

**REPORT ON**  
**SYSTEMIC ISSUES WITH FAXING**  
**PERSONAL HEALTH INFORMATION**



**SASKATCHEWAN INFORMATION AND**  
**PRIVACY COMMISSIONER**

**November 23, 2010**

**Office of the Saskatchewan Information and Privacy Commissioner**

503 – 1801 Hamilton Street  
Regina, Saskatchewan  
S4P 4B4

Phone: 306-787-8350  
Toll Free: 1-877-748-2298  
Fax: 306-798-1603  
Website: [www.oipc.sk.ca](http://www.oipc.sk.ca)

---

**TABLE OF CONTENTS**

---

	<b>PAGE</b>
<b>I. EXECUTIVE SUMMARY .....</b>	<b>1</b>
<b>II. BACKGROUND .....</b>	<b>1</b>
<b>1. Efforts of the OIPC to Contain the Breach .....</b>	<b>2</b>
<b>2. OIPC Investigation .....</b>	<b>5</b>
<b>III. ISSUES.....</b>	<b>7</b>
<b>IV. DISCUSSION .....</b>	<b>7</b>
<b>1. Was there a privacy breach? .....</b>	<b>7</b>
<b>2. Who is responsible for the privacy breach? .....</b>	<b>11</b>
<b>A. Misdirected faxes should be reasonably anticipated .....</b>	<b>11</b>
<b>B. Events that led to the breaches .....</b>	<b>13</b>
<i>1. Does Clinic X have responsibility for the breaches? .....</i>	<i>13</i>
<i>2. Do the trustees that sent the faxes have responsibility? .....</i>	<i>16</i>
<i>3. Does SaskTel bear any responsibility? .....</i>	<i>16</i>
<b>3. Did the trustees respond appropriately to the breach and did each have the appropriate policies and procedures in place pursuant to section 16 of HIPA? .....</b>	<b>17</b>
<b>A. Methodology for evaluating trustee responses .....</b>	<b>17</b>
<b>B. Evaluation of Investigation Reports.....</b>	<b>17</b>

# TABLE OF CONTENTS

---

	<b>PAGE</b>
<i>i. Efforts to notify the affected individual</i> .....	18
<i>ii. Evaluation of Fax Policy</i> .....	19
a. Policies and Procedures .....	19
b. Tips for Sending Faxes .....	19
c. Tips for Fax Equipment .....	21
<i>iii. Commentary on Responses of the Trustees</i> .....	22
a. Investigation Reports .....	24
b. Notice to affected individuals .....	24
c. Written Policies and Procedures .....	25
<i>iv. The three key factors that led to these privacy breaches</i> .....	27
C. Confirming recipient fax numbers and safeguards .....	31
V. CONCLUSION .....	33
VI. RECOMMENDATIONS .....	36

**Saskatchewan Information and Privacy Commissioner**  
**Report on Systemic Issues With Faxing Personal Health Information**  
**November 23, 2010**

---

## **I. EXECUTIVE SUMMARY**

The Office of the Information and Privacy Commissioner (OIPC) was alerted in April 2009 that a private business was receiving, by facsimile (fax) transmission, the personal health information of a number of individuals. The faxes were sent by pharmacies, physicians, regional health authorities (RHAs) and other health care organizations in Saskatchewan - 60 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. The OIPC immediately notified all the health regulatory bodies and RHAs of the misdirected faxes and requested that they communicate the problems with the fax number in question to all of their professional members. Since April 2009, the OIPC has worked with the trustee organizations responsible for the misdirected faxes by encouraging them to apply and follow the OIPC *Privacy Breach Guidelines* and to take appropriate remedial action. This Report reviews the circumstances surrounding the privacy breaches and evaluates systemic issues with the use of faxes by physicians, pharmacists, RHAs and other health care organizations.

## **II. BACKGROUND**

In April 2009, my office was informed by a health region (the Region) that a new third party business located in Saskatoon was receiving several faxes intended for a medical clinic of specialists also located in that City (Clinic X). Many of the faxes contained personal health information as defined in section 2(m) of *The Health Information Protection Act* (HIPA).<sup>1</sup> I thank the Region for bringing this to my attention and for its prompt, proactive response to address this breach.

As the faxes appeared to be from several sources, my office took possession of the faxes to verify the origin. We received three batches of faxes from the third party business, one on each of the following dates: April 9, 2009, April 30, 2009 and June 4, 2009. My office identified the source of each fax containing personal health information.<sup>2</sup> Each of the 31 source organizations is a trustee as defined in section 2(t) of HIPA. Once the source of each fax had been identified, my office opened an “own motion”<sup>3</sup> investigation file for each of the trustees pursuant to sections 42(1)(c) and 52 of HIPA.

---

<sup>1</sup> *The Health Information Protection Act*, S.S. 1999, c. H-0.021 (hereinafter HIPA)

<sup>2</sup> The personal health information contained within these faxes includes health history, referrals, laboratory and other medical exam reports and prescription authorization requests.

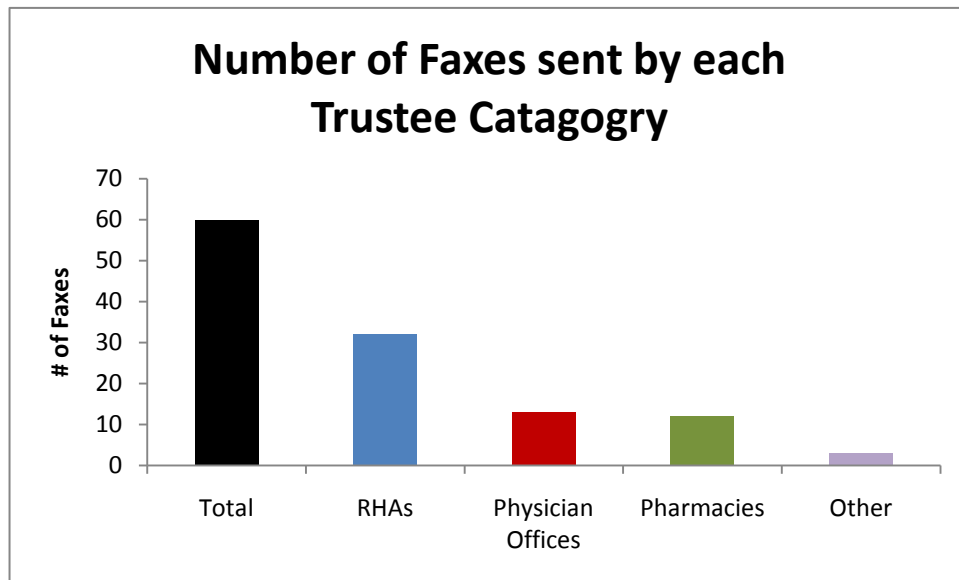
<sup>3</sup> “Own motion” means that there has been no complaint by an affected individual, however, an investigation is warranted regardless.

**Saskatchewan Information and Privacy Commissioner**  
**Report on Systemic Issues With Faxing Personal Health Information**  
**November 23, 2010**

---

I also learned that the fax number which the third party business had recently acquired was once assigned to Clinic X. The number had been out of service for approximately 17 months before the third party business acquired the number. My office also opened an investigation file for the medical clinic so that I could determine what role, if any, it had played in the above noted matter.

I have determined that 60 faxes containing personal health information were sent to the third party business by 31 different trustees. Of the 31 trustees, eight were regional health authorities (RHAs) including the Region, eleven were physician offices, nine were pharmacies and three fell into other categories.



I note that six of the 60 faxes were sent in error to the third party business multiple times. This indicates that even though the fax was not received by the intended recipient after the first time it was faxed, the fax number was not verified by each trustee before sending it subsequent times.

**1. Efforts of the OIPC to Contain the Breach**

On April 6, 2009, a representative of the Region contacted us regarding this matter. She advised that on April 2, 2009, a private business informed the Region that it appeared personal health information of patients had been incorrectly faxed to their business by the Region. The private business was initially referred to the Manager of Health Records for the Region but had to be further redirected to the Lab Manager once it was determined that the faxes consisted mostly of laboratory results of patients.

**Saskatchewan Information and Privacy Commissioner**  
***Report on Systemic Issues With Faxing Personal Health Information***  
**November 23, 2010**

---

The private business had also telephoned a health region official in another community within the Region to identify a concern that it was receiving the personal health information of individuals via their fax machine. This initial concern related to a single physician.

On April 3, 2009 the Lab Manager faxed to the office of the Region's Privacy Officer (the Privacy Officer) the documents received from the private business. This material indicated that a number of items had gone to the wrong location and identified a number of specific physicians the faxes were intended for.

The Privacy Officer then contacted the medical clinic of specialists which was the apparent addressee of the faxes. She was advised that the medical clinic was aware of the misdirected faxes to the private business and that it appeared the business now had the fax number that used to belong to the clinic prior to a number of the specialists splitting off from the clinic. She was further advised that the clinic had sent out a communiqué at that time about the change to the fax number. This would have been approximately three years earlier.

In a further phone conversation between the Privacy Officer and the private business, it was reported that about 125 documents had by then been received by the business. The contact in the business reported to the Privacy Officer that she did not get a very receptive response from the various senders of the misdirected faxes after she contacted those senders to report the error. In fact the business reported that they were advised not to worry, that this happens all the time and she should just shred the documents. The Privacy Officer made arrangements to have the documents retrieved from the business.

In yet another phone conversation, the Privacy Officer spoke with one physician who had formerly been at the medical clinic involved in this matter. This physician related that they had sent out a communiqué that their number had changed about three years ago and was willing to do so again. The Privacy Officer pointed out that a number of the faxes intended for this physician were coming from one laboratory in another community. The physician then volunteered to contact that laboratory.

The Privacy Officer then reported this whole matter to our office. She also undertook to send out memoranda to facilities in other parts of the Region and to the Region's administration personnel. She also undertook to investigate how this happened in that Region by discussions with the medical affairs department in the health region and with direct care managers. The Region proceeded to circulate a memorandum internally on the same day: "Please make sure that all staff is aware that this fax number needs to be updated."

We started reviewing the first package of materials provided to us. Many faxes were sent without cover sheets or anything to clearly identify the sender or source (i.e. no header or a fax was re-faxed). In the cases where the source was clear, we contacted them immediately to advise. We also contacted the third party business to ask it to forward any misdirected faxes it received.

**Saskatchewan Information and Privacy Commissioner**  
***Report on Systemic Issues With Faxing Personal Health Information***  
**November 23, 2010**

---

When we learned that the private business in question was continuing to receive additional faxes containing personal health information, our immediate concern was to stop that practice as quickly as possible. Hence our decision to request that all RHAs, all health professional regulatory bodies<sup>4</sup> and the Saskatchewan Cancer Agency provide notification to their members/facilities/employees of the following:

As you may have recently learned, a fax number originally assigned to the [Clinic X] has now been reassigned to a non-health related business. This business is receiving dozens of faxes each day from a variety of sources including Saskatchewan physicians, clinics and regional health authorities.

We will be commencing an investigation under *The Health Information Protection Act*. Thanks to the cooperation of [the Region], we have taken custody of a large number of faxed documents containing personal health information of many Saskatchewan residents. These faxed documents have been recently received by a business that has been assigned the fax number [...].

We request that you immediately, if you have not done so already, circulate the following message within your Region and then confirm to our office that this has been done:

It has come to our attention that physicians and Regional Health Authorities and perhaps others are continuing to fax personal health information to a fax number that now belongs to a non-trustee. Until approximately three years ago, this number had been assigned to the [Clinic X].

**DO NOT USE FAX NUMBER [...] FOR THE [Clinic X] OR FOR THE FOLLOWING PHYSICIANS:**

[names removed]

If you use pre-programmed fax numbers, please check immediately to ensure that you are not using the above number. If you have been using this number, you should immediately determine where those faxes have been going and what has happened to them over the last three years.

Please acknowledge receipt and confirm you have taken these steps.

Please refer to the *Privacy Breach Guidelines* available on the Information and Privacy Commissioner's website, [www.oipc.sk.ca](http://www.oipc.sk.ca) under the *Resources* tab for other required action to deal with the privacy breach.

---

<sup>4</sup> A full listing can be found on the Ministry of Health's website at <http://www.health.gov.sk.ca/health-professional-associations>.



**Saskatchewan Information and Privacy Commissioner**  
***Report on Systemic Issues With Faxing Personal Health Information***  
**November 23, 2010**

---

As well, we have prepared a resource titled *Privacy Considerations: Faxing Personal Information and Personal Health Information* that may also be circulated. A copy is enclosed for your purposes.

At the same time, we provided the above notification to the bodies noted between April 13, 2009 and April 16, 2009. We also advised the Ministry of Health.

We are very grateful for the efforts extended by these bodies to help communicate the above message once we brought the matter to their attention.

Unfortunately, on April 22, 2009, the private sector business advised us that they were still receiving faxes, and that they would forward them to our office.

## **2. OIPC Investigation**

In June and July of 2009, once the sources of each fax were identified, we opened investigation files for each trustee. At the outset, my office provided notification of our intention to undertake an investigation pursuant to sections 42(1)(c) and 52 of HIPA which states:

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

...

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

52 The commissioner may:

(a) offer comment on the implications for personal health information of proposed legislative schemes or programs of trustees;

(b) after hearing a trustee, recommend that the trustee:

(i) cease or modify a specified practice of collecting, using or disclosing information that contravenes this Act; and

(ii) destroy collections of personal health information collected in contravention of this Act;

(c) in appropriate circumstances, comment on the collection of personal health information in a manner other than directly from the individual to whom it relates;

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

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

**Saskatchewan Information and Privacy Commissioner**  
**Report on Systemic Issues With Faxing Personal Health Information**  
**November 23, 2010**

---

In addition, further authority is found in section 53 of HIPA which reads as follows:

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.

Without describing the personal health information or revealing the identity of the affected individual(s), we provided a description of the faxes believed to have originated from each trustee's organization and asked that they confirm that the fax had originated from their office. Once my office was comfortable that the fax did indeed originate from that trustee, we provided the trustee with a copy of the fax to aid them in their investigations and allow them to inform the affected individual about the breach.

My office also provided notification to Clinic X that we would be investigating its role in this situation.

Also, in the notification letters, trustees were asked to provide my office with a copy of their investigation reports on the incident and a copy of their fax policies required by section 16 of HIPA. To aid them with this, trustees were also provided with a copy, or directed to, two of my offices resources: *Privacy Breach Guidelines (Guidelines)* and *Privacy Considerations - Faxing Personal Information and Personal Health Information (Faxing Considerations)*. Both are available at [www.oipc.sk.ca](http://www.oipc.sk.ca).

In April 2010, my office advised the trustees that I would be issuing a Report pursuant to section 52 of HIPA. Trustees were given further opportunity to provide submissions regarding their investigation reports and fax policies as these would be evaluated as part of the Report. We also advised that they should provide notification to the affected individual and that this would also be part of an overall score given to each trustee.

This fall, we provided each trustee with a copy of their individual evaluation based on their submission and asked them to check for errors. Any reported errors have been corrected.

**Saskatchewan Information and Privacy Commissioner**  
***Report on Systemic Issues With Faxing Personal Health Information***  
**November 23, 2010**

---

In this Report, we do not identify the individual trustees involved in this investigation. I made this decision for several reasons. If it had not been for the Region, 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 our office. 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 have taken remedial action to help prevent a future occurrence. I am also mindful that most of the trustees in question have notified the affected individuals and my office has not received any complaints from those individuals.

### **III. ISSUES**

- 1. Was there a privacy breach?**
- 2. Who is responsible for the privacy breach?**
- 3. Did the trustees respond appropriately to the breach and did each have the appropriate policies and procedures in place pursuant to section 16 of HIPA?**

### **DISCUSSION**

#### **1. Was there a privacy breach?**

We stated in *Faxing Considerations* that “a privacy breach occurs when a government institution, local authority or trustee (organization) fails to take reasonable measures to safeguard personal information or personal health information in its possession/custody or control.”<sup>5</sup>

When faxed by the aforementioned trustees to the third party business, the personal health information contained within was sent to an unintended recipient who had nothing to do with providing health care services to the patients in question. This constituted a disclosure. In terms of disclosures, section 23(1) of HIPA requires that:

23(1) A trustee shall collect, use or disclose only the personal health information that is reasonably necessary for the purpose for which it is being collected, used or disclosed.

---

<sup>5</sup> Saskatchewan Office of the Information and Privacy Commissioner (hereinafter OIPC) *Privacy Breach Guidelines and Privacy Considerations - Faxing Personal Information and Personal Health Information* (Faxing Considerations) at p. 1, available online at [www.oipc.sk.ca](http://www.oipc.sk.ca).

**Saskatchewan Information and Privacy Commissioner**  
***Report on Systemic Issues With Faxing Personal Health Information***  
**November 23, 2010**

---

Further though, section 27 of HIPA authorizes trustees to disclose personal health information without consent for the purposes articulated as follows:

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

(2) A subject individual is deemed to consent to the disclosure of personal health information:

(a) for the purpose for which the information was collected by the trustee or for a purpose that is consistent with that purpose;

(b) for the purpose of arranging, assessing the need for, providing, continuing, or supporting the provision of, a service requested or required by the subject individual; or

(c) to the subject individual's next of kin or someone with whom the subject individual has a close personal relationship if:

(i) the disclosure relates to health services currently being provided to the subject individual; and

(ii) the subject individual has not expressed a contrary intention to a disclosure of that type.

(3) A trustee shall not disclose personal health information on the basis of a consent pursuant to subsection (2) unless:

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

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

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

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

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

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

**Saskatchewan Information and Privacy Commissioner**  
**Report on Systemic Issues With Faxing Personal Health Information**  
**November 23, 2010**

---

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

(e) if the subject individual is deceased:

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

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

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

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

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

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

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

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

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

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

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

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

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

**Saskatchewan Information and Privacy Commissioner**  
**Report on Systemic Issues With Faxing Personal Health Information**  
**November 23, 2010**

---

- (j) subject to subsection (6), where the disclosure is being made for the provision of health or social services to the subject individual, if, in the opinion of the trustee, disclosure of the personal health information will clearly benefit the health or well-being of the subject individual, but only where it is not reasonably practicable to obtain consent;
  - (k) where the disclosure is being made for the purpose of:
    - (i) obtaining payment for the provision of services to the subject individual; or
    - (ii) planning, delivering, evaluating or monitoring a program of the trustee;
  - (l) where the disclosure is permitted pursuant to any Act or regulation;
  - (m) where the disclosure is being made to the trustee's legal counsel for the purpose of providing legal services to the trustee;
  - (n) in the case of a trustee who controls the operation of a pharmacy as defined in *The Pharmacy Act, 1996*, a physician, a dentist or the minister, where the disclosure is being made pursuant to a program to monitor the use of drugs that is authorized by a bylaw made pursuant to *The Medical Profession Act, 1981* and approved by the minister;
  - (o) in the case of a trustee who controls the operation of a pharmacy as defined in *The Pharmacy Act, 1996*, where the disclosure is being made pursuant to a program to monitor the use of drugs that is authorized by a bylaw made pursuant to *The Pharmacy Act, 1996* and approved by the minister;
  - (p) in prescribed circumstances.
- (5) For the purposes of clause (4)(h), where the personal health information in question is about a member of the profession regulated by the health professional body or prescribed professional body, disclosure may be made only:
- (a) in accordance with clause (4)(i);
  - (b) with the express consent of the subject individual; or
  - (c) if the trustee has reasonable grounds to believe that the personal health information is relevant to the ability of the subject individual to practise his or her profession, on the request of the health professional body or prescribed professional body.
- (6) Disclosure of personal health information pursuant to clause (4)(j) may be made only where the person to whom the information is to be disclosed agrees:
- (a) to use the information only for the purpose for which it is being disclosed; and
  - (b) not to make a further disclosure of the information in the course of carrying out any of the activities mentioned in that clause.

**Saskatchewan Information and Privacy Commissioner**  
**Report on Systemic Issues With Faxing Personal Health Information**  
**November 23, 2010**

---

None of the trustees that sent the faxes containing personal health information have attempted to make the case that the third party business had a need to know, or that the disclosure was made for a purpose consistent with the purpose for which it was collected, or did so for one of the purposes enumerated above. As a result, each unauthorized disclosure constitutes a separate privacy breach.

## **2. Who is responsible for the privacy breaches?**

Section 16 of HIPA states:

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.**

[emphasis added]

### **A. Misdirected faxes should be reasonably anticipated**

Misdirected faxes are an all too common occurrence. My colleagues across the country have investigated numerous instances of misdirected faxes containing personal information and personal health information. There are also frequent reports of misdirected faxes in the media. The following is a non-exhaustive list of examples of such investigations and reports:

- 2004 – An Edmonton couple, who managed an apartment building, received misdirected faxes containing personal health information from two different health care organizations in Alberta. The Office of the Privacy Commissioner of Canada and Office of the Information and Privacy Commissioner of Alberta collaborated in investigating this incident.<sup>6</sup> It was concluded that these organizations disclosed personal information without consent in violation of the *Personal Information Protection and Electronic Documents Act* (PIPEDA)

---

<sup>6</sup> Details of the incident may be found at the Privacy Commissioner of Canada website available online at [http://www.priv.gc.ca/incidents/2004/041221\\_e.cfm](http://www.priv.gc.ca/incidents/2004/041221_e.cfm)

**Saskatchewan Information and Privacy Commissioner**  
**Report on Systemic Issues With Faxing Personal Health Information**  
**November 23, 2010**

---

- 2004 – The Office of the Privacy Commissioner of Canada launched an investigation into faxes containing personal information that were misdirected by Canadian Imperial Bank of Commerce (CIBC) to a company in the United States and one in Quebec. This had been occurring from 2001 to 2004. It was found that CIBC did not have appropriate safeguards in place.<sup>7</sup> As a result, a class action suit was brought against CIBC.<sup>8</sup>
- 2007 – For more than three years, an Edmonton couple received misdirected faxes containing personal information from the Bank of Montreal (BMO). This story was reported by CTV news in 2007. The Office of the Privacy Commissioner of Canada was aware of the situation.<sup>9</sup>
- 2007 – CBC reported that a woman in Winnipeg was receiving faxes containing personal health information on her personal fax machine for years from several medical clinics, a health sciences centre and a provincial office. The faxes continued even after she complained to the Ministry of Health.<sup>10</sup>
- 2009 – The Information and Privacy Commissioner of Alberta investigated a health organization that had been sending faxes containing personal health information to the private fax machine of a woman in Alberta. The Commissioner found that the health organization had not taken reasonable steps to protect the personal health information from unauthorized disclosure.<sup>11</sup>
- 2010 – A Winnipeg man received numerous faxes containing personal health information from St. Boniface Hospital. CBC reported that the recipient was acquainted with one of the affected individuals. He continued to receive faxes even after he notified the hospital of the situation.<sup>12</sup>
- 2010 – The *Calgary Sun* reported that its fax machine in its news room received an 11 page misdirected fax detailing a pregnant woman’s health information from her physician’s office. The information included past diseases, pap smears and sexual past.<sup>13</sup>

---

<sup>7</sup> Privacy Commissioner of Canada available online at [http://www.priv.gc.ca/incidents/2005/050418\\_01\\_e.cfm](http://www.priv.gc.ca/incidents/2005/050418_01_e.cfm)

<sup>8</sup> *Speevak v. Canadian Imperial Bank of Commerce*, 2010 ONSC 1128; CanLII – 2010 ONSC 1128

<sup>9</sup> *BMO probing faxes mistakenly sent to Alta. Couple*, June 7, 2007 available online at [http://www.ctv.ca/CTVNews/TopStories/20070607/faxes\\_bank\\_070607/](http://www.ctv.ca/CTVNews/TopStories/20070607/faxes_bank_070607/)

<sup>10</sup> *Medical faxes misdirected to Winnipeg woman’s home*, September 13, 2007 available online at [www.cbc.ca/health/story/2007/09/13/medical-faxes.html](http://www.cbc.ca/health/story/2007/09/13/medical-faxes.html)

<sup>11</sup> Information and Privacy Commissioner of Alberta, Investigation Report H2009-IR-004 available online at <http://www.oipc.ab.ca/pages/OIP/InvestigationReports.aspx?id=2979>

<sup>12</sup> *Patients’ records faxed to wrong numbers*, March 3, 2010 available online at <http://www.cbc.ca/manitoba/story/2010/03/03/mb-faxes-hospital-wayward-winnipeg.html>

<sup>13</sup> *Fax foibles prove need for electronic health records*, April 21, 2010 available online at [http://www.calgarysun.com/news/columnists/michael\\_platt/2010/04/20/13658701.html](http://www.calgarysun.com/news/columnists/michael_platt/2010/04/20/13658701.html)



**Saskatchewan Information and Privacy Commissioner**  
**Report on Systemic Issues With Faxing Personal Health Information**  
**November 23, 2010**

---

- 2010 – CBC’s Yellowknife Newsroom also received two misdirected faxes containing personal health information from the Yellowknife and Fort Smith Health and Social Services Authorities.<sup>14</sup>
- 2010 – The *Toronto Sun* reported that a dentist had been receiving faxes for a physician who specializes in obesity. There is one number difference between the two professionals’ fax numbers.<sup>15</sup>

Several trustees involved in this investigation have also acknowledged that misdirected faxes are a very common occurrence in the health sector. This is clearly a privacy risk that must be reasonably anticipated by trustees.

**B. Events that led to the breaches**

Prior to June 30, 2007, Clinic X was comprised of nine physicians and operated under a different name. It used the fax number that was later reassigned to the third party business. Three of the nine physicians left the clinic between the period of July 2006 and June 2007. On July 1, 2007, Clinic X assumed its current name and acquired new telephone and fax numbers. An additional fax number is also used solely by one of the clinic’s current physicians, Dr. P.

On January 30, 2009, the third party business was assigned the fax number in question. It began receiving faxes containing personal health information on March 27, 2009.

*i. Does Clinic X have responsibility for the breaches?*

Clinic X has advised my office that it took the following steps to advise the medical community of its change of coordinates:

- Advertised the change in the *Saskatoon Star Phoenix* on June 16, 2007, June 23, 2007 and the *Saskatoon Sun* on June 24, 2007.
- A message on the Clinic’s previous phone number listed new coordinates for Clinic X and separated physicians. This message was left on the previous telephone number for three months after the change.
- Canadian Medical Association, College of Physicians and Surgeons of Saskatchewan (CPSS), Saskatchewan Medical Association and Medical Care Insurance Branch were alerted to the change of contact information for Clinic X and asked to update their directories.

---

<sup>14</sup> *More N.W.T. medical records faxed to CBC*, June 25, 2010 available online at [www.cbc.ca/canada/north/story/2010.06/25/nwt-medical-records-cbc.html](http://www.cbc.ca/canada/north/story/2010.06/25/nwt-medical-records-cbc.html)

<sup>15</sup> *Medical Records go to wrong fax*, September 22, 2010 available online at [www.torontosun.com/news/torontoandgta/2010/09/22/15443946.html](http://www.torontosun.com/news/torontoandgta/2010/09/22/15443946.html)

**Saskatchewan Information and Privacy Commissioner**  
**Report on Systemic Issues With Faxing Personal Health Information**  
**November 23, 2010**

---

- A fax notification was sent to health care organizations in June 2007. The fax was sent to 9 medical associations such as CPSS, 39 fax numbers within RHAs around the province, 21 medical clinics within Saskatoon, 14 medical clinics outside of Saskatoon, 82 pharmacies within Saskatoon and 6 other health organizations.
- Clinic X also advised that it destroyed stamps and prescription pads with outdated contact information on June 30, 2007.

My office's *Faxing Considerations* lists the following best practices when changing fax machine numbers:

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.

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.

Although it appears that Clinic X sent fax notification to 171 different health care organizations, only 11 of the 31 trustees that sent misdirected faxes were on this list. The other 20 organizations included RHAs, pharmacies outside of Saskatoon and medical clinics located both within and outside of the city. When asked how the list was compiled, Clinic X simply stated in a letter dated September 20, 2010 "We used the College of Physicians and Surgeons of Saskatchewan mailing list and a fax list of the Saskatoon Pharmacies."

Clearly the list compiled by Clinic X was neither current nor comprehensive and contributed to these breaches.

We have also found that an omission of Clinic X may have contributed to at least one specific privacy breach.

On June 19, 2009, we received a call from one of the 31 trustees, a pharmacy, which sent one of the misdirected faxes. The pharmacy informed my office that they had received a prescription from one of the physicians from Clinic X. The prescription was dated June 9, 2009 and bore Clinic X's former fax number.

**Saskatchewan Information and Privacy Commissioner**  
***Report on Systemic Issues With Faxing Personal Health Information***  
**November 23, 2010**

---

My office raised this issue with Clinic X in a letter dated June 22, 2009; however, it has not addressed this specific issue in any of its submissions to us. Clinic X has informed me that the prescription in question originated from Dr. P. It appears that this physician's prescription pads bearing the outdated contact information were not destroyed on June 30, 2007 as noted by Clinic X.

The misdirected fax that was sent to the third party business by this pharmacy was dated April 6, 2009 and the prescription in question was dated June 9, 2009. Therefore, I cannot conclude with certainty that the outdated prescription pad played a role in any of these privacy breaches. However, its potential to cause them is obvious.

Additionally, as a result of my office's efforts to contain this breach, we were notified by telephone on April 16, 2009 by a physician's office that was not involved in these breaches, that it had received a series of faxes from Clinic X advising of meeting dates and times. The faxes, which did not contain personal health information, were intended for this physician's office. All of the faxes were sent after January 1, 2009. However, the physician's office noticed that the fax header on the top of the faxes bore the outdated fax number. My office asked Clinic X to investigate this issue.

Clinic X addressed the outdated header as follows:

In April 2009 our office received a call from another Medical Office in regards to the wrong header on a fax that was received by to [sic] them. Our office has two fax machines one belonging to [Clinic X] and the other belonging to [Dr. P]'s office. The fax machine that was used to send the fax out was from [Dr. P]'s office and exclusively used by his staff. [Dr. P]'s office obtained the fax machine from the previous office of [Clinic X]. [Dr. P]'s office was unaware that the fax header was incorrect. The fax machine was taken out of service as soon as [Clinic X] and [Dr. P] was notified about the incorrect fax header in April, 2009. On June 16, 2009 the manual for the fax machine was located and the header was changed immediately.

None of the 31 trustees who sent misdirected faxes to the third party business identified the outdated fax header as a factor in the misdirected faxes originating from their office. However, I reiterate that outdated material such as the prescription pad and this fax header had the potential to cause misdirected faxes containing personal health information.

Also, the fact that Clinic X was unaware of the need to change the programmable fax header highlights the need for comprehensive written policies that include procedures for changing contact information as discussed later in this Report.

**Saskatchewan Information and Privacy Commissioner**  
***Report on Systemic Issues With Faxing Personal Health Information***  
**November 23, 2010**

---

I find that Clinic X could have reasonably done more to ensure that personal health information would be safeguarded. It failed to have the administrative, technical and physical safeguards to protect against reasonably anticipated disclosures of personal health information.

Clinic X contributed to the privacy breaches by not advising a comprehensive list of colleagues of the change in its coordinates and by using material that contained outdated contact information. However, the personal health information that was disclosed to the third party business was never in the custody or control of Clinic X. Clinic X did make a series of efforts to communicate its new coordinates and fax number to physicians and pharmacists. As a result it would not be fair to assign all responsibility for the breaches to Clinic X.

***ii. Do the trustees that sent the faxes have responsibility?***

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.

None of the 31 trustees have indicated that they made these disclosures to the third party business by fax intentionally or with the requisite authority. As such, each was an unauthorized disclosure and I must conclude that for every fax it sent, that trustee in question was responsible for the resultant privacy breach.

***iii. Does SaskTel bear any responsibility?***

Throughout my investigation, a few trustees have commented or suggested that SaskTel also had a role to play in these privacy breaches.

One physician's office asked:

Our other concern would then be why would Sasktel assign a used health fax number to the general public. Do they have to answer to the Commission also?

A pharmacy suggested:

As a suggestion, if a fax number is changed, perhaps it should be reissued only as a phone number therefore blocking the possibility of privacy breaches by fax. As well, a more pertinent suggestion would be to issue and use a medical phone number or fax number only once therefore not re-introducing the number to ever create privacy issues.

**Saskatchewan Information and Privacy Commissioner**  
**Report on Systemic Issues With Faxing Personal Health Information**  
**November 23, 2010**

---

As such, I will consider if SaskTel bears any responsibility.

Although I do have privacy and access oversight over this Crown corporation through *The Freedom of Information and Protection of Privacy Act*<sup>16</sup> and HIPA, Sasktel does not have any responsibility in this matter as it is not a trustee for the purposes of section 2(t) of HIPA in this particular case because it, at no time, had custody or control of the personal health information involved in these breaches.

I consulted with SaskTel regarding this situation in April 2009. Its Privacy Officer was helpful in confirming that the number had been inactive for 17 months after Clinic X had changed phone numbers. He confirmed faxes sent to this number during the 17 months would not have been transmitted. He also informed me that there was a business need to recycle fax numbers and they are usually out of service for only about 3 months. SaskTel also offered to change the fax number of the third party business free of charge if my office found it beneficial to do so.

I conclude that SaskTel bears no responsibility for these breaches. I also applaud SaskTel for its cooperation.

**3. Did the trustees who sent the faxes respond appropriately to the breach and did they have the appropriate policies and procedures in place pursuant to section 16 of HIPA?**

**A. Methodology for evaluating trustee responses**

Throughout this investigation my office asked each trustee to meet three requirements:

- To prepare an investigation report;
- Notify the affected individuals; and
- Detail and provide copies of written fax policies and procedures.

These will be the basis of my evaluation.

**B. Evaluation of Investigation Report**

In my office's notification letter to the trustees, we asked each one to send us a copy of its investigation report. They were directed to my office's *Guidelines* to assist them in their investigation. The criteria for investigation reports listed beginning on page 4 of the *Guidelines* will be my basis for evaluating each trustee's report.

---

<sup>16</sup> *The Freedom of Information and Protection of Privacy Act*, S.S. 1990-91, c. F-22.01 (as amended) (hereinafter FOIP)

**Saskatchewan Information and Privacy Commissioner**  
***Report on Systemic Issues With Faxing Personal Health Information***  
**November 23, 2010**

---

The criteria are 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.
  - 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.

The score for the investigation report portion is out of a possible 10 points.

***i. Efforts to notify the affected individual***

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

**ii. Evaluation of Fax Policy**

By means of letters in April 2010, my office advised the trustees of my intention to review their fax policies and procedures. At that time, the trustees were also reminded of our resource entitled *Faxing Considerations* which my office referenced in our notification letters. As such, I rely on the best practices listed in this document as the basis for my evaluation of the fax policies.

The best practices include:

**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.

**Saskatchewan Information and Privacy Commissioner**  
***Report on Systemic Issues With Faxing Personal Health Information***  
**November 23, 2010**

---

- 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.



**Saskatchewan Information and Privacy Commissioner**  
***Report on Systemic Issues With Faxing Personal Health Information***  
**November 23, 2010**

---

- 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 relocate 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.

**Saskatchewan Information and Privacy Commissioner**  
**Report on Systemic Issues With Faxing Personal Health Information**  
**November 23, 2010**

---

- 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.

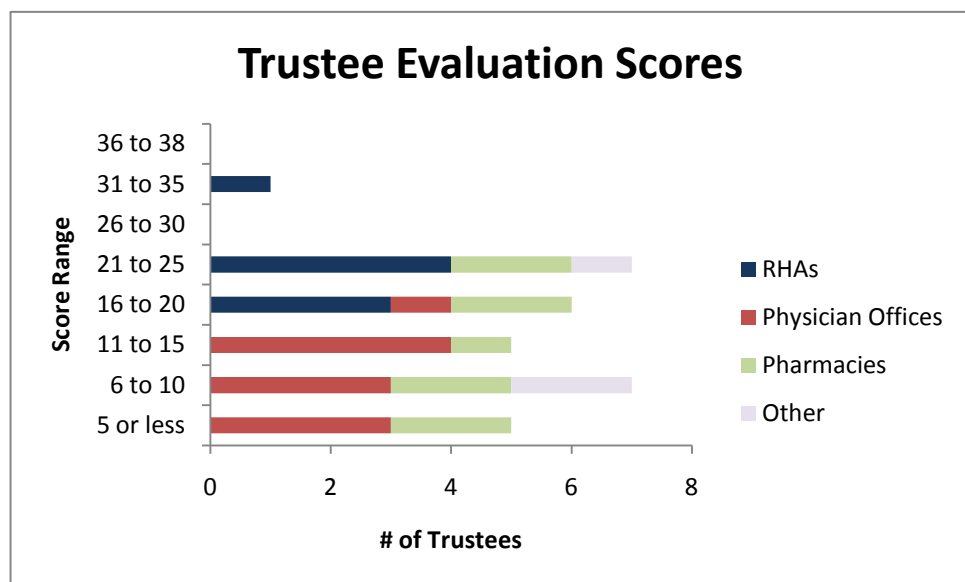
The fax policies of several trustees also included other practices that are helpful for protecting personal health information. Bonus points were awarded for additional good practices.

After evaluating each trustee's investigation report, fax policy and attempts to notify the affected individual a total score out of 38 points was assigned to each trustee.

In September of 2010, I shared my preliminary evaluation with each trustee and asked that any errors or omissions be identified to my office. Necessary adjustments have been made.

***iii. Commentary on Responses of the Trustees***

The average score of the 31 trustees was only 13.7 out of 38. The chart and table below provide further detail on the scores of the trustees.



**Saskatchewan Information and Privacy Commissioner**  
**Report on Systemic Issues With Faxing Personal Health Information**  
**November 23, 2010**

---

		<b>RHAs</b>	<b>Physician Offices</b>	<b>Pharmacies</b>	<b>Other</b>	<b>Total</b>
<b>Score Range</b>	5 or less	0	3	2	0	<b>5</b>
	6 to 10	0	3	2	2	<b>7</b>
	11 to 15	0	4	1	0	<b>5</b>
	16 to 20	3	1	2	0	<b>6</b>
	21 to 25	4	0	2	1	<b>7</b>
	26 to 30	0	0	0	0	<b>0</b>
	31 to 35	1	0	0	0	<b>1</b>
	36 to 38	0	0	0	0	<b>0</b>
	<b>Total</b>	<b>8</b>	<b>11</b>	<b>9</b>	<b>3</b>	<b>31</b>

In my view, the trustees involved in this Report reflect a fair sampling of trustee organizations in this province. This analysis suggests that there is a good deal of work yet to be done by trustees in Saskatchewan.

My first observation is that RHAs have generally scored higher than physician offices. More than one physician's office contended that they have fewer resources at their disposal to develop and implement section 16 policies and procedures than RHAs or larger organizations. One trustee in particular wrote:

Although you state your evaluation system was meant to treat all trustees as fairly and equally as possible all offices do not have equal resources and/or staff at their disposal. As an example, we are a one-physician office with limited staff (ideally, 2 full time employees; often only one full-time employee and, at other times 1 full-time employee with various part time employees). We cannot be compared "equally" to offices with multiple physicians and therefore more employees at their disposal; nor can we be compared to larger clinic settings such as hospitals, etc., who have specific staff designated for implementing policies.

**Saskatchewan Information and Privacy Commissioner**  
**Report on Systemic Issues With Faxing Personal Health Information**  
**November 23, 2010**

---

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.

**a. Investigation Reports**

Many of the trustees did not submit formal investigation reports. These trustees' scores are a reflection of comments pulled from the correspondence with my office.

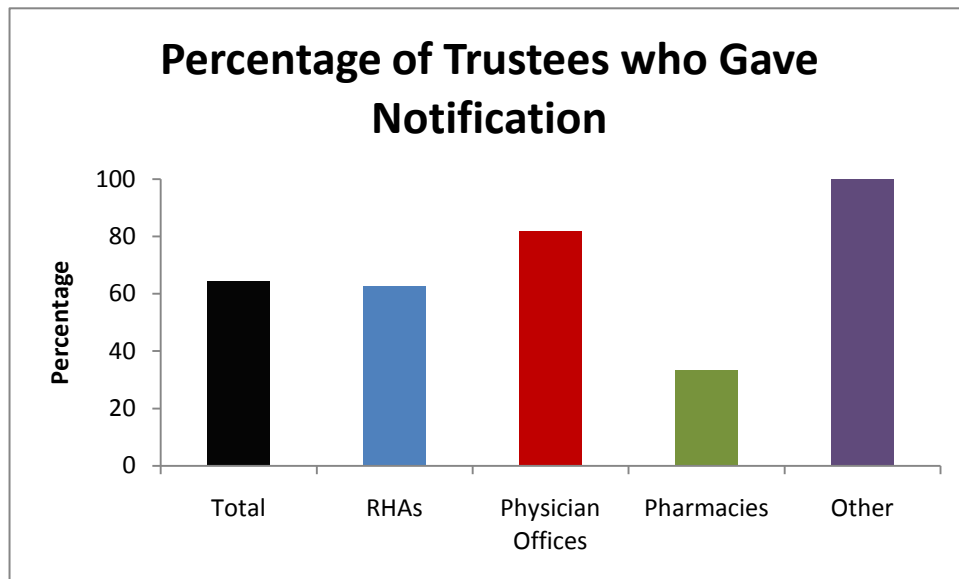
Much of the correspondence from the trustees focused on actions taken to contain the breach, prevent similar occurrences and, in some cases, blame others for the unauthorized disclosure of personal health information. Very few of the trustees actually explored the reasons why the faxes were sent in error. I have found that, besides the change in fax number of Clinic X, the two main causes of the breach were: (1) outdated pre-programmed fax numbers and contact information and; (2) carelessness of trustees as evidenced by a lack of training as explained below.

I have also found during my investigation, that for the most part, trustees have not adequately investigated these breaches. Our review of the fax policies below suggests that trustees have not addressed the substantive causes of the breaches and their fax policies and procedures are inadequate to minimize the risk of future breaches.

**b. Notice to 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.

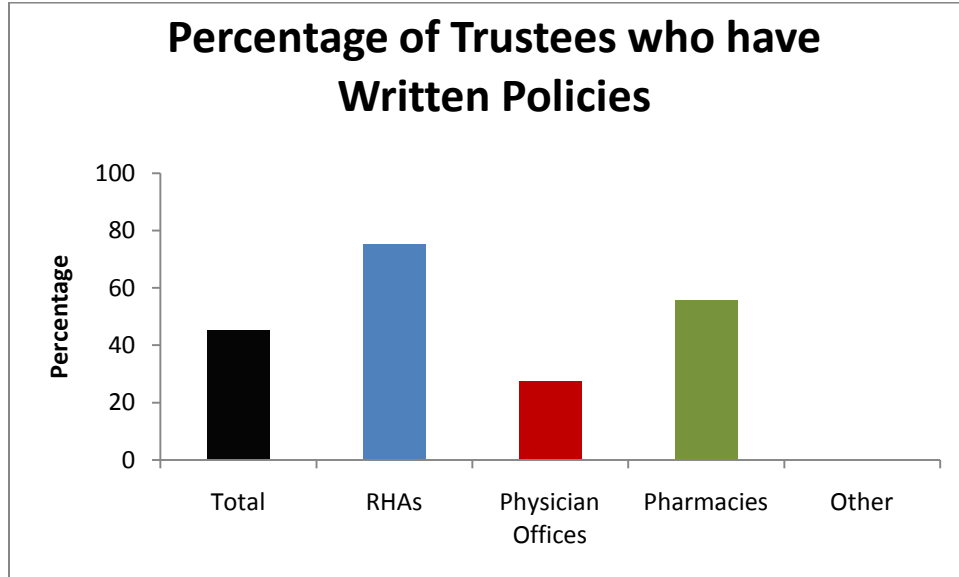
I found that 20 out of the 31 trustees, or 64.5%, provided notification to the affected individuals or made reasonable efforts to do so. Further, 5 of the 8 (62.5%) RHAs, 9 of the 11 (81.8%) physician offices and all 3 (100%) of the trustees that fell in other categories gave notification to the individuals affected in these breaches. However, I find it troubling that only 3 of the 9 (33.3%) pharmacies provided notification to their affected patients.



**c. Written Policies and Procedures**

I asked each trustee to provide a copy of its written policies and procedures regarding faxing personal health information. Only 14 out of the 31 (45.2%) trustees had actual written policies. Some trustees had informed my office that they had written policies, but did not supply my office with a copy as requested. In those cases, a point was not awarded.

I note that even though a trustee was awarded a point for a written policy, it is not necessarily a reflection of the quality of the document. The entire score must be taken into account. In terms of evaluating the policies and procedures of the trustees which do not have written policies and procedures, their points were, again, awarded from statements made in correspondence to my office.



I do note that the RHAs are the trustees with the highest percentage of written policies at 75% (6 of the 8 RHAs have written fax policies). However, as previously discussed, it is the duty of all trustees to have policies and procedures to protect personal health information.

Written policies and procedures are helpful as a reference for employees of trustees, especially when adequate training programs and regular reminder mechanisms are not in place. They help trustees clarify privacy expectations with its employees. As described by the physician who commented on the lack of resources, physicians offices can often have a variety of staff working at different times. Written policies are a tool to ensure that staff are properly trained and can be useful for an office with a high turn over or numerous part-time employees. A well written policy should also advise employees of the risks and consequences of non-compliance.

I expect all trustees in Saskatchewan to adopt comprehensive written policies and procedures that include policy and procedure for faxing personal health information.

**Saskatchewan Information and Privacy Commissioner**  
**Report on Systemic Issues With Faxing Personal Health Information**  
**November 23, 2010**

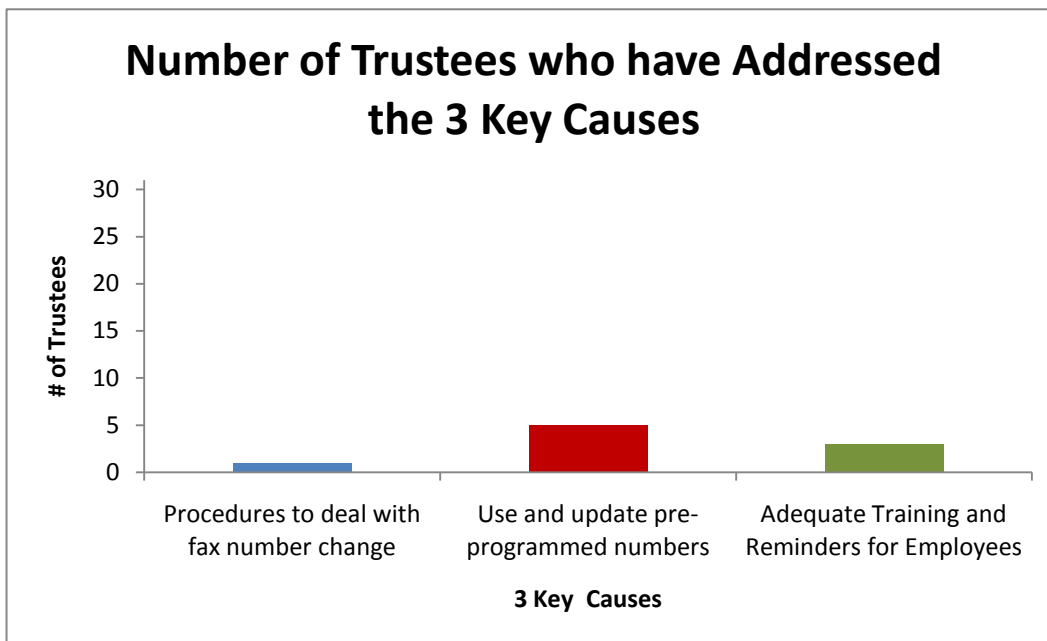
---

*iv. The three key factors that led to these privacy breaches*

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.

However, very few of the trustees have addressed these issues in written policies and procedures or correspondence with our office. The chart below shows the number of trustees in all categories that have adequately addressed these issues.



These low numbers indicate to me that, on the whole, the trustees in question have not adequately investigated these breaches nor have they adopted appropriate safeguards to prevent similar occurrences in the future.

**Saskatchewan Information and Privacy Commissioner**  
***Report on Systemic Issues With Faxing Personal Health Information***  
**November 23, 2010**

---

- ***Procedures to deal with a change of fax number***

I am troubled that only one of the 31 trustees that sent misdirected faxes to the third party business appear to have addressed this issue. I also note, that the single trustee who did address this issue considered only one of the four corresponding best practices. The changing of a fax number was the root cause of this privacy breach and in my office's notification letters, all of the trustees were made aware that this was the case.

What is even of more concern is that several trustees concluded that the breach occurred because they had not been advised of the change in fax number. They attempted to shift responsibility to someone else. Other trustees attributed blame to Clinic X or other bodies. For example, one pharmacy stated:

The list of practitioners outlined in a bulletin from the Saskatchewan College of Pharmacists [...] was checked within a reasonable time after receiving it on April 15<sup>th</sup> of 2009. We found that we had pre-programmed the fax number [in question], for only [Dr. B] in our computer system which could have been the result of the fax going to the wrong office.

A second bulletin outlined the new phone number and fax number of [Clinic X] (generated by [Clinic X] and circulated by fax in Saskatoon on April 16<sup>th</sup>, 2009), and interestingly enough, does not have [Dr. B] listed as a member of that group. This creates the possibility to overlook checking [Dr. B]'s fax number. However, using the first bulletin from the Saskatchewan College of Pharmacists, we did verify [Dr. B]'s fax number.

Therefore the conclusion would be that we acted responsibly to insure that we had the correct fax numbers for the practitioners in question, but only after receiving the bulletin on April 15<sup>th</sup> (the day after the alleged fax was sent to the wrong number). As well no previous bulletin or notification of this fax number change was provided to our business prior to the one that the Saskatchewan College of Pharmacists sent out.

We note that the physician referred to by the pharmacy (Dr. B) left Clinic X on July 1, 2006 and no longer used the fax number in question at that time.

The response of the trustees is inadequate as they did not take responsibility for causing the breach and as they did not address the issue of change of contact information in any real way.



**Saskatchewan Information and Privacy Commissioner**  
***Report on Systemic Issues With Faxing Personal Health Information***  
**November 23, 2010**

---

A meaningful illustration that this may be a broader problem is the following comment from one of the RHAs not involved in this incident:

We have a notification received from [Clinic X], dated May 31, 2007 advising that office was moving and the fax / phone number would be changed effective July 1st 2007. This is less than 2 years ago. We changed and verified the fax number in our [database] to their new fax number on July 3, 2007. (first business day after July 1) ...

**This type of notification from a Physician Office is great to receive but is actually quite rare.** [emphasis added]

Also as an aside, I note that during our investigation which began in June 2009, of the 31 trustees, one pharmacy changed location, one physician's office changed names, and my office noted that another physician was using a prescription pad with outdated contact information.

- ***Use and Update Preprogrammed Fax Numbers***

Several trustees indicated that outdated preprogrammed numbers in their fax machines were to blame for these breaches. I suspect that this also played a role in the cases of those that did not identify any cause of the breach from their office as well.

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.

**Saskatchewan Information and Privacy Commissioner**  
**Report on Systemic Issues With Faxing Personal Health Information**  
**November 23, 2010**

---

Several trustees indicated within their investigation reports or correspondence with my office that the numbers within the electronic medical record (EMR) had not been updated. One physician's office reported:

Included in our electronic medical record was a database with numbers for referrals. This is what we used for the errant fax. We were never formally advised to check the database.

Although I have not inquired about the relationship between each trustee and its EMR provider, I must remind trustees that they are nevertheless responsible for personal health information within an EMR. EMR providers are defined as information management service provider (IMSP) pursuant to section 2(j) of HIPA as cited earlier in this Report.

Again, I have stated in Report H-2007-001 that even when a IMSP is acting on behalf of a trustee, the trustee is still responsible for safeguarding the personal health information.<sup>17</sup>

The *2009 Guidelines for the Protection of Health Information* set out by Canada's Health Information Association provides the following comment:

Technologies such as fax and e-mail have inherent security vulnerabilities. **These inherent weaknesses should be addressed in the context of the business environment, and the way in which they will be used.** Before a fax is used to transmit [personal health information] it should be ascertained that the recipient machine is secure and in a private area.<sup>18</sup> [emphasis added]

Outdated fax numbers is one of the inherent weaknesses that should have been addressed by the trustees with their IMSP.

Most of these 31 trustees have not put in place adequate policies and procedures for preventing errant faxes caused by outdated preprogrammed fax numbers.

- ***Adequate Training and Reminders***

None of the trustees have identified inadequate training and reminders of fax policies and procedures for staff as a cause of these breaches. However, as only three of the 31 (9.7%) trustees have demonstrated that they have adequate training regimes, I must conclude that this was a contributing factor with this breach. This reinforces my view that trustees in Saskatchewan in general need to provide more training to reinforce privacy best practices with their staff.

---

<sup>17</sup> OIPC Report H-2007-001 at [36]

<sup>18</sup> COACH 2009 Guidelines p.194

**Saskatchewan Information and Privacy Commissioner**  
**Report on Systemic Issues With Faxing Personal Health Information**  
**November 23, 2010**

---

Some of the trustees indicated that they do have policies and procedures addressing privacy training for staff that is separate from the fax policies. However, they did not provide copies to my office and therefore, were not awarded a point in this category.

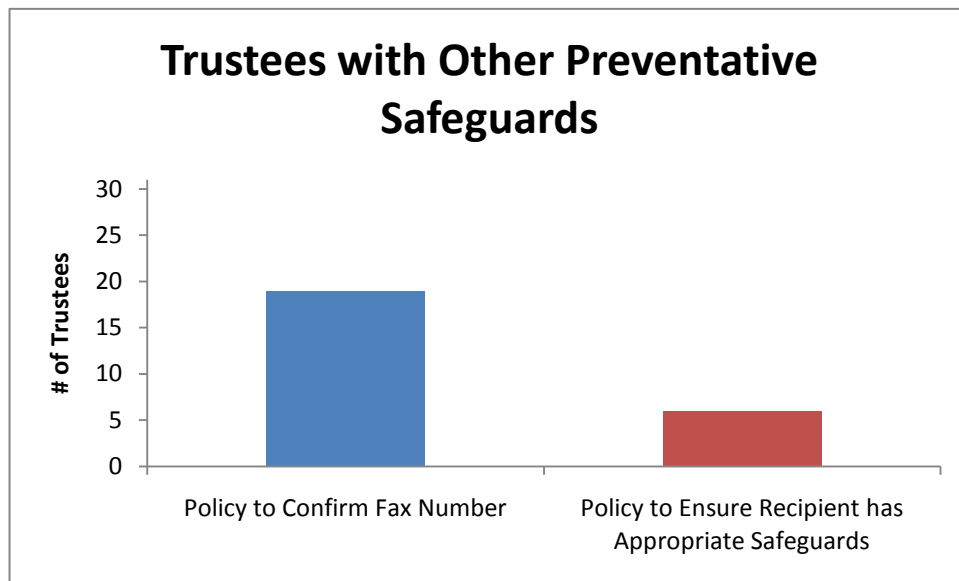
**C. Confirming recipient fax numbers and safeguards**

Two other best practices listed in my office's resource on faxing are:

1. To confirm the fax number by calling the recipient before sending the personal health information; and
2. To verify that the recipient has the appropriate fax safeguards in place.

These two steps could have also prevented the faxes from being sent in error to the third party business.

At present, 19 out of the 31 (61.3%) trustees now have policies or procedures in place directing their employees to confirm fax numbers with the recipient before sending personal health information. However, only 5 out of 31 (16.1%) trustees have policies or procedures in place to enquire about recipient safeguards.



When calling to verify a fax number, it would be a simple next step to also confirm that appropriate safeguards are in place on the receiver's end. I believe it would be simple for more trustees to adopt this best practise.

*i. Fax Cover Sheets*

24 out of the 31 (77.4%) trustees now have policies that instruct employees to use fax cover sheets with confidentiality notices. I note, however, that only 11 of the 60 errant faxes did have a fax cover sheet, not including the cover sheets that contained personal health information. Whether it has a cover sheet or not, once a fax is sent the trustee has lost control of the personal health information contained in the fax. This illustrates that fax cover sheets do not prevent privacy breaches. Cover sheets are simply one way to mitigate harm once a breach has occurred. They are also useful for directing the fax to the person with the appropriate need to know once the fax has reached the correct destination.

Of all the best practices listed in our *Faxing Considerations*, I note that all 31 trustees have chosen to focus on fax cover sheets. This best practice has been adopted by more trustees than any other of the best practises listed. None of the trustees have identified a cover sheet as being one of the factors in these breaches. And, I reiterate, cover sheets do not prevent breaches in the cases of misdirected faxes. I suspect that it was widely adopted because it is a simple measure for trustees to implement.

I applaud the trustees for adopting this measure; however, it is only a modest step in terms of addressing the risks inherent to faxing.

*ii. Designated person to send and receive faxes*

One of the best practises listed in our *Faxing Considerations* is that trustees designate one person in the organization to be responsible for sending faxes. The passage is as follows:

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.

Only four of the 31 (12.9%) trustees have adopted this best practice.

**Saskatchewan Information and Privacy Commissioner**  
***Report on Systemic Issues With Faxing Personal Health Information***  
**November 23, 2010**

---

Upon receiving my evaluations, several of the RHA's provided feedback to my office regarding this practice. They argue that this practice is unreasonable in large organizations and settings that operate 24 hours a day, 7 days a week. One RHA commented:

...the OIPC guideline dictates that "if possible" designate faxing responsibility to one staff member. This is not possible in all departments since all departments have relief staff for coverage, therefore, we feel this should be a bonus evaluation.

I have commented that "section 16 of HIPA does not require a standard of perfection but one of reasonableness."<sup>19</sup> Trustees should consider each best practice and adapt them to suit their individual organizations. I do, however, expect trustees to turn their minds to each best practice and consider how each one can be adapted to their organization in order to improve privacy protection. HIPA applies to thousands of trustee organizations that will vary greatly in size, resources and business issues. Just as HIPA compliance may involve some different features so must our tools and resources be modified as necessary to suit the particular type of trustee.

## **V. CONCLUSION**

Overall, I am underwhelmed by the response of the trustees to these privacy breaches. Most trustees have not adequately investigated the breach. More importantly, their current fax policies and procedures do not address the issues that caused these breaches, and therefore, are not likely to prevent a reoccurrence in the future.

I am aware that 21 of the 31 trustees only sent one misdirected fax each. In other words, 10 of the trustees were responsible for sending the other 39 faxes. Perhaps the majority of the trustees do not feel that one misdirected fax warrants a response that meets our identified expectations. However, the one fax misdirected by one trustee is part of a bigger more systematic breach of 60 errant faxes. Moreover, as I have illustrated above, misdirected faxes containing personal health information are a common occurrence, therefore predictable and preventable if appropriate measures are taken.

---

<sup>19</sup> OIPC Investigation Report H-2007-001 at [44] – [45] available online at [www.oipc.sk.ca](http://www.oipc.sk.ca)

**Saskatchewan Information and Privacy Commissioner**  
**Report on Systemic Issues With Faxing Personal Health Information**  
**November 23, 2010**

---

As noted above, I have commented on reasonableness in the context of section 16 policies and procedures in my Report H-2007-001.

[44] Section 16 of HIPA does not require a standard of perfection but one of reasonableness. In Investigation Report F06-02, a Portfolio Officer with British Columbia's Office of the Information and Privacy Commissioner applied the 'standard of reasonableness'. The relevant excerpts are reproduced as follows:

*[2] Public bodies in British Columbia are under a statutory duty to protect the personal information in their custody or under their control. Section 30 of FIPPA sets out the legal requirement:*

***Protection of personal information***

*30 A public body must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.*

...

*[31] 3.6 Analysis of Data Sensitivity and Protective Measures — Section 30 of FIPPA requires public bodies to take reasonable measures to protect information under their custody or control. In Investigation Report F06-01, Commissioner Loukidelis said this about s. 30:*

*[49] By imposing a reasonableness standard in s. 30, the Legislature intended the adequacy of personal information security to be measured on an objective basis, not according to subjective preferences or opinions. Reasonableness is not measured by doing one's personal best. **The reasonableness of security measures and their implementation is measured by whether they are objectively diligent and prudent in all of the circumstances. To acknowledge the obvious, "reasonable" does not mean perfect. Depending on the situation, however, what is "reasonable" may signify a very high level of rigour.***

*[50] The reasonableness standard in s. 30 is also not technically or operationally prescriptive. It does not specify particular technologies or procedures that must be used to protect personal information. The reasonableness standard recognizes that, because situations vary, the measures needed to protect personal information vary. It also accommodates technological changes and the challenges and solutions that they bring to bear on, and offer for, personal information security.*

*[32] **The reasonableness of security measures will depend on the sensitivity of the information.** As the Commissioner also noted in Investigation Report F06-01:*

*[52] The sensitivity of the personal information at stake is a commonly cited, and important, consideration. For example, a computer disk or paper file containing the names of a local government's employees who are scheduled to attend a conference or take upcoming vacation does not call for the same protective measures as a disk containing the medical files of those employees. [emphasis added]*

**Saskatchewan Information and Privacy Commissioner**  
***Report on Systemic Issues With Faxing Personal Health Information***  
**November 23, 2010**

---

[45] I am of the same view.<sup>20</sup>

Regardless of the quantity of personal health information that has been disclosed without authorization, it is the sensitivity of the information that matters most. It is my view that personal health information is highly sensitive and deserves a higher threshold of protection. I was only impressed with the response of one of the trustees, an RHA, which scored 34/38 or 89.5%. The other scores were unsatisfactory as the next highest score was a 23/38 or 60.5%.

Furthermore, I venture a guess that most trustees do not know how many misdirected faxes are actually sent from their offices. This is evident by the fact that very few of the 31 trustees had fax logging or tracking measures in place. Furthermore, shortly after my office sent notification about the change in Clinic X's fax number, a few trustee organizations contacted us to find out if they had sent one or more of the faxes in question. What we heard from some was not very encouraging. For instance, in one case, we were asked the following:

Is there any way that we can find out if any of the faxes were sent from our health region? Once patient information has been faxed, the information is filed in their Health Records chart. Unfortunately, without pulling charts, we have no way of knowing if we've sent information to the incorrect fax. I would greatly appreciate your assistance in this regard.

I am also concerned with the preoccupation of providers with convenience that has eclipsed the need to respect the privacy of patients. This is reinforced by numerous comments made by the trustees throughout my investigation. One RHA stated:

We would also like to add a comment about faxing in general within health care. Faxing within our organization is an operational necessity. We simply do not have the luxury of prohibiting the faxing of Personal Health Information (PHI) as this is not feasible in our setting. Patients/clients/residents rely on our ability to provide them with services that ensure safe, accurate and timely delivery of care. Faxing allows staff the ability to relay a request for lab tests, medications, consults, etc. In a timely fashion so that patients will receive the services they need.

Our health region is large both geographically and its numbers of employees. We function in an environment where the majority of our facilities/agencies/units operate on a 24/7, 365 days a year basis. This makes the statement that a policy should "require one person to be designated to send faxes" unrealistic or impossible, which is the reason we teach all employees about faxing. Also, given the high volume of faxes in our Region daily, it would be unmanageable to require that staff check for confirmation each and every time they send a fax.

---

<sup>20</sup> Ibid., at [44]–[45]

**Saskatchewan Information and Privacy Commissioner**  
***Report on Systemic Issues With Faxing Personal Health Information***  
**November 23, 2010**

---

There is no doubt we have misguided faxes, we can't and won't deny this fact. We do, however; address this issue very seriously and take actions, proactive and reactive, to mitigate these risks. We believe our commitment is evident since it was our Region who reported this fax breach to your office. Although we do not have a fax policy, we take steps to ensure each of the items outlined in your evaluation are talked about with staff and are followed.

Another trustee, a physician's office, stated:

In any physician's office, our first and foremost duties are dealing with our patients' health issues. Therefore; our time must be spent on phones, in-coming mail/faxes, appointments, booking tests, transcribing letters; and carrying out any and all duties that the physician requests of us during the work day. This leaves little or no time to implement written policies.

These are only two examples of discouraging comments I have received during my investigation. I note that neither of these trustees have written policies and yet insist that they are doing everything they can to ensure that patients' privacy is protected.

I will be sending a copy of this Report along with the final evaluations which will include identification of further areas that require attention to the heads of each of the trustee organizations in question.

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.

## **VII. RECOMMENDATIONS**

I recommend that all trustees establish or strengthen written policies and procedures dealing with faxing personal health information.

I recommend that all trustees, if they have not done so already, establish written policies and procedures to maintain administrative, technical and physical safeguards that will protect the personal health information in their custody or control.

I recommend the trustees look to their regulatory bodies and professional associations for support in establishing the above noted policies and procedures.

**R. Gary Dickson, Q.C.**  
**Saskatchewan Information and Privacy Commissioner**