Office of the Information and Privacy Commissioner for Nova Scotia

---

INVESTIGATION REPORT IR16-02

Nova Scotia Health Authority and Private Practice Physicians

Catherine Tully
Information and Privacy Commissioner for Nova Scotia
November 23, 2016

TABLE OF CONTENTS

Office of the Information and Privacy Commissioner for Nova Scotia
Report of the Commissioner (Review Officer)
Catherine Tully

INVESTIGATION REPORT

November 23, 2016

Nova Scotia Health Authority and Private Practice Physicians

Commissioner's Message

A key component of privacy is the autonomy individuals must have to decide to whom, when and how they discuss sensitive issues like mental illness. In this case, mental health information of three individuals was improperly faxed by health care providers to a Bedford business. Fortunately that business owner carefully protected the personal health information and willingly assisted this office in this investigation.

Errors in the faxing of personal health information have vexed health care systems for many years. Information and privacy commissioners across Canada have attempted to reduce these errors by conducting investigations into mis-sent faxes, making recommendations and issuing guidelines. But the errors continue. This investigation reveals that Nova Scotia is not immune to this problem. In fact, the majority of breaches reported to the Office of the Information and Privacy Commissioner by health custodians are either mis-sent faxes that are received at another custodian's office, or they are wrong names selected from a pick-list in an electronic communications tool.

In this case, a private business reported that it had been receiving faxes intended for a mental health clinic for years. We conducted an investigation into the three most recent fax errors – each by a different health care provider.

The results of this investigation are straightforward. Faxing requires careful attention to detail. The more sensitive the information, the more care is required. In this case it was momentary inattention – essentially human error by three different individuals that resulted in exactly the same error occurring. We conclude that the likelihood of this error occurring again is heightened by the fact that the two fax numbers of the two organizations are so similar.

The problem of mis-sent faxes will not go away. Whenever information is sent via email, by using a provider pick-list in a database or by faxing, the sender must take the time to ensure that the correct recipient has been selected. My expectation is that this report will prompt health custodians across Nova Scotia to revisit their faxing practices and ensure that the four best faxing practices outlined in this report become part of their everyday practice.

Catherine Tully
Information and Privacy Commissioner for Nova Scotia

Executive Summary

[1] In April 2016, CBC News reported that the owner of a Bedford business had been receiving mental health referral information on her fax machine. The referrals were intended to be sent to the Bedford-Sackville Mental Health Clinic (Clinic). The Clinic's fax number was one digit different from the business'. The business owner agreed to turn over to the Office of the Information and Privacy Commissioner (OIPC) the two referral forms that she had received most recently. One was from October 2015, the other from March 2016.

[2] At first our investigation followed the usual approach to privacy breach investigations. We confirmed that the breach was contained and we contacted the two sending physicians to discuss notification requirements and prevention strategies. As those investigations were wrapping up in June 2016, the business owner contacted us to report that she had received a third fax, again from a different physician.

[3] We followed the familiar privacy breach investigation approach with this physician as well. However, the evidence of a recurring pattern led us to consider whether the Clinic's ability to receive faxes was reasonably secure. Our investigation revealed that not only were the two numbers only off by one digit, but also that the only different digit was in the exchange for two adjacent communities, the different digits were side-by-side on the keypad, and both numbers reached fax machines.

[4] Our initial reaction was to suggest to the Nova Scotia Health Authority (NSHA) that the Clinic needed to change its fax number. The NSHA and its telecommunications provider noted several obstacles. The evidence provided satisfied us that changing the fax number was an incomplete solution to the problem while at the same time posing a significant risk to service delivery for patients of the Clinic.

[5] Instead, we focused on training to highlight the importance of good fax practices. The NSHA has provided the OIPC with the names and contact information for the 353 physicians who referred patients to the Clinic within the last year. OIPC staff will be contacting those physicians in the following weeks to reinforce the importance of caution when faxing sensitive personal health information.

[6] I make the following three recommendations:

Recommendation #1: NSHA to red flag the Clinic's fax number
[7] I recommend that the NSHA post a warning notice on the Clinic's website and revise the referral form to include the warning notice. The notice needs to identify that faxing to the Clinic includes a significant risk of a mis-dial. The NSHA has agreed to take this step.

Recommendation #2: NSHA to move away from faxed referrals
[8] As a longer-term solution, I recommend that the NSHA prioritize the development of an electronic referral system.

Recommendation #3: Physicians to implement reasonable security for faxing guidelines
[9] I recommend that the 353 physicians who have referred patients to the Clinic in the last year implement the four best faxing practices identified in this report.

1.0 Purpose and Scope

1.1 Background

[10] On April 1, 2016, a CBC News reporter contacted the OIPC[1] in the course of her research. The reporter told the OIPC that a business owner had been receiving mis-directed faxes containing mental health referral information for approximately 12 years.

[11] That day, an OIPC investigator called the business owner to discuss the breaches. The business owner explained that her fax number and the fax number at the Bedford-Sackville Community Mental Health Clinic were off by one digit. She reported that she had received between 9 and 15 faxes each year for between 13 and 15 years. The faxes were always a form intended for the Clinic.

[12] The business owner stated that over the years she had tried a variety of strategies to deal with the problem. She tried calling the sending physicians and the Capital District Health Authority (CDHA),[2] as it was then. When those calls didn't produce results, she would simply shred the records.

[13] The business owner said that the CDHA told her it would communicate with the physicians to have them program the correct fax number into their machines. The business owner said she was asked to contact a CDHA staff member whose primary responsibility and concern was making sure that the referrals ended up at the Clinic. It is unclear exactly when those discussions took place, or the results of them.

[14] Until the most recent breach, the business owner reported that she had shredded all the faxes she had received. She told the OIPC she had only recently begun keeping copies in order to demonstrate that she was, indeed, receiving these faxes on a regular basis.

[15] Following that conversation, the business owner agreed to turn over all the faxes in her possession to the OIPC. On April 5, 2016, the business owner provided OIPC staff with two mental health referral forms sent by two separate physicians, and intended for the Clinic. The first fax was dated October 1, 2015; the second was dated March 1, 2016. The business owner confirmed verbally that she kept no copies of the faxes, and later confirmed the same with each sending physician in writing.

[16] At the bottom of the October referral, contact for the health authority staff member responsible for patient safety has been hand-written after the fax was received.

[17] On June 14, 2016, the business owner contacted the OIPC to say she had received another fax that day. OIPC staff again attended the business and recovered the fax. The business owner confirmed in writing to the OIPC that she kept no copies of the fax.

---

[1] The Information and Privacy Commissioner for Nova Scotia is also known as the Review Officer and is appointed as the independent oversight authority under the *Freedom of Information and Protection of Privacy Act*, the *Municipal Government Act*, the *Personal Health Information Act* and the *Privacy Review Officer Act*.
[2] On April 1, 2015, the former CDHA was merged with eight other district health authorities to form the Nova Scotia Health Authority.

[18] In a phone conversation on July 22, 2016, the business owner reported that one of the business owner's staff knew the patient identified in the March fax. The business owner says it was this relationship that prompted her to begin looking for a more permanent solution to the issue. She confirmed that she has been receiving the faxes for between 13 and 15 years, though her memory is uncertain on when exactly the faxes started arriving. The business has been open for 19 years, and the faxes did not start immediately on opening the business, but soon after she opened.

[19] She confirmed that the pattern revealed of three breaches in the space of nine months was consistent with her experience dating back through the years. She says that she receives approximately 9 to 14 each year but with no real, discernable pattern. Sometimes, she has gotten two within a couple of weeks of each other; sometimes it can be months between breaches.

[20] On April 5, 2016, the OIPC contacted the Nova Scotia Health Authority to discuss the issue. The NSHA indicated it was aware of the issue and had been working through its Chief of Family Practice on developing a communications strategy. On April 5, 2016, the OIPC turned over copies of the first two faxes so that the NSHA could investigate.

[21] The Clinic is a facility of the NSHA, and as such the NSHA is responsible for the Clinic's compliance with the *Personal Health Information Act* (*PHIA)*.

1.2 Jurisdiction

[22] The Nova Scotia Health Authority is a custodian pursuant to *PHIA* s. 3(f)(iv).[3] Each of the private practice physicians is a custodian as well, pursuant to *PHIA* s. 3(f)(i).

[23] The Commissioner has a statutory mandate to monitor compliance of custodians with *PHIA* to ensure the purposes of the legislation are achieved. The purposes, as stated in s. 2 of *PHIA*, are "to govern the collection, use, disclosure, retention, disposal and destruction of personal health information in a manner that recognizes both the right of individuals to protect their personal health information and the need of custodians to collect, use and disclose personal health information to provide, support and manage health care."

[24] Pursuant to *PHIA* s. 92(2)(b), the Commissioner "may initiate an investigation of compliance if there are reasonable grounds to believe that a custodian has contravened or is about to contravene the privacy provisions and the subject-matter of the review relates to the contravention."

[25] We investigated the privacy practices of each of the physicians as they were brought to our attention. The facts gathered in those investigations provided the Commissioner with reasonable grounds to investigate one particular aspect of the NSHA's security practices.

[3] *PHIA* s. 3(f)(iv).

1.3 Investigative process

[26] Following the initial interviews with the CBC reporter and the business owner, OIPC investigators reviewed the mis-sent faxes and interviewed the three private practice physicians. The results of those interviews led us to believe that the NSHA's participation was required to solve the identified issues. On June 15, 2016, we contacted the NSHA to explain that we were investigating one aspect of the NSHA's security of personal health information. OIPC investigators met with NSHA officials and contacted the chief privacy officer of the telecommunications provider for the Clinic.

2.0 Issues

[27] The issues arising from this investigation are:

(1) Did each physician who sent a fax to the business have reasonable security in place within the meaning of ss. 61 and 62 of *PHIA*?
(2) (a) Do the reasonable security requirements at ss. 61 and 62 of *PHIA* apply to a custodian's collection of personal health information via fax?
(b) If so, is the NSHA's fax security at the Clinic reasonable in this case?

3.0 Analysis and Findings

3.1 What is reasonable security?

[28] Sections 61 and 62 of *PHIA* impose reasonable security obligations on all custodians:

> *61 A custodian shall protect the confidentiality of personal health information that is in its custody or under its control and the privacy of the individual who is the subject of that information.*
>
> *62 (1) A custodian shall implement, maintain and comply with information practices that*
> *(a) meet the requirements of this Act and the regulations;*
> *(b) are reasonable in the circumstances; and*
> *(c) ensure that personal health information in the custodian's custody or under its control is protected against*
> *(i) theft or loss of the information, and*
> *(ii) unauthorized access to or use, disclosure, copying or modification of the information.*
> *(2) A custodian shall implement, maintain and comply with a complaints policy for an individual to make a complaint under this Act.*

[29] With respect to the three physicians that mis-sent faxes, my initial finding is that there was no question that the personal health information was disclosed to a third party business and those disclosures were not authorized. In order to meet the objective of reasonable security, best

practices require that custodians give consideration to "four key steps" when a privacy breach occurs.[4]

1. Did they contain the breach?
2. Did they properly evaluate the risks associated with the breach?
3. Did they notify affected individuals?
4. Did they take steps to prevent future similar breaches?

3.2 Did each physician who sent a fax to the business have reasonable security in place within the meaning of ss. 61 and 62 of *PHIA*?

[30] As noted above, in order to determine if each physician had reasonable security in place we have evaluated their respective responses to the incidents in accordance with best practice articulated by the four key steps.

Description of the Incidents

[31] Our investigation revealed that each incident reflected the same fact pattern.

[32] A general practice physician saw a patient and determined that the patient's mental health care was best managed by the specialist team at Community Mental Health. The physician decided to refer the patient to the Clinic.

[33] To make the referral, the physician filled out the Community Mental Health referral form and sent it via fax. Fax is the Clinic's preferred method of receiving referrals. Instead of arriving at the Clinic, the referrals arrived at the Bedford business. The Clinic's fax number is (902) 865-xxxx. The business' fax number is (902) 835-xxxx. The last four digits are identical.

[34] Each form was filled out specific to one patient, and was filled out in a similar manner with slight but inconsequential differences.

[35] Each of the forms included complete contact information for the patient, including his or her health card number. The physician's working diagnosis or presenting concerns are described in one or two lines. These lines described the mental health condition the patient was seeking treatment for, as well as some of the challenges to everyday life the condition caused for the patient. The forms also described the patient's current medications, if any, as well as his or her current and past mental health treatment strategies.

[36] Each fax was sent by a separate physician. One physician confirmed to the OIPC that he had checked with both the business owner, his own records, and the Clinic to confirm that this was the first time his office had caused such a breach.

---

[4] This practice is articulated by the OIPC in our guidance document "Key Steps to Responding to Privacy Breaches," available on our website at www.foipop.ns.ca. It follows the same approach other jurisdictions use. See, for instance: the Office of the Privacy Commissioner of Canada, "Key Steps for Organizations in Responding to Privacy Breaches"; the Office of the Information and Privacy Commissioner for British Columbia, "Privacy Breaches: Tools and Resources"; the Office of the Information and Privacy Commissioner of Alberta, "Key Steps in Responding to Privacy Breaches"; and the Office of the Information and Privacy Commissioner of Ontario, "Privacy Breach Protocol: Guidelines for Government Organizations."

[37] The business owner confirmed that she had not recognized any pattern of repeat breaches from the same physician, but also admits she stopped reading them carefully. The business owner has turned over all records she has received since October, 2015 to the OIPC.

Step 1 – Containment

[38] Containment requires the custodian take immediate steps on learning of the breach to stop the breach, limit its spread and recover the breached information.

[39] Each of the individual breaches has been contained. OIPC staff have collected all three documents incorrectly faxed to the business. Physicians 1 and 2 agreed to confirm individually with the business owner that she turned over all personal health information to the OIPC.

[40] For breach 3, the business owner signed a form confirming that all personal health information has been turned over to the OIPC.

[41] For each individual breach then, the existing containment is functioning: a custodian faxed a referral form to the business, the business owner called the OIPC, the OIPC collected the referral form and received signed confirmation that all personal health information was turned over to our office for investigation.

[42] In most circumstances where a breach results from a mis-sent fax, this is an acceptable containment strategy. In this case, the long-term pattern of these breaches, and the probability that they will recur, requires a different approach, discussed below.

Step 2 – Evaluate the Risks

[43] Once the breach is contained, deciding the next steps to take requires an analysis of the risk posed by the breach. The following factors applied in each of the three breaches.

Personal Health Information Involved

[44] In each case, the breached information was a mental health referral form. Each physician filled out the form slightly differently, and not every space was completely filled in any of the forms.

[45] Physicians 1 and 3 filled out the same form; physician 2 used a slightly different form. The forms used by all three physicians disclosed the following personal health information.

[46] Individual's identifying information:

- Patient's full name
- Patient's address
- Patient's phone number (with space for home, work and cell numbers)
- Date of birth
- Gender
- Health card number and expiry date

[47] Health care provider information:[5]

- Physician's name, address and phone number
- Header information on the form identifying Capital Health – Community Mental Health as the intended recipient of the completed form.

[48] The form sent by physicians 1 and 3 included individuals' personal health information in response to the following diagnosis / treatment questions:

- Presenting concerns (please include level of distress and impact on their day to day life)
- What questions / issues would you like addressed at this time? (this question did not appear on the form used by physician 2)
- Medications (please include start date, dosage and response)
- Working diagnosis

[49] Neither physician 1 nor physician 3 entered any information in the space requesting "Current and past mental health treatments / services and community supports (attach reports if available)".

[50] The form sent by physician 2 included the following personal health information:

- Presenting concerns (please include level of distress and impact on their day to day life)
- Present medications (please include start date, dosage and response)
- Current mental health providers / community supports
- Services requested

[51] In short, each form contained detailed personal health information that identified the individual, described the presenting concerns and working diagnosis that led to the referral, and the treatment being sought. There is still a considerable stigma around mental health illness. Personal health information of this nature is highly sensitive.

Relationships

[52] Each individual breach was an accidental disclosure to a stranger: a private business owner with no established relationship with the individuals whose personal health information was breached. The business owner reported the breaches to the OIPC and turned over the records to our office.

[53] A private business owner who has no obligation under *PHIA* to protect privacy when receiving personal health information elevates the risk. When the business owner takes proactive steps to see that the personal health information is returned and the breach managed effectively, this helps moderate that risk.

[54] As far as we can determine, the risk rating for the "relationship" portion of this analysis has been low for all but one of the breaches.

[5] See *PHIA* s. 3(r)(ii).

[55] For the breach that occurred in March, 2016, the business owner reported that one of her staff members had an existing relationship with the individual whose personal health information was disclosed. The business owner did not characterize it as a close relationship, but it was enough of a relationship to encourage the business owner to start seeking a comprehensive solution.

[56] The business is a client-service operation, presumably owned and staffed by people who live in or near the Halifax Regional Municipality. The odds are that, if these breaches continue, the individual will one day be well known to the recipient. In other words, the business owner or one of her staff members will discover, through a mis-sent fax, that a client, friend, neighbour or family member is seeking treatment for a mental health issue, the specific diagnosis, and how that diagnosis is affecting the individual's day-to-day life.

[57] When that breach occurs, the risk for the relationship portion of this analysis will become very high. The reputational harm that would result in such an instance will be close to irreparable regardless of the business owner's actions in turning the personal health information over to the OIPC.

Cause and Extent of the Breach

[58] Our investigations established that each individual breach is an accidental disclosure. The referral forms are faxed to a number that is only one digit off from the correct number and received by a private business.

[59] In my view, human error is the primary cause of each of these breaches. The fax machine is convenient, effective, and it's not going anywhere in the health care sector in the short term. But mis-sending a fax is as easy as dialing a wrong number.

[60] There are strategies to make that human error less likely, as discussed below in the section on "prevention strategies."

[61] Our investigation revealed that the three physicians were aware of the risks in faxing personal health information, and that their offices were generally careful. The business owner reported that the faxes didn't routinely come from one physician, and one of the physicians told us he investigated internally to determine that this was the only breach of this type his office had committed.

[62] In each case the number was keyed in incorrectly by hand. In two of the three cases the breach resulted when the physician, who wouldn't normally send faxes, stepped in. The physicians were trying to be helpful and efficient, concerned about making sure their patients' referrals were sent off in a timely manner. But they indicated to us that they were unaware of the usual process. They didn't know if the fax machine had presets and they didn't know where to find cover sheets. They did indicate that they had never heard of a breach when the usual process was followed.

[63] Faxing best practices recommend designating a single authorized individual to handle all sending and receiving of faxes where practical. We recommended to the custodians that they follow these best practices. But policy and practices cannot cover off every aspect of potential

human behaviour. The fact that, in two cases, physicians acted outside the usual practices of the office is not, in my view, indicative of faulty practices.

[64] Moreover, the fax machine is not specialized equipment requiring significant training to use. Dialing a fax is as simple as reading the number off the form and keying it into the machine properly. Each physician made clear to us that he or she recognized the sensitivity of the personal health information breached, and was concerned to ensure the patient was notified of the breach and that the breach was contained.

[65] In addition to human error, four coincidental factors come together to increase the likelihood of that error happening, and of the probability that the error will recur with another custodian.

[66] Factor 1: The two fax numbers are virtually identical.

[67] The fax number at the Clinic is 902-865-xxxx.

[68] The fax number at the business is 902-835-xxxx.

[69] The last four digits are identical.

[70] Factor 2: The communities served by the exchanges 865 and 835 are side-by-side.

[71] The Canadian Numbering Administrator administers the distribution of phone number area codes and exchanges to Canadian telecommunications providers. Its website shows that 865 and 835 are each numbers assigned to Aliant Telecom, with 865 connecting the "Sackville" rate centre,[6] while 835 falls in the "Halifax" rate centre.[7]

[72] A Google search for "902-835" produces a list of businesses primarily in the Bedford area; Googling "902-865" creates a similar list of Sackville area businesses.

[73] The Clinic itself appears on the form as the "Bedford / Sackville" location, so is clearly intended to serve both communities.

[74] The close relationship of the exchanges with the communities was reflected back to us in our investigation, when one of the physicians responded that "It's always 835 when I'm calling Bedford."

[75] Communities in the Halifax Regional Municipality work hard to maintain their individual identities, and this is not to suggest that Bedford and Sackville are not unique. But many organizations, besides the Clinic, link Bedford and Sackville. The immediate results on a Google search for "Bedford-Sackville" include a physiotherapy clinic, a minor football

[6] A rate centre is essentially how billing purposes are managed in the regulatory scheme of telephone number administration: https://en.wikipedia.org/wiki/Rate_centre.
[7] A list of 902 area code exchanges can be found on the website of the Canadian Numbering Administrator, the organization that manages phone numbers for Canada: http://www.cnac.ca data/COCodeStatus_NPA902.htm.

association, a newspaper, a learning network and a trail all with "Bedford-Sackville" in their title.

[76] Factor 3: The only different numbers – three and six – are adjacent to one another on the phone keypad. Particularly given the familiarity with dialing either 835 or 865, it is physically easy to key in the wrong number.

[77] Factor 4: The similar numbers are both fax numbers.

[78] The fax machine is significantly less common than it once was. That two nearly identical numbers in two side-by-side communities would each end up connected to a fax machine, while one of them is intended to receive sensitive personal health information, is the final unfortunate twist in this story.

[79] Given that ordinary humans working in busy offices are expected to communicate with this risk, and the number of physicians potentially referring patients to the Clinic, more of these breaches are, in my view, inevitable unless other prevention strategies are implemented.

Scope of the Breach

[80] For each individual breach, one individual's personal health information was disclosed to a small business owner. The business owner turned the records over to the OIPC. In total, three people were affected by the three breaches.

[81] However, given the likelihood of future breaches, the scope of individuals at risk is, in effect, anyone being referred to the Clinic.

Foreseeable Harm from the Breach

[82] In my view, the main risk here is to the individual's reputation. In all three cases, the breached information is highly sensitive. A key component of privacy is the autonomy individuals must have to decide to whom, when, and how they discuss sensitive issues like mental illness. The potential for this breach to expand before it was contained posed significant reputational harm to the individual.

Step 3 – Notification

[83] At ss. 69-70, *PHIA* requires that an individual be notified of a breach where a custodian determines "on a reasonable basis" that the information has been breached and "there is potential for harm or embarrassment to the individual." If there is no potential for harm or embarrassment, the custodian may choose not to notify the individual, but must then notify the Commissioner.

[84] The pragmatic approach adopted by most other Canadian privacy commissioners is that there must be some value to the individual of receiving the notification. Notification should empower individuals to avoid or mitigate harm to themselves.

[85] In each of these cases it was clear that notification was required by *PHIA* s. 69. In all three cases, the physicians had either already notified their patients by the time we spoke with them or agreed to notify the patient following our recommendation to do so.

Step 4 – Prevention

[86] The final step in managing a breach is to develop strategies to prevent a future occurrence. Strategies should address both the immediate causes of the present breach and should improve the custodian's ability to detect and manage future breaches.

[87] Faxing is such a common and long-standing practice for sending personal information that tip sheets and policies are easily located on privacy commissioners' websites and the website of bodies overseen by commissioners.

[88] That guidance can be summarized as follows:[8]

- Faxing is not preferred and should be used only if necessary. Reasonable security measures to consider whether to receive a fax include the sensitivity of the personal health information, the number of documents, and the urgency of their transmittal.
- Because faxing may, by its nature, not be reasonably secure, policies set a very high standard around the actions needed to make it as secure as possible.
- Fax machines must be located in a closed area and monitored regularly.
- Fax recipients should arrange a time to receive faxes to ensure they collect them in person.
- A recipient waiting on a fax has an obligation to follow up if the fax is not received.
- Encryption, key locks and confidential mailboxes are all encouraged as means to securely receive faxes.
- Fax transmittal must ensure secure collection of personal health information.
- Fax numbers must be kept up to date, any changes to fax numbers thoroughly communicated to potential senders, and public information that includes the outdated fax number destroyed.
- In some cases, policies require recipients to set expectations on how senders should communicate faxed information to them. For instance, all transmissions of faxes must have cover sheets and confidentiality warnings.

[89] The Privacy Commissioner of Canada has released a number of reports of findings into faxing personal information. Those tended to result in recommendations that included policies to employees, using preset numbers, and recognizing that faxing may not be considered reasonably secure.[9] In at least one case, a fax number that was too similar to another fax number was taken out of service, which the Privacy Commissioner of Canada considered an effective prevention strategy.[10]

---

[8] See, for instance, Ontario OIPC, "Guidelines on facsimile transmission security"; Office of the Privacy Commissioner of Canada, "Fact Sheet: Faxing personal information"; BC OIPC, "Privacy and Security in the BC Health Care System Today"; Eastern Health (Newfoundland and Labrador), "Communicating Patient/Resident/Client Personal Information Via Facsimile"; Winnipeg Regional Health Authority policy "Transmission of personal health information via facsimile ("fax")".

[9] See, for instance, OPC *PIPEDA* Case Summary #2003-226; OPC *PIPEDA* Case Summary #2006-332; OPC Incident summary #1 "Misdirected faxes containing health information end up in apartment managers' hands."

[10] OPC Incident Summary #2: "CIBC's privacy practices failed in cases of misdirected faxes," and "Addendum to CIBC fax incident summary."

[90] I find that physicians 1, 2 and 3 did not have reasonable security in place because they:

- did not follow standardized procedures for faxing;
- did not use the fax machines' pre-sets;
- did not regularly review the machine's pre-sets;
- did not uniformly use cover sheets.

[91] We recommended the following prevention strategies to each of the physicians responsible for a breach.

1. Enter the Clinic's correct fax number into the fax machine's pre-sets and send a test fax to the Clinic.
2. Conduct biannual reviews to be sure the Clinic's fax number hasn't changed.
3. Use cover sheets when sending faxes.
4. Develop a systematic approach for sending faxes, document it and communicate it with all staff.

[92] All three physicians agreed to implement our recommendations.

[93] I find that each physician took reasonable steps in response to the privacy breaches. Each physician now has adequate security in place to address the future risk of mis-sent faxes.

3.3 Do the reasonable security requirements in ss. 61 and 62 of *PHIA* apply to a health custodian's collection of personal health information via fax?

What is reasonable security?

[94] Every privacy statute in Canada incorporates some version of a reasonable security requirement for the protection of personal information or personal health information.[11] As a result, reasonable security standards have been well-developed by other Canadian privacy commissioners.[12]

[95] These laws apply across a range of sectors – public, private and health care, but it is clear that the principles underpinning reasonable security stay the same.[13] The statutes considered

---

[11] Canada *Personal Information Protection and Electronic Documents Act*, s. 5(1); Newfoundland and Labrador *Personal Health Information Act* s. 13; Prince Edward Island *Health Information Act*, s. 36; New Brunswick *Personal Health Information Privacy and Access Act*, s. 50(1); Québec *Act respecting access to documents held by public bodies and the protection of personal information*, s. 63.1 and *Act respecting the protection of personal information in the private sector*, s. 10; Ontario *Personal Health Information Protection Act*, s. 10(1); Northwest Territories *Health Information Act*, s. 85(1); Manitoba *Personal Health Information Act*, s. 18(1); Saskatchewan *Health Information Protection Act*, s. 16; Alberta *Health Information Act*, s. 60; Yukon *Health Information Privacy and Management Act*, s. 19; British Columbia *Personal Information Protection Act*, s. 34 and *Freedom of Information and Protection of Privacy Act* s. 30.

[12] BC Order P06-04; Canada OPC and Alberta OIPC joint investigation "Report of an investigation into the security, collection and retention of personal information: TJX Companies Inc. / Winners Merchant International L.P."; Ontario Order MC09-9; BC Investigation Report F06-01; BC Investigation Report F12-02; Alberta Investigation Report H2005-IR-001; Alberta Investigation Report P2010-008; Alberta Investigation Rreport P2013-04; Ontario Order HO-001.

[13] BC Order P06-04.

include the federal *Personal Information Protection and Electronic Documents Act* (*PIPEDA*), Alberta *Personal Information Protection Act* (*PIPA*) and *Health Information Act* (*HIA*), British Columbia's *Freedom of Information and Protection of Privacy Act* (*FIPPA*) and *Personal Information Protection Act* (*PIPA*) and Ontario's *Personal Health Information Protection Act* (*PHIPA*), and *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*). Alberta's *PIPA*, BC's *PIPA* and Ontario's *PHIPA* have been declared "substantially similar" to *PIPEDA*, as has Nova Scotia's *PHIA*. It makes sense then, that the reasonable security standards in *PHIA* would echo those developed by other Canadian privacy commissioners.

Reasonable Security is Contextual

[96] Overwhelmingly, what is clear in the case law is that reasonable security is intended to be an objective standard measured against the circumstances of each case.

[97] The nature and amount of personal information, the form and format in which it is to be transmitted, stored and accessed are all factors to be evaluated in determining what security standards must be applied. Reasonable security requires that the custodian consider a suite of physical, organizational and technological safeguards.[14]

[98] This contextual analysis means that reasonable security can, in certain circumstances, require a very high level of rigor.[15]

Sensitivity

[99] The more sensitive the information, the higher the security standard required. This is stated expressly in the Schedule 1 to *PIPEDA*, which requires that personal information shall be protected by security safeguards appropriate to the sensitivity of the information.[16]

[100] Health information is generally sensitive, as are uniquely identifying numbers from government-issued identification. Context will matter: the use that can be made of the information affects its sensitivity.[17] *PHIA* is clear that it does not apply to personal health information fifty years after the death of the individual.[18] Personal health information of someone who has been deceased for 30 years would be less sensitive than that of a living individual.[19]

Risk to the Information

[101] Reasonable security must take into account the foreseeability of the breach and the harm that would result if the breach occurred. The higher the risk of a breach, the higher the security standard will be.[20]

---

[14] Canada OPC, Alberta OIPC, "TJX / Winners".
[15] BC Investigation Report F06-01, Alberta Order P2013-04.
[16] Section 4.7 of Schedule 1, incorporated as part of *PIPEDA* s. 5.
[17] Ontario Order MC09-9; BC Investigation Report F06-01; BC Investigation Report F12-02; Canada OPC, Alberta OIPC, "TJX / Winners"; Alberta Order P2013-04.
[18] *PHIA* s. 5(2)(b).
[19] BC Investigation Report F06-01.
[20] BC Investigation Report F06-01; Canada OPC, Alberta OIPC, "TJX / Winners"; Alberta Order P2013-04; Alberta Investigation Report H2005-IR-001.

[102] The custodian must then implement security measures that are reasonably responsive to those risks. The use that may be put to the information will affect the analysis of the required safeguards.[21] Reasonableness requires a proactive and speedy response to known or likely risks.[22] Time is of the essence in any privacy breach: the safeguards must ensure that should a privacy breach occur, the custodian and the individual will learn of the breach and have response measures in place quickly and efficiently.[23]

Public Trust

[103] For public sector bodies, reasonable security also includes reasonable assurances to the public that the government is taking privacy protections seriously. Where government holds personal information, the public has an increased level of trust that their personal information is being protected. This creates a high standard for government organizations to ensure security measures are in place.[24]

Standard Practice

[104] Industry standards and codes of practice can illuminate security requirements provided that following those practices reaches the contextual standards of reasonableness.

[105] If the industry standard is less than the contextual evidence demonstrates reasonable security requires, the industry standard is not sufficient. Simply accepting that a third party or contractor will follow industry standards does not demonstrate reasonable security.[25]

Costs

[106] The cost of implementing a new security measure may be a factor but it is on an extreme scale – reasonable security does not require a custodian to ensure against a minute risk at great cost. A custodian cannot dilute security by insisting on a cost efficiency in one area and refuse to pay for reasonable security in another.[26]

Security Through Information Life Cycle

[107] Reasonable security applies to the entire life cycle of the records.

[108] Where a custodian is receiving personal health information, it has an obligation to require secure transmission, and the transmission of health information requires reasonable security measures around the sending and receipt. For instance, data tapes sent by courier in a closed but unsealed container were found not to be reasonably secure.[27]

[21] BC Investigation Report F12-02.
[22] BC Investigation Report F06-01; Alberta Order P2013-04; BC Investigation Report F12-02.
[23] Alberta Order H2005-IR-001.
[24] BC Investigation Reports F06-01 and F12-02.
[25] Ontario Order MC09-9, BC Investigation Report F06-01.
[26] BC Investigation Report F06-01.
[27] Alberta Order H2005-IR-001.

[109] The custodian must maintain control over personal health information in its custody or control. Storing records in a shared space, for example, fails this requirement.[28] Failure to clearly establish custody and control of the records may result in failing reasonable security.[29]

Medium / Format

[110] The medium and format of the records will dictate the nature of the physical, technical and administrative safeguards. This is obvious at its most basic levels: paper needs to be in a locked file cabinet, while a portable electronic device must be encrypted. But a custodian is required to give consideration to additional layers as well. For instance, a portable storage device that was locked in a safe was not reasonably secure because the safe was able to be removed from the premises and the device was not encrypted.[30] The notion that paper is more secure because it is less easily disseminated than electronic information has fallen by the wayside as reasonable security has evolved in response to improvements in scanning technology.[31]

Documented Procedures

[111] Procedures for establishing reasonable security must be documented, and custodians must be prepared to respond to the idea that employees won't always follow the documented procedures.[32]

Receipt of faxes and reasonable security

[112] *PHIA* s. 61 sets out a custodian's obligations with respect to protection of personal health information as follows:

> *61 A custodian shall protect the confidentiality of personal health information that is in its custody or under its control and the privacy of the individual who is the subject of that information.*

[113] It is strictly true that, when the fax is sent and ends up in the wrong destination, the personal health information never enters under the custody or into the control of the custodian who is the intended recipient.

[114] But s. 61 is a two-part requirement. It also obligates a custodian to protect "the privacy of the individual who is the subject of that information."

[28] Ontario Order HO-001, BC Investigation Report F06-01.
[29] Alberta Order P2010-008.
[30] BC Investigation Report F12-02.
[31] BC Investigation Report F06-01.
[32] Alberta Order H2005-IR-001; Ontario Order HO-001; BC Investigation Report F06-01; Alberta Order P2010-008.

[115] In addition, *PHIA* s. 62 places additional obligations on the custodian as follows:

> *62 (1) A custodian shall implement, maintain and comply with information practices that*
> *(a) meet the requirements of this Act and the regulations;*
> *(b) are reasonable in the circumstances; and*
> *(c) ensure that personal health information in the custodian's custody or under its control is protected against*
> *(i) theft or loss of the information, and*
> *(ii) unauthorized access to or use, disclosure, copying or modification of the information.*

[116] "Information practices" are defined at *PHIA* s. 3(n):

> *(n) "information practices", in relation to a custodian or a prescribed entity, means the policies of the custodian or a prescribed entity for actions in relation to personal health information, including*
> *(i) when, **how** and the purposes for which the custodian routinely **collects**, uses, discloses, retains, de-identifies, destroys or disposes of personal health information, and*
> *(ii) the administrative, technical and physical safeguards and practices that the custodian maintains with respect to the information;*
> *[Emphasis added]*

[117] It is clear that information practices encompass the full life cycle of records management, which is generally considered to begin with effective planning on how the record is collected, received or captured.[33]

[118] "Collect" is defined at *PHIA* s. 3(c):

> *(c) "collect", in relation to personal health information, means to gather, acquire, receive, gain access to or obtain the information by any means from any source.*

[119] Collection of personal health information is, by the definition of "information practices," clearly an information practice for which the custodian must have practices in place that meet the requirements of the *Act*, that are reasonable in the circumstances, and that ensure personal health information in the custodian's custody or under its control is protected from the types of unauthorized handling enumerated at s. 62.

[120] Clearly then, information practices apply to how the custodian acquires and receives personal health information.

---

[33] Nova Scotia government, "Records Management Policy": https://novascotia.ca/treasuryboard/manuals/PDF/300/30401-01.pdf. See also Government of Canada, "Records and Information Life Cycle Management": http://www.bac-lac.gc.ca/eng/services/government-information-resources/lifecycle-management/Pages/life-cycle-management.aspx. Stage 2 is Collection, Creation, Receipt & Capture.

[121] Dictionary definitions of "acquire" provide the following:

- "to get as one's own; to come into possession or control of often by unspecified means"[34]
- "gain by and for oneself; obtain; come to possess"[35]

[122] For "receive," dictionaries offer:

- "to come into possession of"[36]
- "to acquire or accept (something offered or given); accept delivery of (something sent)

[123] The action of receiving or acquiring contemplates something not in possession or control of the receiver.

[124] The purpose of *PHIA* provides the following:

> *2 The purpose of this Act is to govern the collection, use, disclosure, retention, disposal and destruction of personal health information in a manner that recognizes both the right of individuals to protect their personal health information and the need of custodians to collect, use and disclose personal health information to provide, support and manage health care.*

[125] Information practices for the receipt or acquisition of personal health information that are reasonably secure in the circumstances achieve both ends. They respect individuals' privacy rights and they help to ensure that the right personal health information finds its way to the right place, for the right person, at the right time.

[126] In my view, s. 62(1)(a) and (b) obligate custodians to have reasonable security measures in place to come into custody or control of personal health information in a reasonably secure way. The greater specificity of s. 62(1)(c) adds clarification to the protections that must be applied to personal health information when it has come under the custody or control of the custodian.

[127] To read this otherwise, and apply reasonable security measures exclusively to personal health information in the custodian's custody or control, would be to say that *PHIA* imposes no obligation to securely collect personal health information.

[128] Taken to its extremes, this would mean that a fax machine could be situated in a public area and checked once a day. It could mean that the physician could leave the exam room door open and have us yell our symptoms across the hall.

[129] I find that reasonable security arrangement required by *PHIA* s. 61 and s. 62 apply to a health custodian's collection of personal health information via fax.

---

[34] Merriam-Webster Collegiate Dictionary.
[35] Canadian Oxford Dictionary.
[36] Merriam-Webster Collegiate Dictionary.

3.4 If so, was NSHA's security reasonable in this case?

Faxes to the Clinic

[130] Our investigation revealed that the NSHA's Clinic received approximately 1,200 faxed referrals in 2015. The NSHA provided the results of a one-week sample for 2016, which showed that the Clinic can expect to receive a similar number this year. There were 353 physicians who referred patients to the Clinic between April 1, 2015 and September 30, 2016. The NSHA explains that the majority of referrals come from private practice physicians, but referrals can come from other health care providers.

[131] The NSHA explained that communicating a change in the Clinic's fax number will be challenging because most physicians' offices will have printed off large numbers of the referral form for ease of use. The referral form has the Clinic's fax number printed on it. Those printed forms can be hard to completely remove from circulation, since it is unlikely that all 353 physicians' offices keep all of the forms stored in a central location like the reception desk.

[132] Faxing remains the Clinic's preferred method of receiving referrals and given the current realities of our health care system, that is not an approach that is going to change in the short term. Moreover, the NSHA described that there is some urgency to the referrals getting to the Clinic. Although it is not an emergency facility, the NSHA explained that there are circumstances in which the Clinic would choose to take urgent action to see a patient following a referral. Referrals will continue to be faxed for the foreseeable future.

[133] The NSHA indicated a potential longer-term solution existed in developing an electronic referral system. Such a system is not without potential privacy challenges that would need careful consideration before the system is introduced. However, an electronic referral system will only send information between credentialed users. This would eliminate the risk, inherent in sending sensitive personal health information by fax, that the recipient will be a private business or other person outside the statutory regime of *PHIA*.

[134] The business owner states that she has received around 9-15 mis-sent faxes each year for at least 10 years but not more than 19 years. The evidence established that the business owner has received 3 mis-sent faxes in the past 9 months, or, one every three months. By their nature, the pattern, frequency and occasions of privacy breaches will vary.

[135] At the low end, this means 0.3% of referrals to the Clinic have gone astray; at the high end, as many as 1.3% have. What's more, the evidence suggests that this rate of breach has been going on for an extended period of time. The evidence establishes that if the circumstances causing these breaches are left unchanged, it is reasonable to predict that the breaches will continue at the same rate. In other words, 4 to 15 Nova Scotians will have their sensitive mental health information faxed to the business in the next year.

[136] The business owner has tried a variety a strategies to stop the mental health referral forms from arriving on her fax machine. She has been in touch with the individual physicians, and with the former district health authority through their patient safety office. The NSHA says it attempted communications with sending physicians, but provided no further details on the scope of these efforts.

Systemic Evidence

[137] When custodians commit a breach of personal health information, they have an obligation to notify either the individual who is the subject of the personal health information, or the Commissioner. Notification to the Commissioner comes when the custodian determines that there is no potential for harm or embarrassment from the breach. Since *PHIA* went into force in June 2013, the Commissioner has received 940 notifications of privacy breaches with no potential for harm or embarrassment.[37] The majority of those breaches are either mis-sent faxes that are received at another custodian's office, or they are wrong names selected from a pick-list in an electronic communications tool.[38]

[138] Further, the no harm or embarrassment breach reports also give us a glimpse of the future. A technological referral system is necessary to solve this faxing problem. Still, the breach reports we have received reveal a common theme of personal health information being mis-sent because the sender selected the wrong recipient from a database drop-down list, or had an incorrect name auto-fill. When an unintended recipient is within the health care system, the disclosure is still unauthorized – it is still a breach. But, the four key steps analysis reveals a more robust containment strategy and the potential to offer more reassurance to the individual whose personal health information has been breached if the recipient is a custodian or agent under *PHIA*.

Contextual Factors

[139] In my view, the contextual factors around these breaches all point to a high standard of reasonable security and an obligation on the NSHA to take steps to prevent future breaches.

Mental Health and Social Relations

[140] The referral forms contain a detailed summary of a general practitioner's diagnosis of an individual's mental health condition. By its very nature, a referral to the Clinic means that an adult is "experiencing significant mental health problems or mental illness."[39]

[141] According to the Canadian Mental Health Association, 20% of Canadians "will personally experience a mental illness in their lifetime."[40] The NSHA indicates that referrals can come from anywhere in the province. Given the number of people potentially affected by mental illness, and the breadth of the pool of people potentially being referred, it is likely a matter of time before someone with a close relationship with the unintended recipient at the business is the individual whose personal health information is breached. This information is highly sensitive.

[142] The business owner provided evidence that the March 2016 breach involved an individual known to one of her staff members. A key factor in analyzing a privacy breach is the relationship between the individual whose personal health information has been breached and the recipient of

---

[37] Statistics current as of the end of fiscal year 2015-16.

[38] Of the 940 breaches reported to our office, 559, or 59%, resulted from personal health information being mis-sent through these communication methods.

[39] Nova Scotia Health Authority, http://www.cdha.nshealth.ca/mental-health-and-addictions/programs-and-services/mental-health/services-community/community-mental-health-services.

[40] Canadian Mental Health Association, "Fast facts about mental illness."

the breached information. Where the individuals have an existing relationship, the potential for harm or embarrassment is greatly increased.

NSHA's Leadership Position

[143] The NSHA is the largest health authority in the province. It employs more than 23,000 staff and more than 3,000 physicians.[41] Its vision, mission and values all point towards community involvement and respect for community members as the NSHA's central focus.[42] This puts the NSHA in a position of leadership with respect to legislated obligations like those found in *PHIA*.

[144] The reasonable security standard for the NSHA is higher than the local small practice physician. This is consistent with reasonable security standards across the country. That higher standard arises because the public that the NSHA serves expects it, and places a high degree of trust in government institutions that they will follow the letter and the spirit of laws like *PHIA*.

[145] Our investigation reveals a long-standing trend of physicians accidentally faxing mental health referral forms to the business. Our investigation reveals that the similarity in fax numbers, the fact that both faxes are located in adjacent communities, and that both numbers are fax numbers means that the probability of a repeat breach is extremely high.

Current Containment Strategy

[146] A containment strategy that ensures that the referral form finds its way to where it belongs is in place but does not and will not stop future breaches from occurring. The business owner has demonstrated a commitment to doing the right thing. She has made sure that personal health information is returned so that the breach can be properly investigated and managed. But in this, she is burdened by a responsibility that is not hers to bear.

[147] It is unreasonable to expect that the business owner voluntarily take on the permanent responsibility of being sure that personal health information is picked up, that the breach is effectively managed, and that the right information, for the right person, gets to the right place at the right time. The breach containment strategy as practiced is not a viable long-term solution.

[148] The specific circumstances that cause each of these individual faxes to be mis-sent when a custodian attempts to reach the NSHA's Clinic have now been brought to the NSHA's attention. In my view, reasonable security demands that the NSHA take a proactive response to help reduce the likelihood that custodians' efforts to contact the Clinic by fax will go awry.

[149] I find that the NSHA has an obligation to ensure that the manner in which it routinely collects personal health information has sufficient technical and physical safeguards in place to ensure that the personal health information is securely protected.

Prevention Strategies

[150] Based on the factors, we identified three possible prevention strategies.

---

[41] NSHA Fact Sheet.
[42] NSHA "Vision, mission and values".

[151] The first prevention strategy we suggested was to change the Clinic's fax number. Our initial response to this series of breaches was that the NSHA should change the Clinic's fax number. The NSHA identified several concerns with this approach. In the NSHA's view, such a change would adversely affect the service offered to mental health patients while at the same time creating the following risks:

- There was no way to guarantee the Clinic's new fax number would not end up one digit off from a different private fax number.
- Once the existing fax number was taken out of service, there was no way to ensure that it would not be reassigned as a fax number.
- Changing the fax number did not stop the primary issue, which is mis-dialing of the numbers by senders.

[152] Our initial observation was that these obstacles did not appear to be insurmountable. We reached out to the chief privacy officer of the Clinic's telecommunications provider. He provided a risk assessment that closely mirrored the NSHA's and was not able to offer effective solutions to the problems changing the fax number would create.

[153] In the end then, we decided that changing the fax number introduced too much uncertainty. It has the potential to create new and different privacy risks. At the same time, a change to the fax number creates a risk of disruption in service delivery. In the circumstances of this case, changing the fax number does not sufficiently solve the privacy problems to justify the risk of service disruption.

[154] Two strategies remain to prevent further breaches of this type. The first is a technological solution. A referral system run through an electronic tool that requires sender and recipient to have log in credentials would greatly reduce the risk that a private citizen or business could be the recipient of a mental health referral form. The NSHA indicated that such a system is in contemplation, among a number of other technological service priorities. As a longer-term solution, I recommend that the NSHA prioritize the development of an electronic referral system.

[155] The second prevention strategy is continued education. I recommended, and the NSHA agreed, to put a warning notice on the Clinic's contact points. The NSHA will update both the form itself and the website where the Clinic's fax number is posted to identify that faxing to the Clinic includes significant risk factors to a mis-dial.

[156] In this case, the OIPC will also play a role in the prevention strategy by communicating the results of this report directly to the 353 physicians who referred patients to the Clinic between April 1, 2015 and September 30, 2016. The NSHA has provided the OIPC with contact information for the 353 physicians.

[157] *PHIA* obligates all physicians, as custodians, to have reasonable security practices. To address the specific risks created by the similarity of the two fax numbers, I am recommending that the 353 physicians who have referred patients to the Clinic since April 1, 2015 implement the following four best faxing practices:

1. Develop a systematic approach for sending faxes, document it and communicate it with all staff. Normally, this will include identifying one person designated to send faxes.
2. Enter the Clinic's correct fax number into the fax machine's pre-sets and send a test fax to the Clinic.
3. Set a reminder to conduct biannual reviews to be sure the Clinic's fax number hasn't changed.
4. Use cover sheets when sending faxes.

4.0 Summary of Findings and Recommendations

[158] I find that physicians 1, 2 and 3 did not have reasonable security in place. The prevention strategies and responses to the breaches now implemented are, in my view, adequate to reduce the future risk of mis-sent faxes.

[159] I find that the NSHA has an obligation to ensure that the manner in which it routinely collects personal health information has sufficient technical and physical safeguards in place to ensure that the personal health information is securely protected.

Recommendation #1: NSHA to red flag the Clinic's fax number

[160] I recommend that the NSHA post a warning notice on the Clinic's website and revise the referral form to include the warning notice. The notice needs to identify that faxing to the Clinic includes a significant risk of a mis-dial. The NSHA has agreed to take this step.

Recommendation #2: NSHA to move away from faxed referrals

[161] As a longer-term solution, I recommend that the NSHA prioritize the development of an electronic referral system.

Recommendation #3: Physicians to implement reasonable security for faxing guidelines

[162] I recommend that, to address the risks identified in this report, the 353 physicians who have referred patients to the Clinic in the last year implement the following four best faxing practices:

1. Develop a systematic approach for sending faxes, document it and communicate it with all staff. Normally, this will include identifying one person designated to send faxes.
2. Enter the Clinic's correct fax number into the fax machine's pre-sets and send a test fax to the Clinic.
3. Set a reminder to conduct biannual reviews to be sure the Clinic's fax number hasn't changed.
4. Use cover sheets when sending faxes.

5.0 Conclusion

[163] Reasonable security depends on context. The critical contextual components in this case are the sensitivity of the personal health information and the likelihood, demonstrated by evidence and by years of experience that, a breach will recur. Without some change to the way referrals are sent to and received at this Clinic, sensitive mental health information will continue to be improperly faxed to the business.

[164] The business owner has demonstrated a commitment to doing the right thing, and we fairly expect she will continue to do so until an effective change is in place. But in this, she is burdened by a responsibility that is not hers to bear. Nor can her effective actions shield custodians from the fact that, by the nature of the information, each of these breaches poses a significant risk of harm or embarrassment to the individuals.

[165] Individuals seeking help for mental health issues place a significant amount of trust in their health care custodians to protect that information. When a custodian fails to actively guard this trust, it creates a negative impact that is outside the affected individuals' control. In order to get help for these important medical issues, individuals, out of necessity, surrender sensitive information to their health custodians. By implementing the recommendations in this report, physicians and the NSHA can demonstrate their willingness to protect that important public trust, and reassure individuals that their personal health information will be actively and vigorously protected.

6.0 Acknowledgements

[166] The three physicians who mis-sent faxes and the Nova Scotia Health Authority cooperated fully with this investigation. I am particularly grateful to the Bedford business owner for reporting these breaches and for protecting the personal health information improperly sent to her business.

[167] I would like to thank Robert Bay, Investigator for his work conducting this investigation and drafting this report.

November 23, 2016

Catherine Tully
Information and Privacy Commissioner for Nova Scotia