Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 136-2017

Prince Albert Parkland Regional Health Authority

August 31, 2017

Summary: Through an audit and an investigation, Prince Albert Parkland Regional Health Authority (Parkland) detected that an employee snooped into the patient records of 14 individuals, including several family members and her own patient record. The Information and Privacy Commissioner (IPC) agreed with Parkland's finding that the root cause of the privacy breach was the employee intentionally breaching privacy. He also found that Parkland has taken appropriate steps to prevent similar privacy breaches in the future. The IPC made a couple of recommendations, including Parkland 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 June 29, 2017, the Prince Albert Parkland Regional Health Authority (Parkland) proactively reported a case of employee snooping to my office. It provided my office with its internal investigation report and other related documents such as a copy of the notification letter sent to affected individuals, and copies of relevant policies and procedures.

[2] Parkland conducts audits using the Electronic Provincial Privacy and Monitoring program (ePPAM), which produces a report called "Same Last Name Look Up". On June 14, 2017, as it was conducting an audit using ePPAM, Parkland discovered that an employee had accessed records of several family members.

[3] Parkland investigated further and determined the employee had accessed the personal health information of 14 patients and her own personal health information. Parkland established that the employee had personal relationships with 13 of the 14 patients.

II DISCUSSION OF THE ISSUES

1. Does *The Health Information Protection Act* (HIPA) apply?

[4] HIPA is engaged when three elements are present: 1) personal health information, 2) a trustee, and 3) the personal health information is in the custody or control of the trustee.

[5] First, personal health information is defined by 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;
>
> (iii) information with respect to the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of 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;

[6] Subsection 2(q) of HIPA defines registration information as follows:

> 2(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;

[7] WinCIS is a patient registration system that includes information about admissions, discharges, and transfers. I find that personal health information is present.

[8] Second, trustee is defined by subsection 2(t) of HIPA, which provides:

> 2 In this Act:
>
> ...
>
> (t) "trustee" means any of the following that have custody or control of personal health information:
>
> ...
>
> (ii) a regional health authority or a health care organization;

[9] Since Parkland is a regional health authority as defined by subsections 2(1)(p) of *The Regional Health Services Act*, I find that Parkland qualifies as a trustee pursuant to subsection 2(t)(ii) of HIPA.

[10] WinCIS is a system used by Parkland to admit, discharge and/or transfer its patients. Therefore, I find that Parkland has custody or control over the personal health information.

[11] I find that HIPA is engaged.

2. Was there an unauthorized use of personal health information?

[12] The term "use" is defined by subsection 2(u) of HIPA, which provides:

> 2 In this Act:
>
> ...
>
> (u) "use" includes reference to or manipulation of personal health information by the trustee that has custody or control of the information, but does not include disclosure to another person or trustee.

[13] Sections 23 and 26 provide how trustees are to use personal health information:

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

> ...
>
> 26(1) A trustee shall not use personal health information in the custody or control of the trustee except with the consent of the subject individual or in accordance with this section.
>
> (2) A trustee may use personal health information:
> (a) for a purpose for which the information may be disclosed by the trustee pursuant to section 27, 28 or 29;
> (b) for the purposes of de-identifying the personal health information;
> (c) for a purpose that will primarily benefit the subject individual; or
> (d) for a prescribed purpose.

[14] Parkland reported that the employee looked up records about herself, family members, and friends out of curiosity. I find that HIPA does not authorize using personal health information to satisfy one's curiosity.

3. Did Parkland respond to the privacy breach appropriately?

[15] My office suggests that trustees undertake the following five steps when responding to a privacy breach:

- Contain the privacy breach
- Notify affected individuals
- Investigate the privacy breach
- Prevent future privacy breaches
- Write an investigation report.

[16] Below is an analysis of each step to determine if Parkland has adequately responded to the privacy breach:

i. Contain the privacy breach

[17] To contain the breach is to ensure that personal health information is no longer at risk. This may include recovering the records, revoking access to personal health information, and stopping the unauthorized practice.

[18] In its internal investigation report, Parkland indicated that prior to this privacy breach, the employee had been found to have snooped on two patients on the Pharmaceutical Information Program (PIP) in May 2017. The employee's director and manager had reviewed privacy expectations with the employee, and then the employee had been suspended for five days.

[19] On June 14, 2017, Parkland discovered that the employee began snooping into personal health information in WinCIS soon after she returned from her suspension. The employee has now been terminated.

[20] I find that Parkland has contained the breach.

ii. Notifying the affected individual

[21] Notifying affected individuals of the privacy breach as soon as possible is important so individuals can determine how they have been impacted and take steps to protect themselves. Notifications should include the following:

- A description of what happened,
- A detailed description of the personal health information that was involved,
- A description of possible types of harm that may come to them as a result of the privacy breach,
- Steps that the individuals can take to mitigate harm,
- Steps the trustee is taking to prevent similar privacy breaches in the future,
- The contact information of an individual within the trustee organization who can answer questions and provide further information,
- A notice that individuals have a right to complain to the Office of the Information and Privacy Commissioner (OIPC),
- Recognition of the impacts of the breach on affected individuals and an apology.

[22] Parkland sent notification letters to the 14 affected individuals on June 28, 2017. The notification letter contained a description of what happened, how Parkland discovered the breach, the type of personal health information that was involved, an apology, the contact information of Parkland's Privacy & Freedom of Information Officer, and the contact information of my office.

[23] While Parkland's notification letter contained appropriate elements, it did not identify the employee who had snooped upon the affected individual. The letter described the employee as an employee who was not involved in the patient's medical care. The identity of the employee is important information for the affected individual to determine the harm or consequences that may come to them as a result of the privacy breach. For example, if the snooper was someone with whom the affected individual had an acrimonious relationship, the affected individual may need to take additional steps to protect him or herself.

[24] Further, Parkland's notification letter did not indicate how Parkland will prevent similar privacy breaches in the future, including that the employee has been terminated.

[25] There may be hesitation to disclose the employee's identity and termination to the affected individuals because that information may qualify as personal information under *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP). However, I note that Parkland is also a local authority as defined by subsection 2(f)(xiii) of LA FOIP. Subsection 28(2)(s) of LA FOIP and subsection 10(g) of the LA FOIP Regulations enables the head of a local authority to exercise his or her discretion when determining whether or not to disclose the personal information of an employee. Subsection 28(2)(s) of LA FOIP and subsection 10(g) of the LA FOIP Regulations provide as follows:

> 28(2) Subject to any other Act or regulation, personal information in the possession or under the control of a local authority may be disclosed:
>
> ...
>
> (s) as prescribed in the regulations.

> 10 For the purposes of clause 28(2)(s) of the Act, personal information may be disclosed:
>
> ...
>
> (g) to any person where the information pertains to:
>
> (i) the performance of any function or duty or the carrying out of any responsibility by an officer or employee of a local authority; or

> (ii) the terms or circumstances under which a person ceased to be an employee of a local authority, including the terms of any settlement or award resulting from the termination of employment;

[26] I find that Parkland's notification letter contains many appropriate elements but is missing a couple of key elements. I recommend that the head of Parkland disclose to the affected individuals the employee's identity and the fact that the employee has now been terminated to prevent a similar privacy breach in the future.

iii. Investigate the privacy breach

[27] Investigating the privacy breach to identify the root cause is key to understanding what happened and to prevent similar breaches in the future.

[28] Parkland's investigation report identifies the root cause of this privacy breach as the employee intentionally breached privacy in spite of the following:

- Receiving 30-minute privacy education session at employee orientation,
- The employee had last signed a confidentiality agreement on August 8, 2016 that explicitly states the following:
  - I will only view, use or disclose confidential information which I have a legitimate need-to-know;
  - I will not view or use databases to access my own personal health information at PAPHR
- Employees are required to sign confidentiality agreements on an annual basis,
- The employee had already been caught snooping in PIP in May 2017 which resulted in:
  - Her director and manager reviewing privacy expectations with her during her discipline meeting, and
  - A 5-day suspension

[29] Based on the above, I agree with Parkland's finding that the root cause was the employee intentionally breaching privacy.

iv. Prevent future breaches

[30] Preventing future breaches means to implement measures to prevent future breaches from occurring.

[31] First, Parkland has terminated this employee. The employee had proven that a 5-day suspension was not enough to give her pause as she had immediately began snooping as soon as she returned from her suspension.

[32] Second, Parkland conducts regular audits of its electronic systems to detect snooping. I applaud Parkland's diligence in its auditing to have detected this employee's snooping in PIP and WinCIS.

[33] Third, Parkland will continue to provide privacy education and privacy awareness.

[34] I find the above to be all reasonable measures by Parkland to prevent similar privacy breaches in the future.

v. Write an investigation report

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

[36] Parkland provided my office with its internal investigation report that described the privacy breach, how it detected the privacy breach, background and history, root cause of the privacy breach, and steps it is taking to prevent similar privacy breaches in the future. I find Parkland has documented this privacy breach and its investigation very well.

III FINDINGS

[37] I find that HIPA is engaged.

[38] I find that HIPA does not authorize using personal health information to satisfy one's curiosity.

[39] I find that Parkland has contained the breach.

[40] I find that Parkland's notification letter contains many appropriate elements but is missing a couple of key elements.

[41] I agree with Parkland's finding that the root cause was the employee intentionally breaching privacy.

[42] I find that Parkland has taken appropriate steps to prevent similar privacy breaches in the future.

[43] I find Parkland has documented this privacy breach and its investigation very well.

IV RECOMMENDATIONS

[44] I recommend that the head of Parkland disclose to the affected individuals the employee's identity and the fact that the employee has now been terminated.

[45] I recommend that Parkland 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 31st day of August, 2017.

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