Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 142-2015

Heartland Regional Health Authority

December 14, 2015

Summary: The Heartland Regional Health Authority (HRHA) proactively reported a case of employee snooping to my office. HRHA advised that an employee had inappropriately accessed personal health information of 901 individuals. The Commissioner found that HRHA had appropriately investigated and responded to the privacy breach. The Commissioner recommended that HRHA forward its investigation file to the Ministry of Justice, Public Prosecutions Division.

I BACKGROUND

[1] On July 21, 2015, Heartland Regional Health Authority (HRHA) contacted my office to proactively report a potential case of employee snooping. HRHA indicated that it believed the privacy breach involved the inappropriate access of more than 100 individuals' personal health information in an electronic health record (EHR) system called *med access*. HRHA advised that they would be conducting a full investigation into the matter and would provide my office with a copy of its investigation report.

[2] On August 5, 2015, HRHA contacted my office and advised they were still conducting their investigation, but that it now appeared there were 885 patients that had been affected by this breach of privacy. HRHA provided my office with an interim internal investigation report and advised that the full investigation report would be provided once complete.

[3] On September 21, 2015, HRHA provided my office with its full investigation report. In that report, it was found that a total of 1,869 inappropriate accesses of 901 patients' personal health information by one HRHA employee.

II DISCUSSION OF THE ISSUES

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

[4] HIPA applies 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] HRHA stated in their investigation report that the EHR system contained the following information:

- demographics (name, address, telephone, age, sex, Health Services Number)
- patient and physician or RN/NP visit information
- consultation reports
- investigation reports
- diagnostic results
- patient letters
- other correspondence regarding the patient

[6] I find that the EHR system contains information that would qualify as personal health information pursuant to subsection 2(m) of HIPA. HRHA qualifies as a trustee pursuant to subsection 2(t)(ii) of HIPA. Finally, HRHA had custody or control over the personal health information in the EHR system.

[7] I find that HIPA applies.

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

[8] Use is defined at subsection 2(u) of HIPA:

> **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 disclose to another person or trustee.

[9] Section 26 of HIPA provides as follows:

> **26** 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 the purpose that will primarily benefit the subject individual; or
>
> (d) for a prescribed purpose.
>
> (3) Nothing in subsection (2) authorizes a trustee as an employer to use or obtain access to the personal health information of an individual who is an employee or prospective employee for any purpose related to the employment of the individual without the individual's consent.

[10] HRHA reported that the employee had inappropriately accessed personal health information without authority under HIPA and therefore would not be considered an authorized use pursuant to section 26 of HIPA.

3. Did HRHA respond appropriately to the breach of privacy?

[11] HRHA's internal investigation report provided as follows:

> The Clinic involved is comprised of three primary health care clinics in three separate rural communities…
>
> On July 2, 2015, a suspected breach of privacy by [a HRHA employee] was reported. A Registered Nurse/Nurse Practitioner (RN/NP) contacted the Care Team Manager

> for the two sites of the three sites with a concern that [an employee] may be accessing personal health information (PHI) in the med access electronic health record (EHR) without the need to know for provision of patient care.
> …
>
> The employees access to the EHR and the Heartland Health Information network were immediately terminated and the employee suspended pending further investigation.
>
> A preliminary audit of information provided by the Clinic for the period July 23, 2014 to July 23, 2015 confirmed that PHI may have been accessed by the employee without the requisite need to know and without the knowledge or consent of the patients.
>
> A full audit for the period May 7, 2014 to July 27, 2015 confirmed that the employee not only accessed PHI without the need to know, but also printed PHI. The Employee was terminated from [HRHA] on August 10th.

[12] The *Privacy Breach Guidelines: Tips for Public Bodies/Trustees dealing with Privacy Breaches* provide the following steps for responding to privacy breach:

- Contain the breach
- Notification
- Investigate the breach
- Prevent future breaches

[13] I will consider each of these steps to determine if HRHA has adequately responded to the privacy breach.

i. Contain the breach

[14] On July 21, 2015, it was suspected that an employee had inappropriately accessed, or snooped in personal health information in an EHR system.

[15] On July 23, 2015, a review of twelve months of data confirmed the suspicions that the employee in question had been snooping.

[16] On July 24, 2015, the employee's access to the EHR system was suspended.

[17] On July 27, 2015, HRHA met with the employee to conduct an interview into the matter. The employee was advised he would be suspended for two weeks while a full investigation was conducted.

[18] Once the investigation was complete, the employee's employment with HRHA was terminated on August 10, 2015.

[19] It appears that HRHA contained the breach.

ii. Notification

[20] When an HRHA Registered Nurse contacted the Care Team Manager regarding the suspected breach of privacy, it was reported to the Privacy Officer.

[21] HRHA's Privacy Officer became aware of the breach of privacy on July 21, 2015 and proactively reported this to our office on the same day. Although it is not mandatory for public bodies to report privacy breaches to our office, it is encouraged.

[22] HRHA had identified the affected individuals and provided notification of the breach of privacy by letter dated August 25, 2015. HRHA indicated that "the letters were sent to people in every province from BC to Quebec & Yukon, USA (Arizona, Rhode Island, Wisconsin), Finland and Germany."

[23] The affected individuals were also provided contact information for my office if they were not satisfied with HRHA's investigation. While my office did receive a number of telephone calls regarding this matter, my office did not receive any formal complaints from the affected individuals.

[24] On August 27, 2015, HRHA sent out a media release regarding this privacy breach.

[25] It appears that HRHA sufficiently provided notice of this privacy breach.

iii. Investigate the breach

[26] HRHA provided my office with the following regarding its investigation of this breach of privacy:

> The Manager of Qualify Improvement/ Privacy and Access Officer requested and received a full export of the employee's activity from Med Access. The data provided by med access was the for period of May 7, 2015 to July 27, 2015 and included login, logout and print information in addition to the details provided in the preliminary audit. The audit of data provided by med access identified that the employee had not only viewed personal health information in the patient chart, it also documented that the employee printed lab reports and patient/provider visit information.
>
> The employee's time sheets for the period May 5, 2014 to July 27, 2015 were correlated with audit data provided by med access.
> …
>
> Interviews were conducted with the employee, two physicians, an RN/NP, the Care Team Manager and two [employees that held the same position as the snooper]. The interviews provided the following information:
>
> - The employee attended the regional orientation which provides information on privacy and confidentiality.
>
> - The employee signed a confidentiality agreement.
>
> - The employee was provided orientation to med access, but there was no specific training locally regarding privacy and access.
>
> - The med access logon screen provides a confidentiality warning… The employee was first approached in March 2015 by the RN/NP regarding a warning that appeared on a computer screen when she tried to access a patient chart. The warning indicated the employee was in the chart. The employee denied being in the chart… The employee's permissions were immediately limited… Staff believed the matter had been dealth [sic] with and did not report it to the Privacy Officer.
>
> - The employee denies accessing personal health information in med access without the need to know.
>
> …
>
> - Regular audits are not being conducted on med access.
>
> …

[27] HRHA obtained audit reports from the EHR system and used the data to identify the accesses by this employee that did not have a corresponding work-related task to determine which individuals' personal health information had been inappropriately accessed. Of the 3,537 registered patients in the three clinics ranging in age from 0 to 102, HRHA identified that the employee had inappropriately accessed 901 patients personal health information. A review of the audit information revealed the following:

> As part of the audit, I was able to merge the dates/locations worked by the employee with the accesses to PHI. When I interviewed RN/NP and the physician on August 4th, I showed them a printout from the audit, I directed their attention to September 17th when the employee accessed 105 patient records, 103 of which were breaches. The RN/NP observed that the patients on the list were not patients of the same site i.e. some were patients of site A and others were patients of site B and some were patients of site C.

[28] HRHA was able to identify factors that contributed to the privacy breach including:

- Employee's access in the EHR system was initially set up to allow the employee access to all personal health information;
- Regular audit of the EHR system was not in place;
- Additional education for employees that handle personal health information required; and
- Confidentiality agreement needs to be revised to include language on HIPA and snooping.

[29] HRHA has provided my office with detail to show that this matter was investigated adequately.

[30] While it appears HRHA has conducted a sufficient investigation, due to the number of records the employee snooped into, I would recommend that HRHA provide their investigation file to the Ministry of Justice, Public Prosecutions Division to review the file and determine whether an offence has been committed and charges should be laid under HIPA.

iv. Prevent future breaches

[31] As discussed in the last section, HRHA identified areas for improvement in their investigation. Each of these factors will be discussed in this section.

Employee's access in the EHR system was initially set up to allow the employee access to all personal health information

[32] HRHA learned during the investigation that all users of this EHR system were set up with full access to all personal health information. HRHA indicated that the employee responsible for setting up users' access in the EHR system was selecting categories such as Lab, RN, Physician, Admin, etc. It was their understanding that this limited the user's access rights based on the category selected. However, HRHA learned that these categories did not limit users' access capabilities. Once HRHA discovered this, it reviewed all users' access rights and permissions were revised based on need-to-know. On a go-forward basis, HRHA advised that users will be manually granted access based on need-to-know rather than selecting job classifications.

Regular audit of the EHR system was not in place

[33] Once it was discovered that regular auditing was not in place, HRHA implemented regular auditing of the EHR system. During the investigation HRHA learned that the EHR system only retained full detail of audit data for a period of three months or 90 days. HRHA was not able to extend the amount of time that the detailed audit reports were available in the EHR system. HRHA advised they had implemented monthly random audits on the previous 30 days of accesses to ensure there is ample time to investigate any questionable accesses.

[34] HRHA advised that the EHR system approvers would be conducting these audits and any concerns would be reported to the Privacy Officer for further investigation.

Additional education for employees that handle personal health information required

[35] HRHA identified that although it provided all employees with privacy training during orientation, further training for employees that access personal health information required additional training. HRHA developed a one-hour privacy training session that it is rolling out via webex and face-to-face sessions. Employees are also required to complete a quiz after the training session and the quizzes are retained by HRHA. HRHA is also considering developing a training video for HRHA employees.

[36] HRHA also indicated that it was investigating if there were any training modules for users on privacy in the EHR system. If none existed, HRHA indicated that it would develop its own privacy training for the EHR system users.

[37] HRHA also developed a number of posters to display near computer stations to remind employees of their obligations under HIPA and to deter employees from snooping.

[38] If not already contemplated, HRHA may want to consider annual privacy training or creating a privacy refresher course for employees.

Confidentiality agreement needs to be revised to include language on HIPA and snooping.

[39] HRHA requires all employees to sign a confidentiality agreement at orientation. As a result of this investigation, HRHA has revised the agreement to include language that specifically addresses obligations and consequences for snooping under HIPA. If not already contemplated, HRHA may want to consider having employees review and sign the confidentiality agreement on an annual basis.

[40] HRHA also indicated that the EHR system had a confidentiality statement on the log-in screen. If not already contemplated, HRHA may want to consider incorporating

obligations and consequences of snooping under HIPA, such as those incorporated into the confidentiality agreements for staff into this statement.

[41] It appears that HRHA has implemented adequate safeguards to help prevent future occurrences of privacy breaches.

III FINDINGS

[42] I find that HIPA applies.

[43] I find that there was an unauthorized use of personal health information.

[44] I find that HRHA has adequately responded to the privacy breach and implemented sufficient safeguards to prevent future occurrences.

IV RECOMMENDATION

[45] I recommend that HRHA forward its investigation file including internal investigation report, audit logs, interviews, and any other relevant materials to the Ministry of Justice, Public Prosecutions Divisions to determine whether an offence has occurred and whether charges should be laid under HIPA.

Dated at Regina, in the Province of Saskatchewan, this 14th day of December, 2015.

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