Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 180-2018, 181-2018, 226-2018

Saskatchewan Health Authority involving Dr. R, Dr. L, and Dr. F

January 29, 2019

Summary: eHealth Saskatchewan (eHealth) detected that three physicians at the Saskatchewan Health Authority (SHA) had inappropriately accessed the personal health information of individuals involved in a collision involving the Humboldt Broncos. eHealth proactively reported these privacy breaches to the Information and Privacy Commissioner (IPC). The IPC made a number of findings, including that privacy breaches occurred when each of the three physicians looked up the patient's personal health information in the Electronic Health Record Viewer after the patients were no longer in their care. The IPC made a number of recommendations including that SHA conduct regular monthly audits of the three physicians to ensure they are accessing personal health information only on a need-to-know basis.

I BACKGROUND

[1] On April 6, 2018, a highway collision occurred involving the hockey team Humboldt Broncos which left 16 dead and 13 injured. Three physicians, Dr. R, Dr. L, and Dr. F, provided emergency care to certain individuals involved in the collision at Nipawin Hospital, which is a part of the Saskatchewan Health Authority (SHA). Then, the patients were transferred and they were no longer in the physicians' care.

[2] On April 9, 2018, eHealth Saskatchewan (eHealth) proactively added the individuals involved in the collision to its watch list. This means that whenever the individual's profile is accessed in the Electronic Health Record Viewer (the Viewer), an email notification is sent to eHealth's Privacy, Access and Patient Safety Unit. As a result, eHealth detected Dr. R, Dr. L, and Dr. Fs' accesses to the Viewer.

[3] From April 7, 2018 to April 9, 2018, Dr. R accessed three individuals' personal health information that was stored in the Viewer. He accessed the personal health information through a web browser and through a feature called "launch-in-context" that is integrated with Nipawin Medi Clinic's electronic medical record (EMR).

[4] On April 9, 2018, Dr. L accessed one of the individuals' personal health information stored in the Viewer. He accessed the personal health information stored in the Viewer through the "launch-in-context" feature of Nipawin Medi Clinic's EMR.

[5] On April 11, 2018, April 13, 2018, and April 19, 2018, Dr. F entered into the Viewer and accessed one of the individuals' personal health information. She accessed the personal health information through a web browser.

[6] eHealth reported to my office that each of these three physicians accessed the personal health information after the patients were transferred because they believed they were in the individuals' "circle of care".

[7] eHealth determined that these three physicians accessed the personal health information without a need-to-know under *The Health Information Protection Act* (HIPA). Therefore, eHealth reported the accesses to my office.

II DISCUSSION OF THE ISSUES

1. Is HIPA engaged?

[8] HIPA is engaged when three elements are present: 1) personal health information, 2) trustee, and 3) the trustee has custody or control over the personal health information.

[9] First, 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
>
> (v) registration information;

[10] I find that information in the Viewer would qualify as personal health information as defined above. This includes the personal health information stored in the Viewer accessed either through the "launch in context" feature of the EMR or directly through a web browser.

[11] Second, the SHA is a trustee pursuant to subsection 2(t)(ii) 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) the provincial health authority or a health care organization;

[12] Third, the primary health care (PHC) agreements between each of the three physicians and the former Kelsey Trail Regional Health Authority (KTRHA) provides that the trustee for all the patient records is the KTRHA. As of December 4, 2017, the KTRHA became a part of the SHA. Therefore, I find that the SHA is the trustee that has control over the personal health information that is collected (viewed) from the Viewer by these three physicians.

[13] Based on the above, all three elements are present in order for HIPA to be engaged. I find that HIPA is engaged.

2. Did privacy breaches occur when each physician viewed personal health information in the Viewer?

[14] A privacy breach occurs when personal health information is collected, used, and/or disclosed without authority under HIPA.

[15] The need-to-know principle is the principle that trustees and their staff should only collect, use, or disclose necessary information for the diagnosis, treatment or care of an individual or other purposes authorized by HIPA. The need-to-know principle is enshrined in section 23 of HIPA which 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.
>
> (2) A trustee must establish policies and procedures to restrict access by the trustee's employees to an individual's personal health information that is not required by the employee to carry out the purpose for which the information was collected or to carry out a purpose authorized pursuant to this Act.

[16] Further, section 24 of HIPA restricts the collection of personal health information by trustees. It provides:

> 24(1) A trustee shall ensure that the primary purpose for collecting personal health information is for the purposes of a program, activity or service of the trustee that can reasonably be expected to benefit the subject individual.
>
> (2) A trustee may collect personal health information for a secondary purpose if the secondary purpose is consistent with any of the purposes for which personal health information may be disclosed pursuant to section 27, 28 or 29.
>
> (3) Nothing in this Act prohibits the collection of personal health information where that collection is authorized by another Act or by a regulation made pursuant to another Act.
>
> (4) A trustee may collect personal health information for any purpose with the consent of the subject individual.

[17] Even though the patients were transferred and were no longer in their care, the physicians collected personal health information from the Viewer because they believed they were in the patients' circle of care. The concept of circle of care is not found in HIPA. Once a patient is transferred from emergency, the physician is no longer involved in the patient's care unless it can be otherwise demonstrated. I find that privacy breaches occurred when Dr. R, Dr. L, and Dr. F looked up the patients' personal health information in the Viewer after the patients were transferred and no longer in their care. I will discuss the circle of care concept later in this report.

3. Did SHA properly respond to the privacy breaches?

[18] If a privacy breach has occurred, my office recommends five best practice steps. These are:

1. Contain the breach;
2. Notify affected individuals and/or appropriate organizations;
3. Investigate the breach;
4. Plan for prevention; and
5. Write an investigation report.

[19] Below is an analysis of each step.

Step 1: Contain the breach

[20] The first step to responding to a privacy breach is to contain the breach. In this case, to contain the privacy breach was to either suspend or terminate the employee's access to the Viewer.

[21] eHealth is the trustee for the Viewer so eHealth took steps to contain the breach. See Investigation Report 161-2018 on eHealth for more information.

Step 2: Notify affected individuals

[22] The second step to responding to a privacy breach is notifying the affected individuals that their personal health information was inappropriately accessed. This is important so that

they can take appropriate steps to protect themselves from any potential harm. Unless there is a compelling reason not to do so, trustees should always be notifying affected individuals. An effective notification 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 organization are taking to prevent similar privacy breaches in the future;
- The contact information of an individual within the 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; and
- Recognition of the impacts of the breach on affected individuals and an apology.

[23] In this case, eHealth notified the affected individuals or the next-of-kin. See Investigation Report 161-2018 on eHealth for more information.

Step 3: Investigate the privacy breach

[24] The third step to responding to a privacy breach is to investigate. Trustees should investigate to understand what happened and to identify the root cause of the privacy breach. An investigation will assist trustees in developing and implementing measures to minimize or prevent similar privacy breaches in the future.

[25] The SHA provided support to eHealth in eHealth's investigation into the matter. It was able to determine that the accesses by the three physicians were without a need-to-know. As already mentioned in my office's Investigation Report 161-2018, the physicians accessed the personal health information because they believed they were in the patients' "circle of care".

[26] As mentioned in my office's Investigation Report H-2013-001, the phrase "circle of care" is unhelpful when it comes to the training of health care workers in trustee organizations for the following reasons:

- First, the phrase "circle of care" is not focused on the patient but on physicians and employees of trustee organizations. It only considers the status of physicians and employees instead of focusing on the patient and particular care transaction in question. The better approach is to utilize the need-to-know principle in section 23 of HIPA which focuses not on physicians or employees but on the individual patient and the health needs presented in any particular health transaction.

- Second, the phrase "circle of care" suggests a static kind of entitlement to information. It suggests that if a physician attends to a patient for one ailment, then the physician can snoop upon that patient's personal health information in the future even if he or she is not involved in the patient's care. Or, even worse, the phrase "circle of care" suggests that any physicians or any other health care provider would be entitled to all personal health information just by virtue of being a physician or any other health provider.

- Third, the circle of care concept has been misinterpreted to only include trustees and their employees when, in fact, non-trustees (such as a police officer, teacher, or a daycare worker) may have a demonstrable need-to-know. The need-to-know principle permits disclosures in appropriate circumstances to non-trustees.

[27] The circle of care concept, which has no basis in HIPA, seems to persist and misguide organizations into breaching the requirements of HIPA. In the *2010-2011 Annual Report*, my office said the following about the circle of care concept:

> We have found this concept has contributed to professionals misunderstanding the requirements of HIPA, particularly the 'need to know principle' in section 23(1) of HIPA. The argument, as we understand it, is that health professions are familiar with the term and have used it for a very long time. Yet, that reliance on old concepts and assumptions has proven, in our experience, to perpetuate an over-confidence that translates into no incentive to learn what HIPA requires. We continue to urge those organizations to instead focus on the 'need to know' which is explicitly provided for in HIPA and which squarely puts the focus on the patient.

[28] I agree with the above. Organizations, including the SHA, should be promoting the need-to-know principle and should stop relying on the circle of care concept. I find that the circle of care concept is in direct contradiction of HIPA and it fails to protect patients' privacy. The need-to-know principle is clearly laid out in subsection 23(1) of HIPA and should be followed and enforced.

[29] In an email dated November 26, 2018, the SHA also noted that, in general, physicians look up the personal health information of former patients so they learn if their initial diagnosis

was accurate. This access is to assist physicians or employees in determining if the diagnosis and/or treatment they provided was correct. In other words, physicians or employees may need to access patient's personal health information for education purposes. On page 45 of my office's document *Striking a Balance: Proposals for Amendments to The Health Information Protection Act* (available at https://oipc.sk.ca/assets/proposals-for-amendments-to-hipa.pdf), my office recommended the following amendment to allow for accesses for education purposes. This amendment would require the physician or employee to seek authorization from the trustee organization prior to accessing patient's personal health information. The amendment is as follows:

> It is proposed that an additional subsection be added to section 26, which might provide as follows:
>
> > 26(2) A trustee may provide authorization for the use of personal health information about an individual
> >
> > ...
> >
> > (d) for educating its employees to provide health services, if it is not reasonably practicable for the consent of the subject individual to be obtained;

[30] I recommend that the Ministry of Health amend the HIPA Regulations to reflect the above.

Step 4: Plan for prevention

[31] Prevention is perhaps the most important step in a trustee's response to a privacy breach. Trustees should learn from the privacy breach and improve its practices in order to avoid similar privacy breaches in the future.

[32] In an email dated November 26, 2018, the SHA indicated that while it conducts audits, it said it is difficult to reconcile what is an appropriate look-up versus one that is not. It currently audits for same name look-ups. However, it often relies on its staff to report unauthorized accesses to its Privacy Officers so its Privacy Officers can investigate further.

[33] Also, the SHA indicated it recently completed and rolled out a privacy training video for all staff. It said it has 46,000 staff in total. Currently, it has set a goal of training 5000 of

its staff by March 31, 2019. Its ultimate goal is training 100% of its active staff by March 31, 2021. This is an impressive goal. I hope once all staff are trained that SHA would begin to have annual refresher training for all staff.

[34] I find the above efforts by the SHA to be appropriate. I recommend that the SHA work with eHealth to conduct regular monthly audits on Dr. R, Dr. L, and Dr. F for a period of three years to ensure they are accessing personal health information only on a need-to-know basis. I recommend that if the SHA finds any of them inappropriately accessing personal health information, then the SHA should request that eHealth disable their account(s). I also recommend that the SHA report any inappropriate accesses to my office and to the College of Physicians and Surgeons of Saskatchewan.

Step 5: Write an investigation report

[35] The fifth step to responding to a privacy breach is writing an investigation report. Trustees should document their investigation, the root causes they have identified, and their plan for prevention. This is to ensure that trustees follow through with their plans to prevent similar breaches in the future.

[36] The SHA provided support to eHealth for eHealth's investigation into the matter. Therefore, it did not complete its own investigation report. I recommend that the SHA, if it has not already done so, document these privacy breaches, the lessons it has learned, and the steps it will take to prevent similar privacy breaches in the future.

III FINDINGS

[37] I find that HIPA is engaged.

[38] I find that privacy breaches occurred when Dr. R, Dr. L, and Dr. F looked up the patients' personal health information in the Viewer after the patients were transferred and no longer in their care.

[39] I find that the circle of care concept is in direct contradiction of HIPA and it fails to protect patients' privacy. The need-to-know principle is clearly laid out in subsection 23(1) of HIPA and should be followed and enforced.

[40] I find that the SHA's efforts described at paragraphs [32] and [33] to be appropriate in preventing similar privacy breaches in the future.

[41] I find that the SHA did not complete its own investigation report into the privacy breaches described in this report.

IV RECOMMENDATIONS

[42] I recommend that the SHA work with eHealth to conduct regular monthly audits on Dr. R, Dr. L, and Dr. F for a period of three years to ensure they are accessing personal health information only on a need-to-know basis.

[43] I recommend that if the SHA finds any of them inappropriately accessing personal health information, then the SHA should request that eHealth disable their account(s). I also recommend that the SHA report any inappropriate accesses to my office and to the College of Physicians and Surgeons of Saskatchewan.

[44] I recommend that the SHA, if it has not already done so, document these privacy breaches, the lessons it has learned, and the steps it will take to prevent similar privacy breaches in the future.

[45] I recommend that the Ministry of Health amend HIPA Regulations to reflect the proposed amendment at paragraph [29].

Dated at Regina, in the Province of Saskatchewan, this 29th day of January, 2019.

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