Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 100-2015

Saskatoon Regional Health Authority

July 27, 2015

Summary: Through regular audits, the Saskatoon Regional Health Authority (SRHA) determined that an employee had viewed her own and other individuals' electronic personal health information without a need-to-know. She viewed the personal health information to satisfy curiosity and to alleviate boredom. SRHA proactively reported the snooping to the Information and Privacy Commissioner (IPC). The IPC made a number of recommendations, including disclosing the details of the disciplinary action taken against the snooper to affected individuals and to employees/practitioners of the regional health authority.

I BACKGROUND

[1] In early 2015, through regular audits, the Saskatoon Regional Health Authority (SRHA) determined that a Health Records Clerk had viewed her own and two other individuals electronic personal health information on the electronic clinical application, Sunrise Clinical Manager (SCM), without a need-to-know.

[2] SRHA commenced an investigation into the matter which included interviewing the Health Records Clerk. Through the investigation, it was determined that she viewed three other individuals' personal health information on SCM without a need-to-know.

[3] In total, the Health Records Clerk viewed six individuals' (including her own) personal health information.

[4] On May 7, 2015, SHRA proactively reported the matter to my office.

[5] On May 11, 2015, my office notified SHRA that it would be monitoring this matter and requested that SHRA provide an internal investigation report. In the notification, my office said that it would work with SHRA pursuant to section 52 of *The Health Information Protection Act* (HIPA) to address any outstanding issues.

II DISCUSSION OF THE ISSUES

1. Does HIPA apply?

[6] HIPA applies 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.

[7] The Health Records Clerk viewed personal health information on SCM. Such information would qualify as personal health information as defined by subsections 2(m)(i), 2(m)(ii), 2(m)(iv), and 2(m)(v). Second, SHRA qualifies as a trustee defined by subsection 2(t)(ii). Finally, personal health information stored on SCM is in the custody or control of SHRA. I find that HIPA applies.

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

[8] Subsection 2(u) of HIPA defines "use" as follows:

> 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.

[9] Further, section 26 of HIPA restricts trustees on how they can use personal health information.

[10] The Health Records Clerk cited curiosity and boredom as her reasons for viewing personal health information in SCM. I find that section 26 of HIPA does not authorize the use of personal health information to satisfy curiosity or to alleviate boredom.

3. Is SRHA's approach to addressing this matter adequate?

[11] One of the steps in addressing privacy breach matters is notifying affected individuals. This is so that affected individuals can undertake action they feel is necessary to protect their personal health information that may be at risk. SRHA has indicated that the affected individuals in this case have been notified that their personal health information was viewed without a need-to-know. I find that SRHA notifying the affected individuals to be appropriate.

[12] Appendix B of SRHA's *Privacy and Confidentiality* policy outlines different levels of privacy violations and the recommended actions that the health region should take. Appendix B categorizes privacy violations into three different levels. Level 1 privacy violations are unintentional, level 2 privacy violations are intentional but non-malicious, and level 3 privacy violations are intentional and malicious.

[13] Based on Appendix B, SHRA determined that the Health Records Clerk's viewing of the personal health information qualified as a level 2 privacy violation. The recommended actions for a level 2 privacy violation are as follows:

- Discussion of applicable SHR policies and procedures,
- Privacy training,
- Sign or re-sign confidentiality agreement,
- Discipline, up to and including suspension, and
- May notify the Office of Saskatchewan Information and Privacy Commissioner (OIPC)

[14] SHRA's internal investigation report advises that the Health Records Clerk received privacy training in late 2014 when she commenced employment with SRHA. She had also signed a confidentiality agreement as well. After the viewing of personal health information without a need-to-know was discovered, the Health Records Clerk's manager reviewed SRHA's privacy policies and procedures with the Health Records Clerk again

and had her re-sign SRHA's privacy and confidentiality agreement. In terms of discipline, SHRA advised that it would be auditing the Health Records Clerk's use of SCM for a period of six months to contain potential privacy breaches. However, SRHA recommended in its internal investigation report that the Health Records Clerk's privileges to use SCM be withdrawn.

[15] Since the Health Records Clerk's privileges could be withdrawn, my office asked if the Health Records Clerk required SCM to complete her job duties. In a letter dated July 9, 2015, SRHA confirmed that the Health Records Clerk requires SCM for her job duties but that it would audit her use of SCM for 24 months, instead of six months.

[16] In terms of discipline, I asserted in my Investigation Report 088-2013 that disciplinary action should be strong enough that it deters future snooping. In that Investigation Report, I noted that a Prairie North Regional Health Authority employee of 25 years who had a clean disciplinary record was terminated after it was discovered she snooped through the personal health information of 99 persons. Her intentions were non-malicious but the arbitrator in that case upheld the decision to terminate the employee. The arbitrator stated that the trust between the health region and its community and its employees would be onerous or impossible to rebuild if the employee was reinstated.

[17] Further, in his report *Detecting and Deterring Unauthorized Access to Personal Health Information* (January 2015), I note that the Information and Privacy Commissioner of Ontario has been pushing for more prosecutions for unauthorized access to personal health information to deter individual from snooping. The report is available at https://www.ipc.on.ca/images/Resources/Detect_Deter.pdf.

[18] On May 29, 2015, my office made the following recommendations to SRHA's approach to snooping:

1. Suspend employees who have snooped. The length of the suspension should be dependent upon the seriousness and frequency of the snooping;
2. Monitor employees who have snooped for a period of years instead of months;
3. Work with eHealth Saskatchewan (eHealth) so that eHealth can audit and monitor the snooper for any electronic system eHealth is a trustee for;
4. Terminate employees who have snooped intentionally and maliciously;

5. Report the snooping to the professional regulatory body to whom the employee/practitioner may belong once the snooping has been investigated and substantiated;
6. Disclose the details of the disciplinary action taken against the employee to the affected individual(s) and to all regional health authority employees and practitioners.

[19] SRHA responded by stating that it agreed to the second and third recommendation stated above.

[20] Regarding the first and fourth recommendation, SRHA asserted that suspension and termination is a part of its progressive discipline process.

[21] For the fifth recommendation, SRHA stated that licensing bodies requires reporting of cases where the employee has been terminated.

[22] Finally, SRHA stated that it wouldn't comply with the sixth recommendation listed above because it regards employee discipline as personal information pursuant to subsection 23(1)(b) of *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP) so it would not disclose such information pursuant to subsection 28(1) of LA FOIP. However, it noted that details of the discipline would be made public if grievances of discipline results in an arbitration ruling.

[23] I agree that employee discipline qualifies as personal information. However, given the seriousness of employee snooping and how it undermines patient trust, I would argue that there is a public interest disclosure of such personal information, and that subsection 28(2)(n) of LA FOIP would authorize the disclosure of such information. The disclosure would help to provide closure to affected individuals and it would also act as a deterrent to snooping by other employees. It could also help to restore Saskatchewan residents' trust that the health region is protecting personal health information appropriately.

[24] Further, subsection 28(2)(s) of LA FOIP and subsection 10(g)(i) of the LA FOIP Regulations enables local authorities to disclose personal information:

> 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;

[25] I note that in Investigation Report HO-010, the former Ontario Information and Privacy Commissioner stated the following regarding the disclosure of disciplinary action taken against a snooper and how our primary concern must lie with those who are snooped upon:

> Note that in Order HO-002, the discipline received by the offending employee was contained in the Order. In addition, when consulted by other hospitals in similar situations, we have advised that an individual whose file has been inappropriately accessed has the right to know, not only the identity of the staff member who accessed their file, but the details of any disciplinary action taken, including the quantum of any penalty.
>
> This level of transparency is important for several reasons. Accessing a patient's personal health information in an unauthorized manner is a serious violation of an individual's privacy and security of the person. In such a situation, the aggrieved individual has a right to a complete accounting of what has occurred. In many cases, the aggrieved parties will not find closure regarding the incident unless all the details of the investigation have been disclosed. Receiving general assurances that "the incident has been dealt with appropriately" falls far short of the level of disclosure that is required.
>
> For other staff members of the hospital involved, knowing that all of the details of the disciplinary action imposed will be publicly disclosed, should serve as a strong deterrent. This is especially true if those details also become known to other employees, either through the actions of the aggrieved individual, the custodian, or both. Employees must understand that, given the seriousness of these types of breaches, their own privacy concerns will take a back seat to the legitimate needs of the victims involved to have a full accounting of the actions taken by the health information custodian. Our primary concern must lie with the aggrieved party, whose privacy was completely disregarded.

[26] Disclosing the disciplinary action taken against the employee is also in line with decisions made by the College of Nurses of Ontario and the College of Pharmacists of Alberta. When a nurse was found to have snooped upon her boyfriend's estranged spouse, the College of Nurses of Ontario's penalty included requiring the nurse that she

provide her employers with a copy of the Discipline Committee's panel's Penalty Order together with the Notice of Hearing or, if available, the panel's written Decision and Reasons, together with any attachments, for a year after she returned to nursing.[1] Further, when a pharmacist was found to have snooped upon the records of several women from her church and posted the information on Facebook, the College of Pharmacists of Alberta sent a copy of the decision, including the name of the pharmacist, to all pharmacy regulatory bodies in Canada.[2]

[27] An employee who has snooped should have a diminished expectation of privacy. I strongly recommend that SRHA disclose the disciplinary action taken against employees who snoop.

III FINDINGS

[28] I find that HIPA applies.

[29] I find that the viewing of the personal health information by the Health Record Clerk was an unauthorized use.

[30] I find that SRHA's notifying the affected individuals to be appropriate.

[31] I find that SRHA's approach to addressing snooping should go further to treat this as an issue of public interest.

[1] Discipline Committee of the College of Nurses of Ontario. College of Nurses of Ontario and Registration No. HB00883. Available at: http://www.cno.org/Global/2-HowWeProtectThePublic/ih/decisions/fulltext/pdf/2009/Kerry%20Smith,%20HB00883,%20July%2010,%202008.pdf.

[2] Hearing Tribunal of the College of Pharmacists of Alberta. Hearing of Registration Number 8214. Available at https://pharmacists.ab.ca/sites/default/files/SonggadanDecision.pdf.

IV RECOMMENDATIONS

[32] I recommend that SRHA amend its approach when dealing with snooping and disclose the disciplinary action taken against employees who snoop to affected individual(s), and employees/practitioners of the regional health authority.

Dated at Regina, in the Province of Saskatchewan, this 27nd day of July, 2015.

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