy is a three page document entitled *Privacy Considerations: Faxing Personal Information and Personal Health Information* and much of the material is identical to our office's resource *Helpful Tips – Privacy Considerations: Faxing Personal Information and Personal Health Information*. SRHA's document uses language such as "Adopt a written policy on faxing personal information and personal health information…" and "If you have a need to continually fax personal information or personal health information…". The appendix is not helpful to employees who must look to this procedure for the rules and procedures for faxing personal health information. Further, SRHA received no points for simply referring

its employees to the *Helpful Tips – Privacy Considerations: Faxing Personal Information and Personal Health Information* resource.

We also note that SRHA was one of the trustees in our 2010 Report (File 094/2009-HIPA/BP). At that time, it simply had posters for guidance for employees. The posters scored a 14/27 in terms of policy and procedure and provided more guidance for faxing than what is available for SRHA employees now.

TOTAL SCORE: 6.7/40

Trustee: Heartland Regional Health Authority
File(s): 043/2013–HIPA/BP, 073/2013–HIPA/BP

Evaluation of Investigation Report: 043/2013–HIPA/BP Category #1	**Evidence**	**PT**
Summary of incident	Yes	1
Steps taken to contain breach	Yes	1
Background of incident (eg. chronology, description of personal health information, etc.)	Yes	1
Description of investigative process	Yes	1
Identified root and contributing causes	Yes	1
Summary of interviews held	No	0
Review of existing safeguards and protocols	Yes	1
Summary of possible solutions and recommendations	Yes	1
Summary of remedial actions	Yes	1
Description of next steps / Timeline	Yes	1
Responsibility for implementation and monitoring	Yes	1
Affected individuals notified	Yes	1
	Total Points:	**11**

Evaluation of Investigation Report: 073/2013–HIPA/BP Category #4	**Evidence**	**PT**
Summary of incident	Yes	1
Steps taken to contain breach	Yes	1
Background of incident (eg. chronology, description of personal health information, etc.)	Yes	1
Description of investigative process	Yes	1
Identified root and contributing causes	No	0
Summary of interviews held	No	0
Review of existing safeguards and protocols	Yes	1
Summary of possible solutions and recommendations	Yes	1
Summary of remedial actions	Yes	1
Description of next steps / Timeline	Yes	1
Responsibility for implementation and monitoring	Yes	1
Affected individuals notified	Yes	1
	Total Points:	**10**

One of the recommendations of HRHA is to ensure "THAT an audit schedule be created to ensure accuracy of fax numbers in the PACS system" by November 30, 2013. RIS is the system at issue, not PACS. It is unknown what HRHA will propose with respect to this audit.

HRHA provided a new, more comprehensive internal investigation report after receiving a draft copy of the analysis for this Investigation Report.

Average of Investigation Report Scores: 10.5

Evaluation of Fax Policy and Procedures – Heartland Regional Health Authority	**Evidence**	**PT**
Policy and Procedures		
Trustee has a written policy or procedure	Yes	1
Policy details training of new employees and regular reminders for staff	No	0
Policy mentions *The Health Information Protection Act* (HIPA)	Yes	1
Policy uses "personal health information" consistently	Yes	1
Policy requires one person to be designated to send faxes	No	0
Sending Faxes		
Policy details when personal health information may be faxed and alternatives	Yes	1
Policy requires employees to explain risks to clients that request that their personal health information be faxed	Yes	1
Policy instructs employees to remove all personal identifiers wherever possible	Yes	1
Policy instructs employees to confirm the correct fax number	Yes	1
Policy instructs employees to confirm that the recipient has appropriate safeguards in place	No	0
Policy requires a cover sheet to be used. Cover sheet should include:	Yes	1
- Sender information	Yes*	0
- Recipient information	Yes	1
- Number of pages sent	Yes	1
- Confidentiality notice	Yes	1
Policy requires a fax header to display sender information, date and page numbers	Yes	1
Policy requires employees to carefully check the number before hitting "send"	No	0
Policy requires employees to check the fax confirmation report	Yes	1
Policy cautions employees not to leave personal health information on fax machine	Yes	1
Policy details security precautions taken after normal business hours	No	0
Tips for Fax Equipment		
Policy requires fax machines to have enhanced security features	No	0
Policy requires fax machines to be located in secure area	Yes	1
Policy details measures to be taken when changing fax numbers such as:		
- Renting the fax number for a few extra months	No	0
- destroy pre-printed forms, fax cover sheets and correspondence that refer to your previous number	No	0
- change pre-programmed a fax header	Yes	1
- ensure that the hard drive has been properly scrubbed to remove all information that was stored on the hard drive or memory	No	0
Policy instructs employees to use pre-programmed commonly used fax numbers	Yes	1
Policy details how and when pre-programmed numbers should be verified and updated	No	0
Bonus points (described below)	Yes	2
	Total points:	**19**

Additional Comments:

I awarded two extra bonus points as HRHA faxing policy/procedure provides instruction on what should be done if a misdirected fax is received (1pt notifying sender, 1pt notifying privacy officer).

HRHA was one of the trustees involved in the 2010 Report (File 090/2009-HIPA/BP). At that time, HRHA scored 6/11 for its investigative report and 11/27 for its policies and procedures. It is encouraging that HRHA has improved both in terms of investigation efforts and faxing policies and procedures.

* As discussed elsewhere in this analysis, we did not award a point for sender information on a fax cover sheet even if the policy/procedure asked for one as RIS cover sheets name all RIS trustees.

TOTAL SCORE: 29.5/40

Trustee: Sunrise Regional Health Authority
File(s): 045/2013–HIPA/BP

Evaluation of Investigation Report: 045/2013–HIPA/BP Category #1	**Evidence**	**PT**
Summary of incident	No	0
Steps taken to contain breach	Yes	1
Background of incident (eg. chronology, description of personal health information, etc.)	Yes	1
Description of investigative process	No	0
Identified root and contributing causes	No	0
Summary of interviews held	No	0
Review of existing safeguards and protocols	No	0
Summary of possible solutions and recommendations	No	0
Summary of remedial actions	Yes	1
Description of next steps / Timeline	No	0
Responsibility for implementation and monitoring	No	0
Affected individuals notified	No	0
	Total Points:	**3**

Sunrise did not provide much detail with respect to this breach.

Evaluation of Fax Policy and Procedures – Sunrise Regional Health Authority	**Evidence**	**PT**
Policy and Procedures		
Trustee has a written policy or procedure	Yes	1
Policy details training of new employees and regular reminders for staff	Yes	1
Policy mentions *The Health Information Protection Act* (HIPA)	Yes	1
Policy uses "personal health information" consistently	Yes	1
Policy requires one person to be designated to send faxes	Yes	1
Sending Faxes		
Policy details when personal health information may be faxed and alternatives	Yes	1
Policy requires employees to explain risks to clients that request that their personal health information be faxed	Yes	1
Policy instructs employees to remove all personal identifiers wherever possible	Yes	1
Policy instructs employees to confirm the correct fax number	Yes	1
Policy instructs employees to confirm that the recipient has appropriate safeguards in place	Yes	1
Policy requires a cover sheet to be used. Cover sheet should include:	Yes	1
- Sender information	Yes*	0
- Recipient information	Yes	1
- Number of pages sent	Yes	1
- Confidentiality notice	Yes	1
Policy requires a fax header to display sender information, date and page numbers	Yes	1
Policy requires employees to carefully check the number before hitting "send"	Yes	1
Policy requires employees to check the fax confirmation report	Yes	1
Policy cautions employees not to leave personal health information on fax machine	Yes	1
Policy details security precautions taken after normal business hours	Yes	1
Tips for Fax Equipment		
Policy requires fax machines to have enhanced security features	No	0
Policy requires fax machines to be located in secure area	Yes	1
Policy details measures to be taken when changing fax numbers such as:		
- Renting the fax number for a few extra months	Yes	1
- destroy pre-printed forms, fax cover sheets and correspondence that refer to your previous number	Yes	1
- change pre-programmed a fax header	Yes	1
- ensure that the hard drive has been properly scrubbed to remove all information that was stored on the hard drive or memory	Yes	1
Policy instructs employees to use pre-programmed commonly used fax numbers	Yes	1
Policy details how and when pre-programmed numbers should be verified and updated	No	0
Bonus points (described below)	Yes	3
	Total points:	**28**

Additional Comments:

I awarded three extra points for describing what to do if a misdirected fax is received (1pt notifying sender, 1pt deciding with sender what to do with the personal health information, 1pt for advising not to send personal health information on).

Sunrise was one of the trustees involved in the 2010 Report (File 096/2009-HIPA/BP). At that time, Sunrise scored 6/11 for its investigative report and 15/27 for its policies and procedures. While it appears that it has enhanced its faxing policy and procedure, it has not gone to as much effort as it did for investigating the faxing breach in 2009.

* As discussed elsewhere in this analysis, we did not award a point for sender information on a fax cover sheet even if the policy/procedure asked for one as RIS cover sheets name all RIS trustees.

TOTAL SCORE: 31/40

Trustee: Mamawetan Churchill River Regional Health Authority
File(s): 046/2013–HIPA/BP

Evaluation of Investigation Report: 046/2013–HIPA/BP Category #1	**Evidence**	**PT**
Summary of incident	Yes	1
Steps taken to contain breach	No	0
Background of incident (eg. chronology, description of personal health information, etc.)	Yes	1
Description of investigative process	Yes	1
Identified root and contributing causes	Yes	1
Summary of interviews held	No	0
Review of existing safeguards and protocols	Yes	1
Summary of possible solutions and recommendations	Yes	1
Summary of remedial actions	Yes	1
Description of next steps / Timeline	No	0
Responsibility for implementation and monitoring	No	0
Affected individuals notified	Yes	1
	Total Points:	**8**

One of the recommendations in MCRRHA's investigation report is as follows:

1. MCRHR is currently working on strengthening its processes around accurate data entry into the WINCIS system through LEAN methodology. This includes a project aimed at eliminating mistakes during data entry into the WINCIS system, such as in this case incorrect physician. Plans for this project include developing standard work for accurate data entry into the WINCIS system, staff training for providers, implementing double checks for accuracy and ongoing monitoring and measurement. MCRHR is working with eHealth to see if any barriers and changes can be made to improve the WINCIS system in order to reduce the risk of these types of errors.

Although a positive step, it does not ensure that physician faxing information in RIS is up-to-date.

I applaud MCRRHA for identifying extra root and contributing causes.

Evaluation of Fax Policy and Procedures – Mamawetan Churchill River Regional Health Authority	**Evidence**	**PT**
Policy and Procedures		
Trustee has a written policy or procedure	Yes	1
Policy details training of new employees and regular reminders for staff	No	0
Policy mentions *The Health Information Protection Act* (HIPA)	Yes	1
Policy uses "personal health information" consistently	Yes	1
Policy requires one person to be designated to send faxes	No	0
Sending Faxes		
Policy details when personal health information may be faxed and alternatives	No	0
Policy requires employees to explain risks to clients that request that their personal health information be faxed	No	0
Policy instructs employees to remove all personal identifiers wherever possible	No	0
Policy instructs employees to confirm the correct fax number	No	0
Policy instructs employees to confirm that the recipient has appropriate safeguards in place	No	0
Policy requires a cover sheet to be used. Cover sheet should include:	Yes	1
- Sender information	Yes	1
- Recipient information	Yes*	0
- Number of pages sent	Yes	1
- Confidentiality notice	Yes	1
Policy requires a fax header to display sender information, date and page numbers	No	0
Policy requires employees to carefully check the number before hitting "send"	No	0
Policy requires employees to check the fax confirmation report	No	0
Policy cautions employees not to leave personal health information on fax machine	No	0
Policy details security precautions taken after normal business hours	No	0
Tips for Fax Equipment		
Policy requires fax machines to have enhanced security features	Yes	1
Policy requires fax machines to be located in secure area	No	0
Policy details measures to be taken when changing fax numbers such as:		
- Renting the fax number for a few extra months	No	0
- destroy pre-printed forms, fax cover sheets and correspondence that refer to your previous number	No	0
- change pre-programmed a fax header	No	0
- ensure that the hard drive has been properly scrubbed to remove all information that was stored on the hard drive or memory	No	0
Policy instructs employees to use pre-programmed commonly used fax numbers	Yes	1
Policy details how and when pre-programmed numbers should be verified and updated	Yes**	0
Bonus points (described below)	Yes	1
	Total points:	**10**

Additional Comments:

I awarded one additional point as MCRRHA's policy and procedure instructs employees to make a notation that personal health information was faxed on the patient's chart.

* As discussed elsewhere in this analysis, we did not award a point for sender information on a fax cover sheet even if the policy/procedure asked for one as RIS cover sheets name all RIS trustees.

** Policy/procedure does not provide enough direction to be effective.

TOTAL SCORE: 18/40

Trustee: Regina Qu'Appelle Regional Health Authority
File(s): 059/2013–HIPA/BP

Evaluation of Investigation Report: 059/2013–HIPA/BP Category #2	**Evidence**	**PT**
Summary of incident	Yes	1
Steps taken to contain breach	Yes	1
Background of incident (eg. chronology, description of personal health information, etc.)	Yes	1
Description of investigative process	Yes	1
Identified root and contributing causes	Yes	1
Summary of interviews held	Yes	1
Review of existing safeguards and protocols	No	0
Summary of possible solutions and recommendations	Yes	1
Summary of remedial actions	Yes	1
Description of next steps / Timeline	No	0
Responsibility for implementation and monitoring	No	0
Affected individuals notified	Yes	1
	Total Points:	**9**

Evaluation of Fax Policy and Procedures – Regina Qu'Appelle Regional Health Authority	**Evidence**	**PT**
Policy and Procedures		
Trustee has a written policy or procedure	Yes	1
Policy details training of new employees and regular reminders for staff	No	0
Policy mentions *The Health Information Protection Act* (HIPA)	No	0
Policy uses "personal health information" consistently	Yes	1
Policy requires one person to be designated to send faxes	No	0
Sending Faxes		
Policy details when personal health information may be faxed and alternatives	No	0
Policy requires employees to explain risks to clients that request that their personal health information be faxed	No	0
Policy instructs employees to remove all personal identifiers wherever possible	No	0
Policy instructs employees to confirm the correct fax number	Yes	1
Policy instructs employees to confirm that the recipient has appropriate safeguards in place	Yes	1
Policy requires a cover sheet to be used. Cover sheet should include:	Yes*	0
- Sender information	Yes	1
- Recipient information	Yes	1
- Number of pages sent	Yes	1
- Confidentiality notice	Yes	1
Policy requires a fax header to display sender information, date and page numbers	No	0
Policy requires employees to carefully check the number before hitting "send"	Yes	1
Policy requires employees to check the fax confirmation report	No	0
Policy cautions employees not to leave personal health information on fax machine	No	0
Policy details security precautions taken after normal business hours	No	0
Tips for Fax Equipment		
Policy requires fax machines to have enhanced security features	No	0
Policy requires fax machines to be located in secure area	Yes	1
Policy details measures to be taken when changing fax numbers such as:		
- Renting the fax number for a few extra months	No	0
- destroy pre-printed forms, fax cover sheets and correspondence that refer to your previous number	No	0
- change pre-programmed a fax header	No	0
- ensure that the hard drive has been properly scrubbed to remove all information that was stored on the hard drive or memory	No	0
Policy instructs employees to use pre-programmed commonly used fax numbers	No	0
Policy details how and when pre-programmed numbers should be verified and updated	No	0
	Total points:	**10**

Additional Comments:

* RQRHA has a policy that requires fax cover sheets to accompany faxes. However, its report states: "Fax cover sheets do not always accompany faxed documents." This indicates that the policy is not enforced; therefore no point will be awarded for this policy.

TOTAL SCORE: 19/40

Trustee: Dr. T. W. Wilson
File(s): 060/2013–HIPA/BP

Evaluation of Investigation Report: 060/2013–HIPA/BP Category #3	**Evidence**	**PT**
Summary of incident	Yes	1
Steps taken to contain breach	Yes	1
Background of incident (eg. chronology, description of personal health information, etc.)	Yes	1
Description of investigative process	No	0
Identified root and contributing causes	No	0
Summary of interviews held	No	0
Review of existing safeguards and protocols	No	0
Summary of possible solutions and recommendations	No	0
Summary of remedial actions	No	0
Description of next steps / Timeline	No	0
Responsibility for implementation and monitoring	No	0
Affected individuals notified	Yes	1
	Total Points:	**4**

As noted, the personal health information in the fax was highly sensitive as it contained details of a hormonal treatment and sexual activity of a transgendered individual. Highly sensitive personal health information should not be faxed as faxing is not a secure form of communication. This was a contributing factor of the breach not identified by Dr. Wilson.

Dr. Wilson's report identified that the mistake in the CPSS directory was the root cause of the breach but made no mention of the corrections acknowledged in the monthly updates by CPSS. As such we cannot except the statement made in Dr. Wilson's report that: "I am certainly aware of the sensitive nature of this information. My office is extra careful with such information."

Evaluation of Fax Policy and Procedures – Dr. T. W. Wilson	**Evidence**	**PT**
Policy and Procedures		
Trustee has a written policy or procedure	No	0
Policy details training of new employees and regular reminders for staff	No	0
Policy mentions *The Health Information Protection Act* (HIPA)	No	0
Policy uses "personal health information" consistently	Yes	1
Policy requires one person to be designated to send faxes	No	0
Sending Faxes		
Policy details when personal health information may be faxed and alternatives	No	0
Policy requires employees to explain risks to clients that request that their personal health information be faxed	No	0
Policy instructs employees to remove all personal identifiers wherever possible	No	0
Policy instructs employees to confirm the correct fax number	No	0
Policy instructs employees to confirm that the recipient has appropriate safeguards in place	No	0
Policy requires a cover sheet to be used. Cover sheet should include:	Yes	1
- Sender information	Yes	1
- Recipient information	Yes	1
- Number of pages sent	Yes	1
- Confidentiality notice	Yes	1
Policy requires a fax header to display sender information, date and page numbers	No	0
Policy requires employees to carefully check the number before hitting "send"	No	0
Policy requires employees to check the fax confirmation report	No	0
Policy cautions employees not to leave personal health information on fax machine	No	0
Policy details security precautions taken after normal business hours	No	0
Tips for Fax Equipment		
Policy requires fax machines to have enhanced security features	No	0
Policy requires fax machines to be located in secure area	No	0
Policy details measures to be taken when changing fax numbers such as:		
- Renting the fax number for a few extra months	Yes	1
- destroy pre-printed forms, fax cover sheets and correspondence that refer to your previous number	No	0
- change pre-programmed a fax header	No	0
- ensure that the hard drive has been properly scrubbed to remove all information that was stored on the hard drive or memory	No	0
Policy instructs employees to use pre-programmed commonly used fax numbers	No	0
Policy details how and when pre-programmed numbers should be verified and updated	No	0
	Total points:	**7**

Additional Comments:

The faxing policy and procedure provided by Dr. Wilson appears to be that of the University of Saskatchewan's College of Medicine. This is not compliant with section 16 of HIPA.

TOTAL SCORE: 11/40

APPENDIX B

Trustee Responses

TRUSTEE RESPONSES

On or about November 7, 2013, my office shared with each of the trustees a copy of a draft analysis for this Investigation Report. They were asked the following:

> We would like you to review the attached draft Report and provide us with the following:
>
> 1) A list of recommendations that you will be committing to accept. We will note your responses in the public Report. Estimated timelines for implementation would be helpful as well…

We asked that we receive the responses no later than December 9, 2013. As noted below, we received responses from all trustees with the exception of FHRHA. Further, the response of Dr. Gary Hunter (Lakeview Neurology) was dated November 12, 2013 but did not arrive in my office until December 19, 2013. With respect to the recommendations, it stated "We have tried to implement all of these suggestions to the best of our comprehension, acknowledging no specific training in Health Information policies or details of e-health privacy regulations." It gave no specific details for each recommendation.

C – Trustee has committed to adopting the recommendation and has already taken steps or provided a plan and timelines.

L – Trustee is looking into possibly adopting the recommendation or has committed but provided no details with respect to implementation.

R – Trustee has rejected the recommendation.

N – Trustee has not provided a response.

Shaded – Recommendation does not apply to the Trustee.

Recommendation	Lakeview Neurology	FHRHA	PAPRHA	PNRHA	SRHA	HRHA	Sunrise	MCRRHA	RQRHA	Dr. T.W. Wilson
That all trustees disable 'auto-suggest' features within its electronic systems if such a technical solution is possible.	N	N	L	R	L	N	R	L	L	N
That all trustees develop consistent privacy breach investigation protocol in accordance with *Helpful Tips: Privacy Breach Guidelines.*	N	N	C	C	C	C	C	C	C	L
That all trustees consistently follow privacy breach investigation protocol when a privacy breach occurs, even if its information management service provider is also investigating the same issue.	N	N	C	C	L	L	C	C	C	L
That all trustees develop comprehensive and specific faxing policies and procedures tailored to its organization as detailed on page 55 of this analysis.	N	N	C	C	C	L	C	C	L	L

C – Trustee has committed to adopting the recommendation and has already taken steps or provided a plan and timelines.

L – Trustee is looking into possibly adopting the recommendation or has committed but provided no details with respect to implementation.

R – Trustee has rejected the recommendation.

N – Trustee has not provided a response.

Shaded – Recommendation does not apply to the Trustee.

Recommendation	Lakeview Neurology	FHRHA	PAPRHA	PNRHA	SRHA	HRHA	Sunrise	MCRRHA	RQRHA	Dr. T.W. Wilson
That all trustees that purchase the CPSS physician directory subscribe so that it will also receive the monthly notifications.	N	N	C	N	C	L	C	C	C	L
That all trustees with subscriptions to the CPSS physician directory develop a procedure that all copies be manually updated in ink when monthly notifications are received rather than keeping the notifications in the book.	N	N	C	N	C	N	C	C	L	L
That all trustees devise strategies and corresponding policies and procedures to audit and update all sources of fax contact information regularly. This includes fax information in EMRs and EHRs, preprogrammed features on individual fax machines and traditional paper directories.	N	N	C	N	L	L	C	C	C	L
That all trustees using the Radiology Information System work with eHealth Saskatchewan to verify relevant fax numbers within the system immediately and on an annual basis.		N	L	R	R	L	L	C	C	
That trustees using the Radiology Information System work with eHealth Saskatchewan and other regional health authorities to devise a strategy for updating fax information within the system. The regional health authorities must then develop internal procedures that complement the strategy.		N	L	L	R	L	N	L	C	
That trustees using the Radiology Information System configure it so that faxes are allowed to be sent to the appropriate physician.		N	L	C	C	L	C	L	C	

C – Trustee has committed to adopting the recommendation and has already taken steps or provided a plan and timelines.

L – Trustee is looking into possibly adopting the recommendation or has committed but provided no details with respect to implementation.

R – Trustee has rejected the recommendation.

N – Trustee has not provided a response.

Shaded – Recommendation does not apply to the Trustee.

Recommendation	Lakeview Neurology	FHRHA	PAPRHA	PNRHA	SRHA	HRHA	Sunrise	MCRRHA	RQRHA	Dr. T.W. Wilson
That trustees using the Radiology Information System ensure there are adequate and up-to-date agreements in place with eHealth Saskatchewan concerning its use.		N	L	C	L	L	L	L	C	
That all trustees using the Radiology Information System ensure a cover sheet compliant with best practices accompanies faxes sent from this system.		N	L	L	R	L	L	L	C	
That all trustees verify that faxes sent from all machines and other sources print a fax header that is compliant with best practices.	N	N	C	C	L	L	C	N	L	L
That all trustees using the Radiology Information System should work with eHealth Saskatchewan to develop a solution so that the Radiology Information System's current design of one fax number per health care provider is not a reason for misdirected faxes.		N	L	L	R	L	L	L	C	
That the Minister of Health consider updating sections 18 and 18.1 of *The Health Information Protection Act* on an expedited basis.										
That all trustees ensure all misdirected faxes have been retrieved and securely destroyed.	N	N	C	N	N	L	C	N	N	C

Note: Many of SRHA's and PNRHA's responses were specific only to the Medical Imaging/Laboratory/Radiology Departments and not to the whole RHA.