Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 240-2018

Saskatchewan Health Authority involving Dr. M

January 29, 2019

Summary: eHealth Saskatchewan (eHealth) detected that a medical resident at the College of Medicine at the University of Saskatchewan (U of S) had inappropriately accessed the personal health information of three 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 how the circle of care concept is in direct contradiction of HIPA and it fails to protect patients' privacy. The IPC made a number of recommendations including that the SHA require all residents to receive privacy training from SHA Privacy Officers prior to being granted access to any personal health information, including information accessible through the Viewer.

I BACKGROUND

[1] In April 2018, Dr. M was a medical resident at Postgraduate Education (PGME), a division of the College of Medicine at the University of Saskatchewan (U of S). As such, she was both a student and an employee of the U of S. She was completing her medical residency at a hospital that is a part of the Saskatchewan Health Authority (SHA).

[2] On April 6, 2018, a highway collision occurred involving the hockey team Humboldt Broncos which left 16 dead and 13 injured.

[3] On April 7, 2018, Dr. M accessed the Electronic Health Record Viewer (the Viewer) and viewed the personal health information of an individual.

[4] On April 8, 2018, she accessed the Viewer and viewed the personal health information of a second individual.

[5] On April 9, 2018, she accessed the Viewer again and viewed the personal health information of a third individual.

[6] Also 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 in the Viewer is accessed, an email notification is sent to eHealth's Privacy, Access and Patient Safety Unit. As a result, eHealth detected Dr. M's accesses to the three individuals' personal health information in the Viewer.

[7] In its investigation, eHealth requested from PGME the reason for Dr. M's accesses. PGME indicated that Dr. M had attended to two of the three individuals in the weeks leading up to the collision. After the collision, Dr. M felt the need to check up on the two individuals to get closure. However, she could not remember the names of the two individuals so she accidentally accessed the third individual's personal health information.

[8] My office had contacted the U of S and the SHA for information regarding Dr. M's accesses. The U of S indicated that Dr. M wanted to know if the two individuals whom she attended prior to the collision had been admitted to the hospital as she might see them at the hospital on her next shift. She was concerned. In contrast, the SHA indicated to my office that Dr. M had attended to one (not two) of the three individuals. It said it did not have evidence that Dr. M had attended to either of the two other individuals at its facilities. My office verified with the medical clinics Humboldt Clinic Limited and Humboldt Family Physicians that Dr. M did not attend to any of the three individuals at either of those clinics.

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

II DISCUSSION OF THE ISSUES

1. Does HIPA apply to this matter?

[10] 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.

[11] 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;

[12] I find that information in the Viewer would qualify as personal health information as defined above.

[13] Second, neither the U of S nor PGME qualify as a trustee as defined by subsection 2(t) of HIPA. 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;

[14] Third, the former Saskatoon Regional Health Authority (SRHA), which is now the SHA, had an affiliation agreement with the U of S. Under this affiliation agreement, there is a subsidiary agreement that was made effective September 1, 2016. This subsidiary agreement provides that the SRHA must provide access to patient records to clinical learners. This suggests that the former SRHA had custody and control of the patient records. Based on the agreement, then, I find that the former SRHA, which is now the SHA, is the trustee that has custody or control over the patient records when it is collected (viewed), used, and/or disclosed by its medical residents.

[15] Based on the above, all three elements are present in order for HIPA to be engaged. When resident physicians are completing their residencies with the SHA, the SHA is the trustee organization responsible for how resident physicians collect, use, and/or disclose personal health information.

2. Did privacy breaches occur when Dr. M viewed personal health information in the Viewer?

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

[17] The need-to-know principle is the principle that trustees and their staff should only collect, use, or disclose information necessary 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.

[18] 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.

[19] As noted in the background, Dr. M had looked up the individuals to get closure and because she was concerned. Those are reasons that are not in accordance with sections 23 and 24 of HIPA. I find that privacy breaches occurred when Dr. M looked up the three individuals' personal health information in the Viewer.

3. Did the SHA properly respond to the privacy breaches?

[20] 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.

[21] Below is an analysis of each step.

Step 1: Contain the breach

[22] 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.

[23] 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

[24] 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.

[25] 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

[26] 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. Even though the SHA is the trustee of personal health information collected (viewed), used, and/or disclosed by its medical residents, my office sought information from the U of S in addition to seeking information from the SHA about what happened.

a. U of S

[27] In its letter to my office dated September 25, 2018, the U of S indicated that Dr. M did not realize that her accesses to the Viewer were privacy breaches. However, it said that Dr. M has now reviewed HIPA and realizes the accesses are not authorized.

[28] The U of S provided my office with a copy of a PowerPoint presentation that is used to train residents on privacy in Academic Family Medicine, which is a part of the PGME at the U of S where Dr. M received the training. It also provided my office with a copy of the Academic Family Medicine's Health Information Privacy Policies & Procedures. Based on a review of the PowerPoint presentation and the policies and procedures, the concept of "circle of care" is used. Neither the PowerPoint nor the policies and procedures defines the term "circle of care".

[29] The term "circle of care" contributes to the misunderstanding of the requirements of HIPA, especially since it contrasts with the need-to-know principle in section 23 of HIPA. Perhaps a reason for Dr. M's not realizing that her accesses qualified as a privacy breach is because the term "circle of care" might convey she is within the circle of care because she had attended to at least one of the individuals prior to the collision.

[30] 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.

[31] 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.

[32] I agree with the above. Organizations 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.

[33] I recommend that the U of S amend its PowerPoint presentation and its Health Information Privacy Policies and Procedures to remove the concept of circle of care and replace it with section 23 of HIPA and the need-to-know principle.

b. SHA

[34] In its letter dated October 31, 2018, the SHA indicated the following:

- It does not play a role in provisioning access to the Viewer to Dr. M but it is PGME that provides access to the Viewer;
- It is uncertain whether or not it provided privacy training to Dr. M at the beginning of her residency in 2015;
- Dr. M signed a confidentiality agreement with the former Saskatoon Health Region on June 10, 2015 wherein the first clause of the confidentiality agreement emphasizes the need-to-know principle. The first clause provides as follows:

> 1. I will use confidential information only as needed to perform my legitimate duties with the Saskatoon Health Region. This means, among other things, that:
>
>   (a) I will only access confidential information for which I have a need to know in connection with the services I am providing to the Saskatoon Health Region;

[35] I find that the SHA not playing a role in provisioning access to the Viewer may have contributed to the privacy breach. It should be the SHA, not PGME, which authorizes medical residents to have access to the Viewer. This is because medical residents such as Dr. M are accessing personal health information in the custody or control of the SHA, not PGME. Prior to approving medical residents to having access to the Viewer, the SHA should have delivered privacy training, and be satisfied that the medical residents understand HIPA and the need-to-know principle.

Step 4: Plan for prevention

[36] 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.

a. U of S

[37] In an email dated October 16, 2018, the Privacy Officer at the U of S indicated it intends on meeting with SHA's Executive Director of Privacy and Health Information Management to discuss gaps and to improve training provided to resident physicians. I find this to be an appropriate step to take in preventing similar privacy breaches in the future.

b. SHA

[38] In an email dated November 20, 2018, the SHA informed my office that while it has provided privacy training to residents, it does not do so regularly or on a yearly-basis. I recommend that the SHA require all residents to receive privacy training from its Privacy Officers at their orientation prior to being granted access to any personal health information, including information accessible through the Viewer. Then, residents should receive privacy training annually.

Step 5: Write an investigation report

[39] 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.

[40] In this case, my office requested and received information regarding the privacy breaches from both the U of S and the SHA. Therefore, both of them have documented these privacy breaches. However, if they have not already done so, I recommend that both the U of S and the SHA document these privacy breaches, the identified root causes, and their plans for prevention.

III FINDINGS

[41] I find that HIPA is engaged.

[42] I find that privacy breaches occurred when Dr. M looked up the three individuals' personal health information in the Viewer.

[43] 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.

[44] I find that the SHA not playing a role in provisioning access to the Viewer may have contributed to the privacy breach.

[45] I find the U of S's intention to meet with the SHA to discuss gaps and to improve privacy training provided to resident physicians to be an appropriate step to take in preventing similar privacy breaches in the future.

IV RECOMMENDATIONS

[46] I recommend that the U of S amend its PowerPoint presentation and its Health Information Privacy Policies and Procedures to remove the concept of circle of care and replace it with section 23 of HIPA and the need-to-know principle.

[47] I recommend that the SHA require all residents to receive privacy training from SHA Privacy Officers at the resident physicians' orientation prior to being granted access to any personal health information, including information accessible through the Viewer.

[48] I recommend that SHA provide privacy training to resident physicians annually.

[49] I recommend that both the U of S and the SHA document the privacy breaches discussed in this report, the identified root causes, and their plans for prevention, if they have not already done so.

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

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