



Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 230-2016

Keewatin Yatthè Regional Health Authority

April 21, 2017

Summary:

Through a previous Investigation Report, the Commissioner became aware of a possible breach of privacy related to an RN having access to patient files for a period of time that exceeded the amount of time required to complete her patient charting and that the RN was making personal notes in the patient files. The Commissioner found that Keewatin Yatthè Regional Health Authority (Keewatin) did not contain the breach of privacy or provide notification to the affected individuals. Further, the Commissioner found Keewatin did not meet the duty to protect under HIPA and did not conduct an adequate investigation. The Commissioner made a number of recommendations to Keewatin including interviewing the RN immediately about this incident, reviewing all patient files that the RN had access to, and providing notification to the affected individuals and updates to the Saskatchewan Registered Nurses Association about this incident. The Commissioner also made recommendations surrounding policies and training within Keewatin.

I BACKGROUND

- [1] Through Investigation Report 062-2016, my office was made aware of a possible breach of privacy within the Keewatin Yatthè Regional Health Authority (Keewatin) at the Buffalo Narrows Health Centre (Health Centre).
- [2] Keewatin provided my office with a copy of a previously prepared Occupational Health and Safety Report (Report) dated November 19, 2015, that it advised represented its Investigation Report.

- [3] In the Report, Keewatin advised my office that on the morning of January 21, 2014, a Registered Nurse (RN) began her reassessment for her Transfer of Medical Function (TMF). The TMF is where an RN reaches a level of knowledge and skill that he or she can manage certain medical functions and decisions that in the past were outside the scope of an RN and typically managed by physicians. According to the Report, it appears the TMF at that time was a requirement in order for an RN to work within the Health Centre.
- [4] In the afternoon of January 21, 2014 and upon completion of her reassessment, the RN was informed by her nursing educator that there were concerns with the RN's nursing practice and the RN's TMF assessment was being suspended until they were able to work on some basic areas of practice.
- [5] The Executive Director of Health Services (Executive Director) informed the RN that she would no longer be able to continue working at the Health Centre Clinic (clinic), as she required the TMF to work within the Health Centre. It was decided they would reconvene the next day in order to set out an education plan with a target to reassess the RN for her TMF in six months.
- [6] My office was further advised that the RN told the Executive Director that she needed a few minutes to complete patient charting of three files. It was estimated that this charting should take between 15 to 30 minutes. The RN was allowed to stay to finish the charting in the treatment room in the clinic. However the arrangement made with the Executive Director was she was to leave once the on-call RN was finished seeing a patient in emergency.
- [7] Once the on-call RN was finished with the patient, she informed the RN as such. However, even though the conditions were that the RN would stay and finish charting until the on-call RN was finished with the patient, she did not leave the clinic at that time. The on-call RN returned two times to see patients in Emergency, however the RN continued to chart. This allowed her unsupervised access to approximately 2,000 patient charts for approximately three hours.

[8] It was discovered that the RN had made personal notes in various patient charts, which included “workload became unmanageable”, “working alone”, and “working for several nights without back up or EMS.”

[9] My office notified Keewatin on September 20, 2016 that we would be initiating an investigation.

II DISCUSSION OF THE ISSUES

1. *Is The Health Information Protection Act (HIPA) engaged?*

[10] 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.

[11] First, the alleged breach occurred at the Health Centre. Services provided at the Health Centre include physician services, registered nurse and nurse practitioner services, a public health nurse, emergency medical services, addictions counselling, a mental health therapist, medical transportation, etc. Since the Health Centre is a facility of Keewatin which is a “trustee” pursuant to subsection 2(t)(ii) of HIPA, I find the first requirement is met.

[12] Subsection 2(m) of HIPA defines “personal health information” as follows:

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

(C) registration information;

[13] Keewatin advised that the RN was permitted to finish the patient charting in the treatment room, however she would have had unsupervised access to the file room where the clinic patient files are housed. It is clear from the services offered at the Health Centre, and from the Report provided by Keewatin, that personal health information is involved. As the information in question is stored on its premises, I find Keewatin has custody of the personal health information in question. HIPA is therefore engaged.

2. Did Keewatin respond appropriately to the privacy breach?

[14] The IPC Guide to HIPA includes Privacy Breach Guidelines that are specifically geared to trustees. Appendix C in this resource recommends the following five steps for responding to a breach of privacy:

- Contain the breach,
- Notification,
- Investigate the breach,
- Prevent future breaches, and
- Privacy breach report.

[15] I will consider each of these steps to determine if Keewatin adequately responded to the privacy breach.

Contain the breach

- [16] The first step in responding to a privacy breach is containing the breach, which means to stop the unauthorized practice when the trustee learns of it.
- [17] In its Report, Keewatin advised that on January 21, 2014, the RN was alone in the treatment room with access to the file room for approximately three hours after she had been told that her TMF would be suspended. It appears Keewatin did not recognize this as a potential privacy breach at the time because the Report that included this incident was not started until September 2015, almost a year later. Keewatin advised that the RN involved in the incident in question had filed various complaints regarding her workplace. At the time, she did not want anything done with her Occupational Health and Safety (OH&S) concerns, and requested that Keewatin document her concerns should future incidents warrant further action. However in June 2015 when the RN's TMF concerns arose, the RN changed her mind and requested that the OH&S issues be investigated. In a letter dated June 3, 2015 to the RN, it was agreed that a third party investigation would take place.
- [18] On January 21, 2014 at approximately 4:30 p.m., when the RN did not pass her TMF reassessment she was told she could not practice at the Health Centre without it, however she was allowed to stay to finish her charting unsupervised. The RN was unsupervised in a treatment room with access to the file room that houses approximately 2,000 patient charts. Keewatin was unable to confirm whether or not any of the charts were removed from the file room by the RN. When asked, Keewatin did not explain what type of file inventory management system they utilized.
- [19] It is important that the Health Centre maintain an inventory of their patient charts to ensure that if a breach occurs or files go missing, affected individuals can be notified. If the Health Centre does not have this, they should take immediate steps to inventory the files and create and continue to update a patient file index.

[20] The security and integrity of patient personal health information was put at risk when the RN was allowed to stay unsupervised for three hours. HIPA imposes an explicit duty to protect upon trustees. The duty to protect requires that a trustee has administrative, technical and physical safeguards in place to protect personal health information. This is found under section 16 of HIPA, which 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.

[21] Allowing her to remain in the Health Centre treatment room unsupervised for approximately three hours increased the risk of the RN having the opportunity to snoop in patient files. Employee snooping occurs when an employee who has the means to access personal information or personal health information of clients, patients or other employees does so without a legitimate business purpose. Motivations for snooping can include curiosity, boredom, profit or harm to other individuals; none of which are acceptable.

[22] Keewatin advised that it had not taken the steps to interview the RN regarding this incident as she is currently on an unpaid education leave and not expected to return until May of 2017. Because they did not interview the employee, Keewatin has no way to determine how many patient files she accessed without authority.

[23] In addition, had the RN been interviewed she could have been reminded of her obligations not to disseminate any of the information she may have viewed in any way. As noted above, the RN added personal notes to a number of patient files, so clearly she did access those files improperly.

[24] Therefore, I am unable to conclude that Keewatin has contained the breach.

Notification

[25] 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.

[26] In this case, Keewatin advised that it did not notify any affected individuals.

[27] Keewatin's decision to not notify the affected individuals is problematic. First of all, there is the possibility that the employee was snooping in numerous patient files due to the amount of time she had unsupervised access to the files. Secondly, Keewatin advised my office that the RN had entered "personal notes for protection" into patient files. This action is contrary to HIPA. Subsection 23(1) of HIPA provides:

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.

[28] Subsection 23(1) of HIPA is based upon two principles – need-to-know and data minimization. The need-to-know principle means that personal health information should only be available to those employees in an organization that have a legitimate need-to-know that information. Further, a trustee should limit collection and use of personal health information to what he or she would need-to-know to do their job and not collect information that is nice-to-know. The data minimization principle means that a trustee or

employee should collect, use or disclose the least amount of identifying information necessary for the purpose.

[29] In this case, there are a few instances where the need-to-know and data minimization principles were not followed. First, the RN was alone in the treatment room with access to the file room for close to three hours; therefore the risk of employee snooping significantly rises. Second, the RN entered personal notes into patient charts that appear to relate more to the RN and not the patient. Finally, Keewatin informed my office that it was a legal requirement for the RN to complete her patient charting for the day and they have also identified that patient charting should have taken a maximum of 30 minutes. As she had access to the patient files for close to three hours, I must conclude that she no longer held the requisite need-to-know beyond the first 30 minutes.

[30] As such, affected individuals have the right to review their patient files to ensure accuracy of the information. Keewatin should provide written notification letters to the three affected individuals whose charts they are aware the RN wrote personal notes in. In addition, I understand that Keewatin has not reviewed the other patient files to assess if personal notes were added by the RN. If this is the case, Keewatin should review those files and determine who should be notified about this incident. Further, Keewatin should provide a general notification to all clinic patients by posting a notice in the clinic reception area offering patients the opportunity to view their charts at no cost. The contact information of Keewatin's Privacy Officer and the IPC should also be available if anyone wishes to make a complaint.

[31] Although Keewatin has not yet notified the affected individuals, during the course of this investigation Keewatin has informed my office of its intention to now do so.

[32] Other than the affected individuals and my office, trustees should also consider whether or not it is appropriate to notify other organizations, for example, law enforcement or other regulatory bodies that oversee particular professions.

- [33] My office was not directly notified about this potential breach of privacy. We learned of it while investigating another privacy concern with Keewatin which can be found in Investigation Report 062-2016.
- [34] Finally, my office would usually recommend that the individual's governing body be contacted for any further disciplinary action. In the case of the RN, this would be the Saskatchewan Registered Nurses Association (SRNA).
- [35] As noted in paragraph [1], this breach was discovered by my office while conducting a previous investigation that I addressed in Investigation Report 062-2016. The SRNA was one of the parties involved in Investigation Report 062-2016 as it was made aware of alleged employee misconduct issues of the RN. During the course of this investigation, Keewatin informed my office that it has advised the SRNA of its concerns surrounding the RN's patient charting and intends to follow up with the SRNA once this report is issued in case there are further concerns that warrant disciplinary action.

Investigate the breach

- [36] The next step in responding to an alleged privacy breach is to investigate. Keewatin advised it had intended to interview the employee regarding the breach; however my understanding is that the employee is currently off on an unpaid education leave for a period of two years. My office was advised that it is Keewatin's practice to not contact employees while on leave of any kind as there is a risk of a grievance or harassment complaint by the employee and by the Union.
- [37] A similar instance occurred in Investigation Report 030-2016 where an employee found to have breached the privacy of various patients had not been interviewed as she was away on leave. The health region in that case had a similar practice where they did not contact employees who were on leave.
- [38] I find this practice to be unreasonable as it essentially protects the employee who has violated the privacy of a patient. In addition, it prevents a public body or trustee to fully

determine the extent of damage a breach of privacy may have caused, and delays proper notification to affected individuals. I encourage all employers to carry out an investigation as quickly as possible that includes interviewing employees regardless of whether or not they are on leave. I also encourage all professional associations and unions to cooperate with such requests to interview an employee regarding a privacy breach. Such a request is not harassment or unreasonable, it is merely completing an investigation of a privacy breach.

[39] It is my understanding that Keewatin will complete the investigation upon the employee's return. This is unacceptable as the breach took place two years ago and it is unfair to any affected individuals. Keewatin must also consider that there is potential that the employee may not return to Keewatin once the education leave concludes. This highlights how important it is for public bodies and trustees to interview employees at the time a privacy incident occurs, even if the employee is currently on leave.

[40] Once Keewatin has the opportunity to interview the employee and determine what corrective measures would be appropriate, I would request that Keewatin update my office with this information.

Prevent future breaches

[41] The most important part of responding to a privacy breach is to implement measures to prevent future breaches from occurring. Through this process, a trustee should determine what steps can be taken to prevent a similar privacy breach.

[42] Keewatin advised that it does not have a specific policy that speaks to handling staff that have been terminated, however they indicated they do follow the best practice of escorting terminated staff off the premises. Although the RN was not terminated the suspension of her TMF had the potential to create a contentious atmosphere for the RN and Keewatin. Therefore, Keewatin should have employed the best practice in this situation. However, it did not.

[43] In its Report, Keewatin asserted that the reason the RN was allowed to stay to finish her charting unsupervised was because it required quick charting. This is not an acceptable reason. Instead, if the charting needed to be completed the RN should have been supervised for the duration of the patient charting and by someone who was in a management or supervisory role.

[44] Although the RN was not terminated, section 15 of Canada's Health Informatics Association (COACH) *2013 COACH Guidelines for the Protection of Health Information* (Guidelines), part 15.8.3.3 addresses after employment (termination) and offers useful information for circumstances such as this. Part 15.8.3.3 of COACH provides:

Managers and supervisors should notify IT [Information Technology] and Security as soon as they know the date an employee is scheduled to leave the organization, and they should collect identification badges, keys and authentication devices when the person leaves. IT and Security should terminate all access privileges as soon as an employee leaves, including access to information systems and facilities.

[45] I would suggest organizations consider what security measures should be in place where an employee's circumstances become contentious. This could include situations where unexpected educational, job performance or disciplinary issues exist. In situations such as this, extra precautions should be taken.

[46] Keewatin advised that they are currently reviewing and updating their Human Resources and privacy policies which include training sessions with management to ensure they are aware of the proper procedures.

Privacy Breach Report

[47] The final step in responding to an alleged privacy breach is to formalize what was discovered through the previous four steps by preparing a privacy breach report.

[48] Through this investigation, I have determined that Keewatin has not taken the appropriate measures in responding to this privacy incident. Going forward, I would suggest

Keewatin utilize my office's resource *Privacy Breach Guidelines for Trustees* to assist in the steps required to properly respond.

[49] However, I am encouraged as Keewatin has advised my office that they have learned from this experience and plan to implement changes to its policies and procedures.

[50] Upon reviewing my office's draft Investigation Report, Keewatin advised it intends to follow the recommendations at paragraphs [55] to [57], [59], and [61] to [63]. Further it advised that it will look into options surrounding the recommendation at paragraph [60]. Finally, Keewatin advised that it does not agree with my recommendation at paragraph [58]. However it advised that it has pamphlets and posters available for clients and patients regarding their rights to access files. I encourage Keewatin to reconsider posting a notice in the clinic regarding this specific incident.

III FINDINGS

[51] I find that Keewatin did not contain the breach of privacy.

[52] I find that Keewatin did not meet the duty to protect under HIPA when the RN was allowed access to patient files beyond the timeframe required for her to complete the patient charting.

[53] I find that Keewatin did not conduct an adequate investigation.

[54] I find that Keewatin did not provide notification to affected individuals.

IV RECOMMENDATIONS

[55] I recommend that Keewatin interview the RN immediately, regardless of her being away on educational leave and I encourage SRNA and SUN to support this request for an interview.

- [56] I recommend Keewatin review all patient files that the RN had access to in order to assess if there are any further files that the RN entered personal notes into.
- [57] I recommend Keewatin provide written notification to the three or more affected individuals whose charts they know the RN entered personal notes into.
- [58] I recommend that Keewatin post a public notice in the clinic reception area regarding the incident and provide patients with the opportunity to view their chart free of charge.
- [59] I recommend that Keewatin revise its procedures in responding to a privacy breach to include interviewing the employee who has allegedly violated the privacy of another individual, regardless of whether or not the employee is on leave.
- [60] I recommend Keewatin revise its records management policies to include an index of patient charts in the Health Centre file room.
- [61] I recommend Keewatin include in their policies mandatory supervision of staff placed on unexpected leaves, terminations or where other possible contentious situations with staff arise until they have left the premises.
- [62] I recommend Keewatin conduct annual privacy training for all employees that includes employee snooping.
- [63] I recommend that Keewatin further update the SRNA about this privacy breach so it can determine if disciplinary action is necessary.

Dated at Regina, in the Province of Saskatchewan, this 21st day of April, 2017.

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