Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 284-2017

Saskatchewan Health Authority
(formerly Sun Country Regional Health Authority)

April 30, 2018

Summary: The Saskatchewan Health Authority (the SHA) (formerly Sun Country Regional Health Authority) proactively reported a privacy breach where an employee accessed the personal health information of 880 individuals without a need to know. The Commissioner found that the SHA appropriately responded to the breach. He recommended that the SHA create a procedure where its privacy officer is alerted to potential breaches of privacy as soon as they are suspected. He also recommended that the employee be terminated and that the SHA forward its investigation file to the Ministry of Justice, Public Prosecutions Division to determine whether an offence has occurred and whether charges should be laid under *The Health Information Protection Act* (HIPA).

I BACKGROUND

[1] On November 8, 2017, Sun Country Regional Health Authority (Sun Country) proactively reported a privacy breach. An Employee in the Home Care department of Sun Country (the Employee) was suspected of snooping in an electronic database which contained personal health information of homecare patients, Procura. Suspicion was raised when the Employee knew more personal health information then what an individual in this position would have needed to know to complete duties of the position. Further, the Employee performed a duty that was not in the scope of the duties of the position.

[2] On November 9, 2017, my office notified Sun Country that I would be monitoring this matter.

[3] On December 4, 2017, Sun Country became part of the Saskatchewan Health Authority (SHA). As such, I will first discuss the breach under the legislation in effect at that time. I will then discuss how the SHA should proceed.

II DISCUSSION OF THE ISSUES

1. Does HIPA apply in these circumstances?

[4] *The Health Information Protection Act* (HIPA) applies in full when three elements are present. The first element is personal health information, the second element is a trustee, and the third element is if the personal health information is in the custody or control of the trustee.

[5] In its Investigation Report, Sun County indicated that the breach included unauthorized access of the personal health information of 880 homecare patients in Procura. It also noted that Procura contains the entire health care record of its homecare patients. This includes name, contact information, health services number, physician name, records of visits with physicians, consultation reports, investigation reports, diagnostic results, bills and correspondence.

[6] Personal health information is defined in subsection 2(m) of HIPA which provides:

> 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;

[7] Registration information is defined in subsection 2(q) of HIPA as follows:

> 2 In this Act:
> …
> (q) "registration information" means information about an individual that is collected for the purpose of registering the individual for the provision of health services, and includes the individual's health services number and any other number assigned to the individual as part of a system of unique identifying numbers that is prescribed in the regulations;

[8] The information that Sun Country indicated was accessed in Procura qualifies as personal health information pursuant to subsections 2(t) and (q) of HIPA.

[9] At the time of the privacy breach, subsection 2(t)(ii) of HIPA provided:

> 2(t)(ii) a regional health authority or a health care organization;

[10] Now, subsection 2(t) of HIPA defines a trustee. The relevant provisions are as follows:

> 2(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;
> …

[11] At the time of the breach, Sun Country qualified as a trustee pursuant to subsection 2(t)(ii) of HIPA.

[12] At the time of the breach, the personal health information was in the custody and under the control of Sun Country. HIPA applies to these matters.

2. Did Sun Country respond appropriately to this privacy breach?

[13] In circumstances where there is no dispute that a privacy breach has occurred, the focus for my office becomes one of determining whether the trustee has appropriately handled the privacy breach. In order to be satisfied, my office would need to be confident that Sun Country took the privacy breach seriously and appropriately addressed it. My office's resource, *IPC Guide to HIPA*, recommends five best practice steps be taken by a trustee when responding to privacy breaches. These are:

1. Contain the breach;
2. Notify affected individuals and/or appropriate organizations;
3. Investigate the breach;
4. Plan for prevention; and
5. Write a privacy breach report.

[14] I will use these steps to assess Sun Country's response to the breach.

Contain the Breach

[15] Upon learning that a privacy breach has occurred, trustees 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.

[16] Sun Country noticed that the Employee in question discharged a patient in the Procura system on April 4, 2017. This was not a function of the Employee's position at Sun Country. This raised suspicion regarding the Employee's activities in Procura. Throughout the months of April and May, the Home Care department investigated this matter. This initiated an extensive audit of all of the Employee's activities in Procura. Thousands of views, edits and deletes were evaluated.

[17] Sun Country's privacy officer was not notified of the breach until May 29, 2017. On May 31, 2017, Sun Country restricted the Employee's access in Procura.

[18] While restricting the Employee's access to personal health information in Procura and then terminating it altogether once a more thorough investigation took place is a right step, it should have occurred at an earlier date. Sun Country noted that there was no privacy officer in place during the beginning phases of the investigation.

[19] I note that on May 11, 2017, the Home Care manager addressed general topics related to the breach with the staff, such as not performing tasks outside of one's role and the implications that has on the protection of personal health information.

[20] The SHA will undoubtedly have a larger access and privacy unit than Sun Country did. I recommend that the SHA create a procedure where its privacy officer is alerted to potential breaches of privacy as soon as they are suspected.

Notify affected individuals and/or appropriate organizations

[21] Notifying an individual that their personal health information has been inappropriately accessed 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 access. Unless there is a compelling reason not to, trustees should always notify affected individuals.

[22] After an audit, Sun Country determined that the personal health information of 880 home care patients were affected by the breach since June 2010. At the time of the investigation, Sun Country also determined that 266 of the affected individuals were deceased. Sun Country provided notification to 614 affected individuals.

[23] It is also best practice to proactively report privacy breaches to my office so that my office may offer advice and monitoring of the trustee's response to the incident. Sun Country reported the incident to my office, eight months after the discovery of the breach. Again, I recommend that the SHA find ways to formally address breaches in a more timely manner.

Investigate the breach

[24] Once the breach has been contained and appropriate notification has occurred, the trustee should conduct an internal investigation. The investigation is generally conducted by the trustee's access and privacy unit because it has the appropriate privacy expertise to do so and understand what the relevant privacy legislation requires of the organization. The investigation should address the incident on a systemic basis and should include a root cause analysis. It should also consider whether the safeguards that were in place at the time of the incident were adequate. The investigation should be documented in an internal privacy breach investigation report. At the conclusion of its investigation, the trustee should have a solid grasp on what occurred.

[25] Sun Country interviewed the Employee in question. It also interviewed the home care manager at the time the breach was discovered as well as a previous manager. Sun Country also conducted an extensive audit of the Employee's activities in Procura.

[26] Through the audit, Sun Country was able to identify unauthorized accesses and the affected individuals.

[27] From this analysis, it was determined that the Employee had inappropriately accessed a excessive number of clients in Procura. The access included:

- co-workers,
- clients outside the designated area,
- a relative and
- clients for which there was no need-to-know.

[28] The audit also revealed that the Employee had continued to make inappropriate accesses after two initial meetings about the breach, which occurred on April 10, 2017 and May 11, 2017. The Employee's roles and responsibilities with respect to Procura were outlined at these meetings and need-to-know was discussed.

[29] In July and August 2017, Sun Country conducted the interviews.

[30] From its interview with the Employee, Sun Country obtained the following information:

- the Employee was often asked to look up information for other home care employees as they do not have access to Procura while in the field;
- the Employee received calls regarding clients in other home care areas from another area looking for more information,
- the Employee covered responsibilities of other staff when they were away or when the position was unfilled;
- the Employee was unaware that these would classify as privacy breaches;
- other home care employees may have accessed Procura after the Employee logged in under the Employee's username;
- the Employee indicated no accesses were motivated by curiosity.

[31] Sun Country reported that the Employee did not provide an explanation as to how other home care employees may have gotten access under the Employee's user name when the Employee reported the username and password was not shared.

[32] Sun Country also interviewed the Employees two most recent Managers. The Managers rejected the Employee's claim that the Employee was often asked to look up information for other home care employees who do not have access to Procura while in the field. The Managers said that the Employees are trained to call their supervisors for this information. The Managers also rejected claims that the Employee had received calls regarding clients in other home care areas from another area looking for more information. The Managers were of this opinion based on their experience.

[33] The Managers confirmed that before the Employee held the current position, the Employee did have to cover others duties that would have involved entering personal health information in Procura. However, this activity was identified in the audit and was not included in the 880 inappropriate accesses.

[34] Additionally, Sun Country's interviews with the managers resulted in the following information:

- the Employee was never directed to look at the minimum data set tab (MDS), diagnosis or to check Procura for completion or accuracy;
- there were numerous discussions with the Employee about staying within the job description;

- the Employee was told to stop looking at MDS and to stop questioning client care or actions of other employees;
- there was no reason for the Employee to discharge a client; and
- there was no reason for the Employee to access the records of clients from other home care areas.

[35] Sun Country provided my office with a copy of the Employee's job description. It does not appear that an individual in this role would be required to use the personal health information of individuals, other than registration information, to perform the duties in this role.

[36] Pursuant to section 16 of HIPA, trustees have a duty to protect personal health information. It provides:

> 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.

[37] Sun Country also looked into the safeguards it had in place at the time of the breach. Sun Country reported that the Employee had privacy training by Sun Country in 2008, prior to starting in the current position in 2010. It also reported that the Employee reviewed the training and re-signed a confidentiality agreement again in 2011. Finally, privacy was reviewed at a staff meeting in May 2017.

[38] Sun Country also noted that it had granted the Employee with more access privileges in Procura than was required for the position of the Employee.

[39] Sun Country identified the following root causes of the breach:

- Sun Country did not have the capacity to implement a proactive audit and monitoring program for Procura because the system did not have the ability to produce audit reports;
- the employee had access to more personal health information in Procura than was required by the job description;

[40] Sun Country concluded, however, that the main root cause was that the Employee intentionally breached privacy in spite of the privacy training that was received.

[41] I am satisfied with Sun Country's investigation of the breach.

Plan for prevention

[42] The next step is to formulate a plan to avoid future breaches of a similar nature. Some changes that are needed may have revealed themselves to the trustee during the investigation phase, such as deficient policies or procedures, a weakness in the system, a lack of accountability measures or a lack of training. This is an important step in addressing a privacy breach because a privacy breach cannot be undone but the trustee can learn from it and improve.

[43] In December 2017, *The Regional Health Services Act* was repealed and replaced with *The Provincial Health Authority Act*. The SHA now qualifies as a trustee pursuant to subsection 2(t)(ii) of HIPA as amended. The SHA is now responsible for prevention.

[44] The internal investigation report provided the following action items as its plan for prevention:

- Improve role-based permissions in Procura so that users are given access limited to what personal health information is required for their job function.

- Continue and improve staff education and training on privacy and confidentiality in Procura.
- Implement a "roles & responsibilities" or user agreement for Procura users which will display in the pop up message box that appears every time a user logs into the system. This has been implemented.
- Require all staff to review and sign the Privacy and Confidentiality Pledge annually.
- Develop a new and improved privacy oath which will be used to have home care employees sign.
- Implement auditing in Procura so that the SHA is able to perform audits on users and do not have to rely on eHealth for this. Develop auditing work standard. This has been achieved.

[45] I recommend that the SHA implement these preventative measures across the entire province.

[46] The employee no longer has access to Procura. A decision has not been made as to the long term future of the Employee in the SHA. Given the excessive number of affected individuals, I recommend the SHA terminate the Employee.

[47] I also recommend that the SHA forward its investigation file to the Ministry of Justice, Public Prosecutions Division to determine whether an offence has occurred and whether charges should be laid under HIPA.

Write a privacy breach report

[48] Sun Country has created a privacy breach report. It indicates that it will be updated once I have concluded my investigation.

III FINDINGS

[49] I find that HIPA applies in these circumstances.

[50] I find the Employee intentionally accessed personal health information for which there was no need-to-know.

[51] I find Sun Country responded appropriately to the breach.

IV RECOMMENDATIONS

[52] I recommend that the SHA create a procedure where its privacy officer is alerted to potential breaches of privacy as soon as they are suspected.

[53] I recommend that the SHA continue implementing the preventive measures that have been identified throughout the whole organization.

[54] I recommend that the SHA terminate the Employee.

[55] I also recommend that the SHA forward its investigation file to the Ministry of Justice, Public Prosecutions Division to determine whether an offence has occurred and whether charges should be laid under HIPA.

Dated at Regina, in the Province of Saskatchewan, this 30th day of April, 2018.

Ronald J. Kruzeniski, Q.C.
Saskatchewan Information and Privacy Commissioner