Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 103-2017

Sun Country Regional Health Authority

September 25, 2017

Summary: Records containing the personal health information of approximately 55 patients were stolen from the backseat of a locked vehicle. Sun Country Regional Health Authority (Sun Country) proactively reported this privacy breach to the Information and Privacy Commissioner (IPC). The IPC made a number of recommendations, including that Sun Country offer credit monitoring to affected individuals for a minimum of 5 years. He also recommended that Sun Country revise its draft policy and procedure so that records are not left unattended.

I BACKGROUND

[1] To prepare for a clinic the following day, an occupational therapist placed outpatient records into a locked box and stored the box in the backseat of a vehicle on May 10, 2017. She parked the vehicle at home. Overnight, the vehicle was broken into and the box was stolen. The following day, the occupational therapist discovered the box was missing.

[2] Sun Country Regional Health Authority (Sun Country) took steps to recover the patient records including searching through nearby garbage bins and reporting the matter to the Royal Canadian Mounted Police (RCMP).

[3] On May 19, 2017, Sun Country proactively reported a privacy breach to my office.

II DISCUSSION OF THE ISSUES

1. Is HIPA engaged?

[4] *The Health Information Protection Act* (HIPA) is engaged when three elements are present: 1) a trustee, 2) personal health information, and 3) the trustee must have custody or control over the personal health information.

[5] First, Sun Country qualifies as a trustee as defined by subsection 2(t) of HIPA.

[6] Second, the information contained within outpatient records would qualify as personal health information as defined by subsection 2(m) of HIPA:

> 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] Third, since the records belong to patients receiving therapy services from Sun Country, Sun Country has custody and control over the personal health information.

[8] I find that HIPA is engaged.

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

[9] My office recommends that trustees take the following five steps when responding to a privacy breach:

- Contain the breach,
- Notify affected individuals,
- Investigate the breach,
- Prevent future breaches, and
- Write a privacy breach report.

[10] I will consider each of these steps to determine if Sun Country adequately responded to the privacy breach.

Contain the breach

[11] The first step in responding to a privacy breach is containing the breach. This means to recover the personal health information or to stop the unauthorized practice when the trustee learns of the breach.

[12] As noted in the background, Sun Country made efforts to recover the personal health information by searching through nearby garbage bins and reporting the matter to the RCMP. Unfortunately, though, the personal health information was not recovered.

[13] I find that Sun Country has made reasonable efforts to contain the breach.

Notify affected individuals

[14] 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.

[15] In this case, Sun Country reported that there were approximately 55 affected individuals. Of the affected individuals, Sun Country was only able to identify 25 affected individuals. For these 25 individuals, Sun Country sent letters on July 24, 2017 to notify them of the privacy breach. To notify the remainder of the affected individuals, Sun

Country indicated it issued a media release to the Carlyle Observer and Kipling Citizen. I find that Sun Country has notified the affected individuals.

[16] Of note, Sun Country had worked with my office to create its notification letter and media release. As part of taking responsibility for a privacy breach, my office recommends that trustees or public bodies offer credit monitoring to protect affected individuals from identity theft or fraud. Therefore, when working with Sun Country, my office had recommended that Sun Country offer credit monitoring from a credit bureau to affected individuals for a minimum of 5 years. Sun Country did not accept the recommendation.

[17] My office's recommendation remains in that I recommend that Sun Country offers credit monitoring for a minimum of 5 years to the affected individuals.

[18] I also recommend to affected individuals that they seek credit protection services from a credit bureau. Depending on the service, there may be costs involved. I suggest they request that Sun Country pay these costs. If Sun Country refuses to pay for the service, then I suggest they seek legal advice on how to file a class-action lawsuit under the law *The Privacy Act*.

Investigation

[19] The next step in responding to a privacy breach is to investigate what caused the breach. Determining the cause and/or contributing factors will help the trustee prevent future breaches.

[20] At the time of the privacy breach, Sun Country had a policy regarding the access and security of personal health information (policy # IM-05-05-00). This policy applied to all patient records and had two specific instructions regarding the removal of patient records offsite and transporting them:

- Original health records are not to be removed from the facility except by order of subpoena, summons, or appropriate search warrant. Other exceptions include

> Long Term Care resident interfacility transfers and Community Services records that are utilized for continuing client care.
> …
> - Health information that is being transported or transmitted by any means is to be protected from viewing by unauthorized personnel, i.e. in a sealed envelope or tote. All health information being transported by vehicle is to be placed in the trunk.

[21] In this case, as noted in the background, the records were locked in a box and placed in the backseat of a locked vehicle. The policy was not followed.

Prevent future breaches

[22] In response to this privacy breach, Sun Country developed a draft policy and procedure for transporting records specifically for its Department of Therapies. Instructions within the draft policy and procedure are as follows:

1) One should question themselves if taking this information out of the office is necessary.

2) Record the patient's name and HSN on the sign out sheet prior to taking any health record out of the office.

3) Health records should be taken directly from one office to another office and carried by the person in a brief case.

4) Once the individual carrying the health record is in the office or where the information is being transported, the file should be locked in a filing cabinet.

5) If on route and the worker will not be back in the office, health records should be locked in the trunk of the car.

6) Personal health records should not be taken into a restaurant or any other public place.

7) Only health records that will be used within the week and are required to provide personal care to the person should be moved out of the office.

8) Document return of the record on the sign out sheet when the record is returned to the office.

[23] I find that most of the above is appropriate. In the course of my office's investigation, my office recommended that Sun Country revise the fifth instruction. Records should be

locked in the car trunk. However, unless there is no alternative, records should never be left unattended in a car trunk while the employee is elsewhere. Also, instructions should be added so that when an employee is working outside the office, records should be kept under the constant control of the employee including meals and other breaks. If this is not possible, the records should be temporarily stored in a secure location such as a locked room or desk drawer. Sun Country has indicated that it will revise its policy pursuant to my office's recommendation.

IV FINDINGS

[24] I find that HIPA is engaged.

[25] I find that Sun Country has made reasonable efforts to contain the breach.

[26] I find that Sun Country has notified the affected individuals.

[27] I find that Sun Country has investigated the privacy breach.

[28] I find that Sun Country's draft policy and procedure for transporting records is mostly appropriate.

V RECOMMENDATIONS

[29] I recommend that Sun Country offers credit monitoring for a minimum of 5 years to the affected individuals.

[30] I recommend that Sun Country follow through with its commitment to revise its draft policy and procedure to say that records should be locked in the car trunk. However, unless there is no alternative, records should never be left unattended in a car trunk while the employee is elsewhere. A copy of the revised policy and procedure should be provided to my office within 30 days of receiving this final report.

[31] I recommend that Sun Country follow through with its commitment to revise its draft policy and procedure to say that when an employee is working outside the office, records should be kept under the constant control of the employee including meals and other breaks. If this is not possible, the records should be temporarily stored in a secure location such as a locked room or desk drawer. A copy of the revised policy and procedure should be provided to my office within 30 days of receiving this final report.

[32] I recommend to affected individuals that they seek credit protection services from a credit bureau. Depending on the service, there may be costs involved. I suggest they request that Sun Country pay these costs. If Sun Country refuses to pay for the service, then I suggest they seek legal advice on launching a class-action lawsuit under the law *The Privacy Act*.

Dated at Regina, in the Province of Saskatchewan, this 25th day of September, 2017.

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