



## **INVESTIGATION REPORT** **126-2019, 137-2019, 182-2019, 191-2019**

### **Saskatchewan Health Authority**

**December 6, 2019**

**Summary:**

The Saskatchewan Health Authority (SHA) proactively reported a number of privacy breaches where the schedules of Continuing Care Aides (CCAs) containing patient personal health information were either stolen or lost. The Commissioner found that the SHA's prevention strategies are not sufficient or standardized, and it has not consistently prepared adequate investigation reports for every incident. The Commissioner recommended that the SHA determine appropriate safeguards to fulfill its duty to protect; implement consistent policies and procedures throughout the province; monitor the compliance of its CCAs with these policies and procedures in all offices across the province; and consistently follow best practices for writing breach investigation reports.

### **I BACKGROUND**

- [1] These four files involve printed home visit schedules of Continuing Care Aides (CCA) employed by the Saskatchewan Health Authority (SHA) containing patient personal health information that were lost or stolen in Saskatoon and Regina involving a total of 59 patients.
- [2] The information contained on the schedules involves patient name, address and telephone number, MRN, gender, appointment time, the health of the individual, and the care the patient requires. Of these schedules, one page was recovered. This page also contained information on how to gain access to the patient's residence. It is unknown whether the other schedules contained this same type of information.

- [3] Three of the incidents involve vehicles being broken into and the schedules stolen while the CCA was either at home or at a patient's address. The fourth incident involved one page of a schedule found in a parking lot.
- [4] The earliest of these incidents occurred on September 19, 2018, with the most recent occurring on June 10, 2019. Given that these types of incidents continue to occur even after interventions by the SHA and involve highly sensitive information of nearly 60 patients, our office has looked collectively at all incidents to determine if a systemic problem may exist that has yet to be fully addressed.
- [5] This assessment will also involve two separate privacy breaches that my office investigated in 2017 that involves two additional incidents where the CCAs lost the schedule of home visits containing the same type of information involving 21 patients. It should be noted that these two incidents occurred prior to the amalgamation of the regional health authorities into the SHA on December 4, 2017.
- [6] On August 1, 2019, my office notified the SHA that my office would be undertaking an investigation and requested the SHA respond to some questions concerning these matters. The SHA was provided with numerous opportunities to respond to my questions. As of the date of this Report, the SHA has refused to completely answer my questions, but rather, the SHA has provided a response indicating, "...we feel that 4 such incidents within a 12 month period is not a systemic issue". Therefore, I will regrettably conduct my investigation with a lack of complete information.

## **II DISCUSSION OF THE ISSUES**

- 1. Is *The Health Information Protection Act* (HIPA) engaged and do I have the authority to investigate this matter?**

[7] HIPA is engaged when three elements are present: 1) personal health information, 2) a trustee, 3) the trustee has custody or control over the personal health information. Below is an analysis to determine if these three elements are present.

***Personal health information***

**2** In this Act:

...

(m) “personal health information” means, with respect to an individual, whether living or deceased:

(i) information with respect to the physical or mental health of the individual;

(ii) information with respect to any health service provided to the individual;

...

(iv) information that is collected:

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

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

(v) registration information;

[8] The information contained within the schedules qualifies as personal health information as defined by subsection 2(m) of HIPA.

***Trustee***

[9] Subsection 2(t)(ii) of HIPA defines “trustee” as follows:

**2** In this Act:

...

(t) “trustee” means any of the following that have custody or control of personal health information:

...

(ii) the provincial health authority or a health care organization;

[10] Based on subsection 2(t)(ii) of HIPA, the SHA as the provincial health authority is therefore a trustee.

*Custody or control*

[11] Since the records involve patients receiving home care services from the SHA and the records are created and maintained by it, the SHA has custody and control of the personal health information in question.

[12] I find that HIPA is engaged and I have authority to investigate this matter.

**2. Was the duty to protect pursuant to section 16 of HIPA fulfilled?**

[13] Section 16 of HIPA imposes a duty upon trustees to protect information. Specifically, subsection 16(b) of HIPA provides that trustees must have reasonable safeguards to protect against the loss of personal health information. Subsection 16(b) of HIPA provides as follows:

**16** Subject to the regulations, a trustee that has custody or control of personal health information must establish policies and procedures to maintain administrative, technical and physical safeguards that will:

...

(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;

[14] Loss of personal health information can occur due to a number of causes, including human error, lack of knowledge and crime (such as theft) and can lead to its unauthorized disclosure; therefore, organizations should have policies, procedures and training in place to minimize the potential for such incidents to occur.

- [15] The SHA has implemented various methods, such as work standards, procedures and policies, to protect this type of information.
- [16] The SHA has provided my office with copies of work standards and policy and procedures relating to the management of the CCA's schedules. These are not consistent between the Regina and Saskatoon offices and the SHA has not provided information on what safeguards are in place in other areas of the province.
- [17] I am advised that the SHA's policy and procedure is to print each day's schedule and then shred it after each shift. One of the incidents involved 20 shifts while another involved one month of schedules.
- [18] In larger centres with a home care office, personal health information is to be printed for each shift and kept on their person at all times then shredded at the end of their shift. In rural locations with no office, any personal health information is to be kept on their person at all times and taken into the CCA's residence at the end of each shift, where it is to be kept securely until it can be shredded. However, in spite of this policy and procedure, a number of CCAs still left the schedules in their vehicles unattended and two of them had printed and were transporting 20 – 30 days of schedules.
- [19] It is important that public bodies consider potential discipline in instances where policies and procedures are not being followed. According to SHA's investigation reports, in each instance, the CCAs acknowledged that they each were familiar with the expectations of protecting the schedules. In that case, then, I would expect the SHA to take further remedial action to follow-up with each CCA to help ensure this does not happen again. Nothing was provided as to what consequences each faced, if any, for not following the policy.
- [20] The SHA's policies also indicate that, "Storage of client information/record overnight in a locked trunk of a vehicle is prohibited". They are to keep personal health information on them at all times and bring it back to the office, or in rural locations where it is not possible to bring it back, they are to take the information into their homes and ensure that it is

secured. The SHA also offers secure drop-off locations throughout Saskatoon, where the schedules can be shredded if it is more convenient than going back to the home care office.

[21] The SHA has various policies and procedures in place to limit the amount of schedules, which are printed, and how they are to be transported and disposed of. The Regina office indicated in October 2018 that it initiated a process whereby CCA's return of schedules are monitored. My office asked the SHA if this monitoring was consistent in other areas of the province. My office has not received a response, and therefore, is not aware of any monitoring practice occurring outside of the Regina office.

[22] As breaches continue to occur, I find that the SHA is not doing enough to ensure the protection of the schedules.

### **3. Has the SHA responded to the privacy breach appropriately?**

[23] My office suggests that the following five best practice steps be taken by a trustee organization when a privacy breach has occurred:

1. contain the breach;
2. notify affected individuals;
3. investigate the breach;
4. plan for prevention; and
5. write an investigation report.

[24] Below is an analysis of these five steps.

#### ***Contain the breach***

[25] Upon learning that a privacy breach has occurred, a trustee organization should immediately take steps to contain the breach. Depending on the nature of the breach, this can include stopping the unauthorized practice, recovering the records, shutting down the system that has been breached, revoking access privileges, or correcting weaknesses in physical security.

- [26] In the three incidents where either a binder or bag were stolen from vehicles, police were notified, but the schedules were never located.
- [27] In the instance where the schedule was found in a parking lot, it was couriered to my office. The SHA advised it is unaware of how long the schedule was missing.
- [28] I find that the SHA has made reasonable efforts to contain the breaches.

*Notify the affected individual*

- [29] Notifying affected individuals that their personal health information has been inappropriately disclosed is important for a number of reasons. Not only do individuals have a right to know, they need to know in order to protect themselves from any potential harm that may result from the inappropriate disclosure. Unless there is a compelling reason not to, trustees should always notify affected individuals.
- [30] The SHA sent letters to the affected individuals to notify them of the privacy breach. I find that the SHA has notified the affected individuals.

*Investigate the breach*

- [31] To investigate a privacy breach is to understand what happened that led to the privacy breach. As part of this investigation, the trustee organization should undertake a root cause analysis. Understanding the root causes will assist in the next step of managing a privacy breach, which is to implement a plan to prevent similar privacy breaches from occurring.
- [32] At the time of the breaches, the SHA had policies and procedures in place, which were to reduce the risk of this type of privacy breach from occurring. These policies and procedures provide that only the current days schedule is to be printed and that once printed, they are to remain with the CCA at all times. At the end of their shift, the CCAs are to shred their schedules. In each of the incidents, the SHA had determined that the CCAs were not following these policies and procedures.

[33] I find that the SHA investigated the breaches.

*Plan for prevention*

[34] Prevention is perhaps the most important step in responding to a privacy breach. While a privacy breach cannot be undone, a trustee organization can learn from and improve its practices. To avoid future breaches, a trustee organization should formulate a prevention plan. Some changes that are needed may have revealed themselves during the investigation phase; for example, deficient policies or procedures, a weakness in the system, a lack of accountability measures or a lack of training.

[35] Since the initial reported breaches in 2017, the SHA has presented the following areas where it has or would be enhancing the method of protection:

1. September 2017 – 293-2017 (Yorkton)

- In its submission, the SHA indicated it was working on implementing an application called Procura that might replace the clipboard/paper schedules that CCAs relied on. This application has not yet been implemented.

2. September 2018 – 191-2018 (Regina)

- The SHA updated the work assignments of the administrative/supervisory personnel to include specific requirements for verification of schedule returns at end of shift.
- Mandatory Privacy Refresh Video and Training will be rolled out in 2018/19 for all the employees of the Saskatchewan Health Transport.
- Protocol review is underway and will be strengthened for the security of the personal health information. Once determined, a complementary Work Standard will be written for employees.
- A new end of shift requirement to employee process has been implemented – Paper schedules are to be returned to office and placed in the Confidential Shredding Bin at the end of shift. Initial the attendance sheet once paper schedule has been placed in the bin. Supervisors will confirm all employees have initialed at the end of shift.

3. April 2019 – 126-2019 (Saskatoon)



- The SHA was not clear what actions were taken. Its submission indicated the privacy violation was a Level III and contained recommended actions for the individual which includes reviewing work standards and policies and procedures, repeat training, sign confidentiality agreement, warning of possible termination, discipline (doesn't state what type of discipline).

4. April 2019 – 137-2019 (Saskatoon)

- The SHA indicated the employee was to watch privacy video and take quiz as a refresher.

5. June 2019 – 182-2019 (Regina)

- The SHA indicated they would be updating their Secure Transport Work Standard.

[36] The SHA has indicated that it has currently provided privacy training to over 50% of its staff. I acknowledge the SHA aggressive efforts in this regard. I am hopeful that the SHA will continue to provide training to the other 50%.

[37] The SHA has indicated that it has strengthened and implemented new policies and procedures; however, it appears that staff are not consistently following these policies and procedures and therefore, these types of breaches have continued to occur.

[38] My office enquired whether the SHA is tracking the frequency of personal health information being returned to the office for shredding after each shift; however, the SHA did not provide my office with a response. It also appears that policies and procedures are not consistent throughout the province.

[39] The SHA has indicated that each of the CCAs involved in the breaches will receive training. It has not indicated what other consequences exist when CCAs do not follow policies or procedures, except in the one case above indicating a Level III violation occurred.

[40] What is also evidenced by the above responses is that some strategies were proposed, but not, to my knowledge, all implemented and there seems to be a disconnection with respect to what is the solution across the board.

[41] I find that the SHA's prevention strategies have not been sufficient to address the loss of CCA's schedules and that there is no apparent standardization across the province. I recommend that a standardized approach is developed and implemented across the SHA.

***Write an investigation report***

[42] Documenting a trustee organization's investigation into a privacy breach is a method to ensure that the trustee organization follows through with plans to prevent similar breaches in the future.

[43] My office has developed *Privacy Breach Guidelines for Government Institutions and Local Authorities*, which outlines the best practices for managing a breach and creating a report, as follows.

The report should include the following:

- A summary of the incident and immediate steps taken to contain the breach.
- Background of the incident. Timelines and a chronology of events.
- Description of the personal information involved and affected individuals.
- A description of the investigative process.
- The root and contributing causes of the incident.
- A review of applicable legislation, safeguards, policies and procedures.
- A summary of possible solutions and recommendations for preventing future breaches. This should include specific timelines and responsibility for implementation of each action.

[44] SHA provided my office with its internal reports or, in the Saskatoon instances, what appears to be an employee discipline report. These reports do not all include the elements, which my office identifies should be included in an investigation report.

[45] I find that the SHA has not prepared adequate investigation reports in all cases.

**III FINDINGS**

[46] I find that HIPA is engaged.

- [47] I find that in each incident, a privacy breach occurred.
- [48] I find that the SHA has not fulfilled its duty to protect these types of patient records.
- [49] I find that the SHA has made reasonable efforts to contain the breach.
- [50] I find that the SHA has notified the affected individuals.
- [51] I find that the SHA has investigated the privacy breach.
- [52] I find that the SHA's prevention strategies are not standardized and have not been sufficient.
- [53] I find that the SHA has not consistently prepared adequate investigation reports in all cases.

#### **IV RECOMMENDATIONS**

- [54] I recommend that the SHA determine appropriate safeguards to fulfill its duty to protect.
- [55] I recommend that the SHA implement consistent policies and procedures throughout the province.
- [56] I recommend that the SHA monitor the compliance of its CCAs with these policies and procedures in all offices across the province.
- [57] I recommend that the SHA consistently follow best practices for writing breach investigation reports.

Dated at Regina, in the Province of Saskatchewan, this 6th day of December, 2019.

Ronald J. Kruzeniski, Q.C.

Saskatchewan Information and Privacy  
Commissioner