Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 161-2018

eHealth Saskatchewan

January 29, 2019

Summary: Following the high-profile collision involving the Humboldt Broncos hockey team, eHealth Saskatchewan (eHealth) began monitoring the Electronic Health Record Viewer (Viewer) profiles of individuals involved in the collision. It detected inappropriate accesses, or snooping, into the profiles of individuals involved in the collision. eHealth proactively reported these privacy breaches to the Information and Privacy Commissioner (IPC). The IPC made a number of findings including how eHealth took the appropriate steps to respond to these privacy breaches. The IPC made a number of recommendations to eHealth, including that it conduct regular monthly audits of the physicians who inappropriately accessed personal health information in the Viewer, that it comply with the need-to-know principle instead of the circle of care concept, and that eHealth develop a solution to force users of the Viewer to review eHealth's training and to take quizzes on an annual basis. He also recommended that the Ministry of Health amend the HIPA Regulations.

I BACKGROUND

a. What happened?

[1] On April 6, 2018, a highway collision occurred involving the hockey team Humboldt Broncos that killed 16 individuals and injured 13 others. It resulted in significant media attention and interest from across the province, country, and world. Due to the high-profile nature of the collision, eHealth Saskatchewan (eHealth) understood that the risk of snooping, or the unauthorized accesses into patients' personal health information would be heightened. Therefore, on April 9, 2018, eHealth began monitoring the profiles of the

patients within its system, the electronic Health Record Viewer (Viewer), to detect snooping.

[2] Between April 9, 2018 and May 15, 2018, eHealth detected eight users of the Viewer, mostly physicians, accessed without apparent authority the profiles of ten patients. This report focuses on eHealth and the inappropriate accesses of six users. Investigation Report 206-2018, 207-2018, 208-2018, 214-2018 focuses on the remaining inappropriate accesses.

[3] On July 5, 2018, eHealth proactively reported the snooping to my office.

[4] Before proceeding to the analysis of the issues, I will provide a description of the Viewer and how eHealth provisions access to the Viewer.

b. Viewer

[5] The Viewer enables users to view the following types of personal health information:

- Laboratory results;
- Medication information;
- Immunization information;
- Transcribed reports;
- Clinical encounters;
- Structured medical records; and
- Chronic disease information.

[6] The personal health information stored on the Viewer is retrieved from other organizations, including medical clinics or the Saskatchewan Health Authority (SHA). Then, whenever a user views personal health information on the Viewer, eHealth is *disclosing* personal health information to that particular user (or the user’s employer). Therefore, this report focuses on eHealth’s *disclosure* of personal health information. Related reports focused on the *collection* of personal health information are as follows:

- Investigation Report 162-2018 (Dr. Falah Majid P.C. Inc.),
- Investigation Report 177-2018 (Dr. Russom Ockbazghi and Dr. Warren N. Huber of Humboldt Clinic Limited involving Dr. D),

- Investigation Report 240-2018 (Saskatchewan Health Authority involving Dr. M.),
- Investigation Report 180-2018, 181-2018, 226-2018 (Saskatchewan Health Authority involving Dr. R, Dr. L, Dr. F), and
- Investigation Report 206-2018, 207-2018, 208-2018, 214-2018 (eHealth Saskatchewan and University of Saskatchewan).

II DISCUSSION OF THE ISSUES

1. Is HIPA engaged?

[7] *The Health Information Protection Act* (HIPA) is engaged when three elements are present: 1) a trustee, 2) personal health information, and 3) the trustee has custody or control over the personal health information. Below is an analysis to see if these three elements are present and that HIPA is engaged.

[8] First, eHealth is a trustee as defined by subsection 2(t)(i) of *The Health Information Protection Act* (HIPA), which reads:

> 2 In this Act:
>
> ...
>
> (t) "trustee" means any of the following that have custody or control of personal health information:
>
> (i) a government institution;

[9] eHealth is a government institution pursuant to subsection 2(1)(d) of *The Freedom of Information and Protection of Privacy Act* (FOIP) and Part I of the Appendix of *The Freedom of Information and Protection of Privacy Regulations*.

[10] Second, the Viewer enables users to view the information listed at paragraph [5]. Such information qualifies as personal health information as defined by subsection 2(m) of HIPA, which provides:

> 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;
>
> ...
>
> (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;

[11] Third, eHealth developed and maintains the Viewer. Therefore, eHealth has custody and control over the personal health information. I find that HIPA is engaged.

2. Did privacy breaches occur? If so, did eHealth manage the privacy breaches properly?

[12] Privacy breaches occur when personal health information is collected, used, and/or disclosed without authority under HIPA. I will determine if privacy breaches occurred in the cases that eHealth proactively reported to my office. If I find that privacy breaches did occur, then I will need to determine if eHealth properly managed the breaches.

[13] As illustrated in the background, each time a user of the Viewer accesses personal health information, eHealth is disclosing personal health information. Therefore, I need to determine if eHealth had authority under HIPA to disclose personal health information in each case.

[14] To "disclose" personal health information is to expose personal health information to a separate entity that is not a division or branch of the trustee organization that has custody or control of the personal health information. eHealth should only be disclosing personal health information in accordance with sections 27, 28, or 29 of HIPA or *The Health Information Protection Regulations*. If there is no authority for the disclosure, then a privacy breach has occurred.

[15] 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.

[16] If I find that a privacy breach has occurred in each case, then I will determine if the privacy breach has been properly managed.

[17] Below is a description of each case.

a. Dr. Falah Majid P.C. Inc.

i. Did privacy breaches occur?

[18] On April 9, 2018, an employee, S, at the Dr. Falah Majid Medical P.C. Inc. accessed the Viewer and viewed the personal health information of two individuals involved in the collision. Then, on April 17, 2018, eHealth masked the Viewer profiles of the deceased individuals. On April 18, 2018, the employee attempted to view the personal health information of one more individual but that individual's profile was masked. Therefore, the employee was only able to view the individual's demographic information. The employee admitted she accessed the personal health information of the three individuals for the following reasons:

- her family members had heard one of the individuals had died and she wanted to verify the information,
- she thought another individual was a patient at the Dr. Falah Majid P.C. Inc. so she looked up the individual, and
- she wanted to verify a detail that was reported by the media about one of the individuals.

[19] I find that neither HIPA nor its regulations authorize eHealth to disclose personal health information for the above reasons. Therefore, I find that privacy breaches occurred in each instance.

ii. Did eHealth properly respond to the privacy breaches?

Step 1: Contain the breach

[20] The first step in responding to a privacy breach is to contain the breach. This means to stop the breach from being ongoing. This includes recovering the personal health information. It can also include suspending or terminating the employee's access to the Viewer.

[21] According to eHealth's investigation report, it contacted Dr. Falah Majid P.C. Inc. on April 20, 2018 seeking an explanation for the employee's viewing of personal health information. On that same day, eHealth received an explanation as to why the employee accessed one of the three individuals' personal health information but it did not receive an explanation as to why she accessed the two other individuals' personal health information. Since it did not receive a fulsome explanation, eHealth suspended the employee's access to the Viewer on April 25, 2018. eHealth had indicated to Dr. Falah Majid that it would reactivate the employee's Viewer account once she completed privacy training.

[22] Dr. Falah Majid provided eHealth further information regarding the employee's accesses and was satisfied the employee had received additional privacy and confidentiality training. Therefore, eHealth reactivated the employee's Viewer account on May 2, 2018. However, the employee resigned from her job and was no longer an employee as of May 31, 2018.

[23] On July 13, 2018, eHealth learned that Dr. Falah Majid did not contact eHealth to permanently disable the employee's account once the employee left. Therefore, eHealth submitted a ticket to its Access Management Services to have the account deactivated. Also, eHealth has added this employee to its watch list. This means that the Privacy, Access and Patient Safety unit at eHealth will be alerted if her account is ever reactivated.

[24] I find that eHealth has contained this privacy breach.

Step 2: Notify affected individuals

[25] 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 is 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.

[26] eHealth notified the affected individuals or their next-of-kin letters dated September 18, 2018. eHealth indicated to my office that its notification letters were “high-level” and offered an invitation to speak to eHealth for more specific information.

[27] Based on a review of the letters, I find that they contain the appropriate elements of a notification letter. I find that eHealth has notified the affected individuals or their next-of-kin.

[28] I note, however, in describing steps eHealth will take to prevent similar privacy breaches in the future, eHealth explained it would explore amendments to HIPA to consider the concept of “circle of care” and circumstances in which a health care provider can reasonably be considered to be within the circle of care of a patient.

[29] I recommend that eHealth comply with the need-to-know principle and not the circle of care. A person has a legitimate need-to-know if he or she requires the information to provide diagnosis, treatment, or care to a patient or for 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.

Step 3: Investigate the privacy breach

[30] 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. Its investigation will assist trustees in developing and implementing measures to minimize or prevent similar privacy breaches in the future.

[31] In its investigation, eHealth determined that the employee's curiosity and not knowing that snooping was unacceptable were the root causes of the privacy breaches.

[32] When users log into the Viewer for the first time, a pop-up featuring the Joint Services/Access Policy (JSAP) appears. The JSAP will be discussed later in the report but it acts as an agreement between eHealth and organizations (referred to as "Authorized Provider Organizations" or APOs). It outlines eHealth's expectations of and the responsibilities of APOs and its employees or contractors ("users"). The user must agree to comply with the JSAP by clicking "Accept" on the pop-up.

[33] Section 5.2 of the JSAP provides that information from the Viewer is to only be used for the purpose of supporting or providing care to the patient and to whom the information relates. It says:

> <u>5.2 Identifying Purposes</u>. The EHR Data shall be collected and used through the EHR Viewer or Integration only for the purpose of supporting or providing care to the patient to whom the information relates and to whom the APO is providing current health services (the "Authorized Health Purpose").

[34] The employee accepted the pop-up on December 5, 2016. However, a root cause of this privacy breach was that she was unaware that snooping was unacceptable.

[35] In addition to the first pop-up, a second pop-up appears that users must also accept. The second pop-up is a "eHR Viewer Training Declaration". By accepting the declaration, users declare they have completed eHealth's Viewer training that is available at https://www.ehealthsask.ca/services/ehr-viewer/Pages/Access-Training-Resources.aspx. The training includes a video on privacy and security, which explicitly provides that users are to only access the personal health information of patients to whom they are providing care. They are not permitted to view other records including their own. The employee also accepted the second pop-up on December 5, 2016. In spite of this, she still was unaware that snooping was unacceptable.

[36] eHealth requiring the employee to accept the two pop-ups when she first logged into the Viewer did not stop the employee from snooping. In Step 4, I will discuss eHealth's plans for prevention.

Step 4: Plan for prevention

[37] 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.

[38] eHealth indicated it will undertake the following four steps to prevent a similar privacy breach in the future:

1) Create a pop-up that will appear the next time users of the Viewer logs in. The pop-up will remind users of the appropriate use of the Viewer. The user must agree to the pop-up in order to proceed;
2) Update the JSAP;
3) Develop standard protocol for future high profile cases; and
4) Develop a communication plan to educate Viewer users on appropriate collect, use and disclosure of Viewer data.

[39] I find that the above four steps for prevention are appropriate but not enough. I recommend that eHealth require its users to accept the two pop-ups described at paragraphs [32], [35] and [38] every six months. I also recommend that eHealth develop a solution to force users of the Viewer to review eHealth's training and to track which users have taken the training. Ideally, eHealth should require both new and active users to take a training course with quizzes on an annual basis. New users should not be granted user privileges until they successfully complete the quizzes. Active users should be given a two-month window to complete the training and quizzes. The two month-window should allow them to plan and schedule when to complete the training and quizzes in a timely manner.

Step 5: Write an investigation report

[40] 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.

[41] eHealth completed an investigation report that documents its investigation, the root causes, and its plan for prevention. I find that eHealth has fulfilled this final step of responding to privacy breaches.

b. Dr. Russom Ockbazghi and Dr. Warren N. Huber of Humboldt Clinic Limited involving Dr. D

i. Did privacy breaches occur?

[42] On April 7, 2018, Dr. D of Humboldt Clinic accessed the Viewer and viewed the personal health information of two individuals. From April 8, 2018 to April 10, 2018, Dr. D again viewed the personal health information of one of the individuals.

[43] Humboldt Clinic indicated that the two individuals were Dr. D's patients. Dr. D attended to one of the patients 13 times from August 22, 2016 to January 18, 2018. Dr. D attended to the other patient nine times from September 2, 2014 to January 18, 2018.

[44] For one of the individuals, Humboldt Clinic explained Dr. D wanted to know what injuries the individual sustained, if the individual received care, or if it was an instant fatality. For the other individual, it explained Dr. D was concerned.

[45] According to eHealth's investigation report, Dr. D explained to eHealth that there is a delay in the personal health information appearing in Humboldt Clinic's electronic medical record (EMR). Therefore, he was not able to access the personal health information through Humboldt Clinic's EMR right away. As such, he accessed the personal health information through the Viewer.

[46] I find that neither HIPA nor its regulations authorize disclosures for the above reasons. Therefore, I find that privacy breaches occurred.

ii. Did eHealth properly respond to the privacy breaches?

Step 1: Contain the breach

[47] The first step to responding to a privacy breach is to contain the breach.

[48] In this case, eHealth did not suspend nor terminate Dr. D's access to the Viewer. Instead, it sent a letter dated May 14, 2018 to Dr. D to explain that his use of the Viewer was not authorized by the JSAP. It informed Dr. D to consider the letter as a notice that any further incidents "may be considered a subsequent case of non-compliance and may initiate further review regarding [his] access privileges to the Viewer."

[49] I find that eHealth has taken action to contain the breach. However, it could take further action, which will be discussed at Step 4 below.

Step 2: Notify the affected individuals

[50] The second step to responding to a privacy breach is notifying the affected individuals that their personal health information was inappropriately accessed. The importance of notifying individuals and the elements of an effective notification was explained earlier in this report.

[51] eHealth notified the affected individuals or their next-of-kin in letters dated September 18, 2018. eHealth indicated to my office that its notification letters were "high-level" and offered an invitation to speak to eHealth for more specific information.

[52] Based on a review of the letters, I find that they contain the appropriate elements of a notification letter. I find that eHealth has notified the affected individuals or the next-of-kin.

[53] Again, however, in eHealth's notification letter, eHealth explained it would explore amendments to HIPA to consider the concept of "circle of care" and circumstances in which a health care provider can reasonably be considered to be within the circle of care. I recommend that eHealth comply with the need-to-know principle found in section 23 of HIPA. Users of the Viewer should only be accessing the Viewer for the purpose of providing diagnosis, treatment or care to patients. Concern or curiosity should not be enough reason to snoop upon patients' personal health information.

Step 3: Investigate the privacy breach

[54] The third step to responding to a privacy breach is to investigate.

[55] As explained earlier, users must accept two pop-ups when they access the Viewer for the first time. Accepting the first pop-up implies the user agrees to comply with the JSAP. Accepting the second pop-up means the user has completed eHealth's Viewer training.

[56] Based on information provided to my office by eHealth, Dr. D accepted the JSAP pop-up on May 13, 2014. Then, he accepted the Viewer training pop-up on April 8, 2015. In spite of accepting both pop-ups, Dr. D still accessed the personal health information of the two individuals even though he was not providing care to the two individuals. He was merely concerned.

[57] Further, as described earlier, Dr. D attempted to access the personal health information on Humboldt Clinic's EMR but was unable to do so. Therefore, he accessed the personal health information on the Viewer instead. This suggests Dr. D is unfamiliar with section 23 of HIPA and the need-to-know principle. He should not have accessed the two individuals' personal health information using either system.

[58] I find that eHealth investigated the privacy breach. I find that the root cause of the privacy breaches is Dr. D's not knowing section 23 of HIPA and the need-to-know principle.

Step 4: Plans for prevention

[59] 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.

[60] As already mentioned, eHealth will undertake the four steps listed at paragraph [38] to prevent a similar privacy breach in the future. In addition to the four steps, I recommend that eHealth conduct regular monthly audits of Dr. D's accesses to the Viewer for at least three years to ensure compliance. I recommend that the Humboldt Clinic cooperate and assist eHealth with the audits. If eHealth finds Dr. D inappropriately accessing the Viewer, I recommend that eHealth disable his account. I also recommend eHealth report any inappropriate activity to my office and to the College of Physicians and Surgeons of Saskatchewan (CPSS).

Step 5: Write an investigation report

[61] The fifth step to responding to a privacy breach is writing an investigation report. eHealth completed an investigation report that documents its investigation, the root causes, and its plan for prevention. I find that eHealth has fulfilled this final step of responding to the privacy breaches.

c. Saskatchewan Health Authority involving Dr. M

i. Did privacy breaches occur?

[62] 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 rural family medicine rotation at a hospital that is a part of the SHA.

[63] As a medical resident at PGME, Dr. M had requested user privileges to the Viewer. According to information provided to my office by the U of S, residents are instructed to go to eHealth's website to register for a Viewer account. As a part of the registration process, residents must select an organization. They are instructed to select PGME as their organization. On January 23, 2018, Dr. M registered and received access to the Viewer.

[64] On April 7, 2018, Dr. M accessed the Viewer and viewed the personal health information of an individual involved in the collision. Then, on April 8, 2018, she accessed the Viewer and viewed the personal health information of a second individual involved in the collision. Lastly, on April 9, 2018, she accessed the Viewer again and viewed the personal health information of a third individual.

[65] In its investigation, eHealth requested from PGME the reason for Dr. M's accesses. PGME indicated to eHealth 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.

[66] In the course of my office's investigation, the U of S indicated that Dr. M saw two of the three individuals while on shift in the emergency department. The two individuals were provided with directions for follow-up if necessary but there was no direct plan for ongoing care and there were no follow-up appointments scheduled. The U of S indicated that Dr. M accessed these two individuals' personal health information after the collision had occurred because she wanted to know if the two individuals had been admitted to the hospital as she might see them on her next shift. She was concerned.

[67] In contrast to PGME and the U of S' investigation, 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 attended to either of the two other individuals. Nevertheless, I find that neither HIPA nor its regulations authorize disclosures so that the physician can get closure or because she is concerned. Therefore, I find that privacy breaches occurred.

ii. Did eHealth properly respond to the privacy breaches?

Step 1: Contain the breach

[68] The first step to responding to a privacy breach is to contain the breach.

[69] Similar to Dr. D, eHealth did not suspend nor terminate Dr. M's access to the Viewer. It sent a letter dated May 14, 2018 to Dr. M to explain that her use of the Viewer was not authorized by the JSAP. It informed Dr. M to consider the letter as a notice that any further incidents "may be considered a subsequent case of non-compliance and may initiate further review regarding [her] access privileges to the Viewer."

[70] I find that eHealth has taken action to contain the breach. However, it could take further action, which will be discussed at Step 4 below.

Step 2: Notify the affected individuals

[71] The second step to responding to a privacy breach is notifying the affected individuals that their personal health information was inappropriately accessed. The importance of notifying individuals and the elements of an effective notification was explained earlier in this report.

[72] eHealth notified the affected individuals or their next-of-kin in letters dated September 18, 2018. eHealth indicated to my office that its notification letters were "high-level" and offered an invitation to speak to eHealth for more specific information.

[73] Based on a review of the letters, I find that they contain the appropriate elements of a notification letter. I find that eHealth has notified the affected individuals or their next-of-kin.

[74] Similar to the notification letters to the affected individuals or their next-of-kin in Dr. D's case, eHealth explained it would explore amendments to HIPA to consider the "circle of care" consent and circumstances in which a health care provider can reasonably be considered to be within the circle of care. Again, as I have said earlier, I recommend that eHealth comply with the need-to-know principle and not the circle of care.

Step 3: Investigate the privacy breach

[75] The third step to responding to a privacy breach is to investigate.

[76] As explained earlier, users must accept two pop-ups when they access the Viewer for the first time. Accepting the first pop-up implies the user agrees to comply with the JSAP. Accepting the second pop-up means the user has completed eHealth's Viewer training.

[77] Based on information provided to my office by eHealth, Dr. M accepted both pop-ups on January 23, 2018. In spite of this, Dr. M still accessed the personal health information of the two individuals even though she was apparently not providing care to the individuals. In Step 4, I will discuss eHealth's plans for prevention.

[78] I find that eHealth has investigated this matter.

Step 4: Plans for prevention

[79] 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.

[80] As already mentioned, eHealth will undertake the four steps listed at paragraph [38] to prevent a similar privacy breach in the future. In addition to the four steps, I recommend that eHealth conduct regular monthly audits of Dr. M's access to the Viewer for at least three years to ensure compliance. If eHealth finds Dr. M inappropriately accessed the Viewer, I recommend that eHealth disable her account. I also recommend that eHealth report any inappropriate access to my office and to CPSS.

[81] In addition, I recommend that eHealth remove PGME as an APO and to no longer require medical residents to select PGME as the organization with which to be associated when registering for access to the Viewer. eHealth should require medical residents to select the organization with which they are completing their residency. In this case, eHealth should have instructed Dr. M to select the SHA as the organization. This is because Dr. M was working on behalf of the SHA and was accessing personal health information in its custody or control. I will address this matter further in my Investigation Report 240-2018.

Step 5: Write an investigation report

[82] The fifth step to responding to a privacy breach is writing an investigation report. eHealth completed an investigation report that documents its investigation, the root causes, and its plan for prevention. I find that eHealth has fulfilled this final step of responding to privacy breaches.

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

i. Did privacy breaches occur?

[83] On April 6, 2018, three physicians, Dr. R, Dr. L, and Dr. F, provided emergency care to individuals involved in the collision at the Nipawin Hospital. Then, the patients were transferred on April 6, 2018 and they were no longer in the physicians' care.

[84] 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).

[85] 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.

[86] 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.

[87] 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".

[88] HIPA does not contemplate the concept of "circle of care". Therefore, I find that neither HIPA nor its regulations authorized eHealth to disclose personal health information to these three physicians once the patients were no longer in their care. I find that privacy breaches occurred in the above instances.

ii. Did eHealth properly respond to the privacy breaches?

Step 1: Contain the breach

[89] The first step to responding to a privacy breach is to contain the breach.

[90] Similar to cases involving Dr. D and Dr. M, eHealth did not suspend nor terminate Dr. R, Dr. L, or Dr. Fs' access to the Viewer. It sent letters dated May 14, 2018 to each of them. The letters contained the same message it had for Dr. D and Dr. M.

[91] I find that eHealth has taken action to contain the breach. However, it could take further action, which will be discussed at Step 4 below.

Step 2: Notify the affected individuals

[92] The second step to responding to a privacy breach is notifying the affected individuals that their personal health information was inappropriately accessed. The importance of notifying individuals and the elements of an effective notification was explained earlier in this report.

[93] eHealth notified the affected individuals or their next-of-kin in letters dated September 18, 2018. eHealth indicated to my office that its notification letters were "high-level" and offered an invitation to speak to eHealth for more specific information.

[94] Based on a review of the letters, I find that they contain the appropriate elements of a notification letter. I find that eHealth has notified the affected individuals or their next-of-kin.

[95] Similar to the notification letters to the affected individuals or their next-of-kin in the other cases discussed in this report, eHealth explained it would explore amendments to HIPA to consider the "circle of care" consent and circumstances in which a health care provider can reasonably be considered to be within the circle of care. Again, as I have said earlier, I recommend that eHealth comply with the need-to-know principle and not the circle of care.

Step 3: Investigate the privacy breach

[96] The third step to responding to a privacy breach is to investigate.

[97] As explained earlier, users must accept two pop-ups when they access the Viewer for the first time. Accepting the first pop-up implies the user agrees to comply with the JSAP. Accepting the second pop-up means the user has completed eHealth's Viewer training.

[98] Based on information provided to my office by eHealth, Dr. R accepted both pop-ups on July 15, 2016. Dr. L accepted both pop-ups on September 1, 2016. Dr. F accepted both pop-ups on January 19, 2017. In spite of accepting the pop-ups, all three physicians still accessed the personal health information of individuals in the Viewer without a need-to-know. In Step 4, I will discuss eHealth's plans for prevention.

[99] I find that eHealth has investigated this matter.

Step 4: Plans for prevention

[100] 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.

[101] As already mentioned, eHealth will undertake the four steps listed at paragraph [38] to prevent a similar privacy breach in the future. In addition to the four steps, I recommend that eHealth conduct regular monthly audits of Dr. R, Dr. L, and Dr. Fs' accesses to the Viewer for at least three years to ensure compliance. If eHealth finds any of them to inappropriately access the Viewer, I recommend that eHealth disable their account(s). I also recommend that eHealth report the inappropriate access to my office and to CPSS.

Step 5: Write an investigation report

[102] The fifth step to responding to a privacy breach is writing an investigation report. eHealth completed an investigation report that documents its investigation, the root causes, and its

plan for prevention. I find that eHealth has fulfilled this final step of responding to privacy breaches.

3. Did eHealth meet its duty to protect pursuant to section 16 of HIPA?

[103] Section 16 of HIPA imposes a duty to protect personal health information upon trustees. Since eHealth is a trustee, it must have safeguards in place to protect personal health information. Section 16 of HIPA provides as follows:

> 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.

[104] In its investigation report, eHealth identified two safeguards, the JSAP and its Electronic Provincial Privacy Audit and Monitoring (ePPAM) service, as the safeguards it has in place to meet its duty to protect. I will discuss these two safeguards below. In addition, I will discuss a third safeguard, masking of Viewer profiles.

a. First safeguard: Joint Services/Access Policy (JSAP)

i. JSAP and the physician-approval process

[105] The JSAP was finalized on July 31, 2013. It acts as an agreement between eHealth and an APO. APOs are organizations whose employees or contractors (including physicians) may access personal health information in the Viewer. In order for an organization to become an APO, it must seek approval from eHealth by submitting a Viewer Request for Organizational Approval form to eHealth.

[106] Once an organization is approved by eHealth to be an APO, the JSAP provides that APOs must appoint an individual (or individuals) to be its Authorized Approver. An Authorized Approver approves or denies requests by the APO's employees or contractors for access to the Viewer. If they are approved, they become a "user". The JSAP provides as follows:

> 1. Prior to eHealth or the Ministry disclosing personal health information to an authorized provider organization ("APO"), the APO must agree, in writing, to comply with and to be legally bound by the provisions of this Policy. Each APO will be given a copy of or access to this Policy.
>
> 2. Prior to an individual who is employed by or associated with an APO and who has been authorized to access the EHR Viewer or Integration (a "User") accessing the personal health information, the User must be:
>   - Approved by a designated approver appointed by the APO;
>   - Agree electronically to comply with and to be legally bound by the provisions of this Policy; and
>   - Given a copy of or access to this Policy.

[107] Prior to October 21, 2014, the process set out in the JSAP was followed. That is, an organization would have to be approved by eHealth to become an APO. Only after an organization became an APO could its employees or contractors (including physicians) request to become a user of the Viewer. However, the process for organizations to be approved by eHealth to become an APO was perceived as too much of a time-consuming activity and physicians required timelier access to the Viewer.

[108] Therefore, eHealth set out to create and implement an approval process so that physicians obtain timelier access to the Viewer. According to an email by a former eHealth Vice President dated October 21, 2014 to organizations such as the former regional health authorities, the Ministry of Health, and CPSS, eHealth no longer required physicians to associate themselves with an actual APO. eHealth created an APO called "eHS Physicians".

[109] When registering to become a user of the Viewer, physicians no longer have to associate themselves with an actual APO but with eHS Physicians. Then, since physicians are no longer required to associate with an actual APO, eHealth would act as the Authorized Approver. That is, when physicians request user access to the Viewer, eHealth approves or

denies the requests. As long as the physician has a "good standing" status within CPSS's Provider Registry System, eHealth would approve the physician. Below is a quote from eHealth's email dated October 21, 2014 which explains the two reasons for changing its physician approval process:

> i. Physicians are named Trustees under *The Health Information Protection Act* (HIPA) and are therefore individually responsible for the proper use and disclosure of personal health information.
>
> ii. Use cases for the majority of physicians show utilization of the eHR Viewer within multiple organizational settings where a provincial approval process is better suited.

[110] According to eHealth's email dated October 21, 2014, eHealth stated that CPSS would investigate any complaints of inappropriate access to the Viewer. The email says:

> The College of Physicians and Surgeons will act as the investigation and disciplinary body for complaints of inappropriate access to patient information within the eHR Viewer.
>
> - As per their mandate CPS will respond accordingly to any complaint issued directly to them or through eHealth Saskatchewan to any inappropriate activity within the eHR Viewer.

[111] It should be noted that the physician-approval process set out in eHealth's email dated October 21, 2014 is not reflected in the JSAP. The JSAP was finalized on July 31, 2013. The above process came into effect October 21, 2014. Therefore, the JSAP is not being consistently followed and it is out-of-date.

[112] Below are concerns my office has with eHealth's process as set out in eHealth's email dated October 21, 2014.

1. Physicians are not the trustees with custody or control over the personal health information collected from the eHR Viewer

[113] One of the reasons cited in eHealth's email dated October 21, 2014 for implementing its physician-approval process is that physicians themselves are trustees under HIPA. This is short-sighted.

[114] eHealth should take note of which trustee and/or organization actually has custody or control over the patient records once it discloses the records. Physicians often do not have custody or control over patient records. For example, physicians are often contractors or employees of a medical clinic. In these cases, it would be the medical clinic retaining the responsibility for the electronic and paper patient records so they, not the physicians, have custody or control over the records. Unless physicians own a medical clinic, they are not the ones responsible for patient records. Similarly, physicians may have practicing privileges with the SHA. The SHA would have custody or control over the patient records, not the physicians.

[115] If physicians require access to the Viewer to do work, they are doing work on behalf of an organization such as a medical clinic or the SHA. Therefore, when eHealth discloses personal health information through the Viewer, it is disclosing personal health information to the organization (such as the medical clinic or the SHA) and not to physicians.

[116] As such, it is essential that eHealth have an agreement between itself and the organization for whom the physicians work prior to allowing physicians to gain access to the eHR Viewer. This is so that eHealth can be assured it is disclosing personal health information to the organization for purposes authorized by HIPA. The JSAP acts as that agreement. However, the physician-approval process as set out in eHealth’s email dated October 21, 2014 undermines the JSAP by not requiring organizations to seek approval by eHealth to become an actual APO prior to physicians requesting access to the Viewer. eHealth is instructing physicians to associate themselves with the fabricated entity “eHS Physicians”. Without the JSAP or any agreement between itself and actual organizations, eHealth does not have a mechanism to hold organizations accountable for how their physicians are using the Viewer.

[117] I find that the JSAP is currently ineffective as a safeguard because it is not being followed by eHealth.

[118] I recommend that eHealth end the practice of approving physicians directly through eHS Physicians. I also recommend that eHealth no longer follow the physician-approval process outlined in the October 21, 2014 email. I recommend that eHealth require organizations to be approved as an APO before its physicians can be approved as users. As a part of the approval process for organizations to become APOs, I recommend that eHealth develop a checklist of specific safeguards that the JSAP requires the potential APOs to have in place. This would include:

- customized privacy policies and procedures that address access to and personal health information collected from the eHR Viewer;
- a privacy officer;
- HIPA compliant technical safeguards on all devices that will be used to access the Viewer;
- annual HIPA training for all employees;
- a procedure to ensure all approved users of the Viewer have taken eHealth training on an annual basis; and
- HIPA compliant physical safeguards.

[119] I recommend that eHealth have the organizations fill out the checklist and sign it before being approved as an APO.

[120] Only once an organization is approved as an APO should its physicians be allowed to request to become a user. Physicians should associate themselves with an actual APO when registering to become a user of the Viewer. I recognize that this is a time-consuming activity. However, if physicians need to gain access to the Viewer quickly, then eHealth should encourage organizations to initiate the process to be approved as an APO sooner. Patient privacy should not be compromised in the process. Finally, I recommend that eHealth have all existing APOs complete and sign the checklist within one year. I recommend that eHealth require APOs to sign and submit the checklist annually.

2. CPSS to investigate misuse

[121] eHealth's October 21, 2014 email provided that CPSS would be the organization that would investigate any complaint about inappropriate activity within the Viewer. eHealth should always undertake its own investigations into any alleged privacy breaches involving the Viewer and not rely on another organization to conduct investigations.

[122] This case was different in that there was no complaint about the snooping. eHealth proactively monitored and detected the snooping in the Viewer. I commend it for doing so. This suggests that eHealth is not relying on another organization to conduct investigations into inappropriate activity within the Viewer. I recommend that eHealth continue to undertake its own investigations.

[123] In response to my office's draft version of this report, eHealth clarified that it is responsible for investigating breaches of the Viewer. It has an agreement with CPSS that if it needs to escalate a breach of privacy, then CPSS would cooperate and work with eHealth on that investigation.

3. Criteria for approving physicians

[124] According to eHealth's October 21, 2014 email, physicians only need a "good standing" in CPSS' Provider Registry System in order to be approved by eHealth for access to the Viewer. The criteria should be much higher. A "good standing" in CPSS' Provider Registry System does not mean the physician understands the need-to-know principle and how to appropriately use the Viewer.

[125] Physicians should be able to demonstrate their knowledge of HIPA, the JSAP, and eHealth's privacy and security training materials prior to being approved for access to the Viewer. As I have recommended earlier, I recommend that eHealth develop a solution to force users of the Viewer to review eHealth's training and to track which users have taken the training. Ideally, eHealth should require new users to take a training course with quizzes and the issuing of a certificate on an annual basis.

ii. JSAP and approving non-physicians

[126] For approving non-physicians, eHealth is still following the JSAP. That is, an organization still needs to be approved as an APO prior to any of the employees/contractors who are non-physicians requesting access to the Viewer. I recommend that eHealth continue to follow this process.

b. Second safeguard: ePPAM Service

[127] ePPAM Service is the auditing and monitoring feature in the Viewer. eHealth used ePPAM Service to detect every time the patient profile of an individual involved in the collision was accessed in the Viewer. By doing so, eHealth was able to determine which accesses were legitimate and which accesses were not.

[128] I find that the ePPAM Service was an effective tool in detecting snooping.

[129] I recommend that eHealth use the ePPAM Service to regularly audit the physicians in these cases to ensure they are accessing the Viewer legitimately for a period of at least three years.

[130] I recommend that eHealth proactively conduct random audits on users of the Viewer to ensure they are complying with HIPA.

c. Third safeguard: Masking of Viewer profile

[131] According to eHealth’s website, masking is a control mechanism that allows individuals the opportunity to hide, or “mask”, their personal health information from being viewed in the Viewer. When health care providers attempt to access personal health information in that case, they will not be able to do so unless:

1) the individual provides consent to the health care provider to viewing the personal health information,
2) in an emergency situation where the individual is unable to provide consent,
3) dangerous use of prescription drugs is suspected,
4) they (health care providers) need to view the personal health information to correct, verify, or complete information for a previously provided health service,
5) the masked personal health information is required by law.

[132] Individuals may request that eHealth mask their Viewer profiles. If they wish to do so, they can go to https://www.ehealthsask.ca/access for more information.

[133] In this case, as mentioned at paragraph [18], eHealth proactively masked the Viewer profiles of the deceased individuals. This proactive masking prevented the employee at Dr. Falah Majid Medical P.C. Inc. from accessing one particular individual's personal health information. I find that the masking of Viewer profiles of the deceased individuals was helpful in minimizing snooping.

4. Is the "circle of care" concept adequate in protecting patient's privacy?

[134] The phrase "circle of care" has been mentioned throughout this investigation report, including how eHealth conveyed to affected individuals or their families that it is exploring amendments to HIPA to consider the concept of "circle of care", as well as eHealth indicating that Dr. R, Dr. L, and Dr. F believed they were in the patients' circle-of-care.

[135] 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.

[136] 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.

[137] I agree with the above. Organizations, including eHealth, 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.

[138] Trustee organizations have raised with my office that physicians or employees may need to access patient’s personal health information once the patient has been transferred elsewhere for further care. 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;

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

III FINDINGS

[140] I find that HIPA is engaged.

[141] I find that privacy breaches occurred when the employee, S, at Dr. Falah Majid Medical P.C. Inc. accessed the Viewer to view her own personal health information and the personal health information of three individuals involved in the collision.

[142] I find that eHealth contained the privacy breaches in the cases discussed in this report but that it could take further action.

[143] I find that eHealth notified the affected individuals or their next-of-kin in the cases discussed in this report.

[144] I find that eHealth investigated the privacy breaches in the cases discussed in this report.

[145] I find that eHealth's pop-ups did not stop the employee, S, at Dr. Falah Majid Medical P.C. Inc, Dr. M, Dr. D, Dr. R, Dr. L, Dr. F from snooping.

[146] I find that the four steps eHealth plans to undertake to prevent similar privacy breaches in the future described at paragraph [38] are appropriate.

[147] I find that eHealth has completed an investigation report into the privacy breaches discussed in this report.

[148] I find that privacy breaches occurred when Dr. D of Humboldt Clinic accessed the personal health information of two individuals involved in the collision.

[149] I find that the root cause of the privacy breaches is Dr. D not knowing section 23 of HIPA and the need-to-know principle.

[150] I find that privacy breaches occurred when Dr. M accessed the personal health information of three individuals involved in the collision.

[151] I find that privacy breaches occurred when Dr. R, Dr. L, and Dr. F accessed personal health information in the Viewer when they did not have a need-to-know.

[152] I find that the JSAP is currently ineffective as a safeguard because it is not being followed consistently by eHealth.

[153] I find that the ePPAM Service was an effective tool in detecting snooping.

[154] I find that the masking of Viewer profiles of the deceased individuals was helpful in minimizing snooping.

[155] I find that the circle of care concept is in direct contradiction of HIPA and it fails to protect patients' privacy.

IV RECOMMENDATIONS

[156] I recommend that eHealth comply with the need-to-know principle and not the "circle of care".

[157] I recommend that eHealth require its users to accept the pop-ups described at paragraphs [32], [35], and [38] every six months.

[158] I also recommend that eHealth develop a solution to force users of the Viewer to review eHealth's training and to track which users have taken the training. Ideally, eHealth should require both new and active users to take a training course with quizzes on an annual basis. New users should not be granted user privileges until they successfully complete the quizzes. Active users should be given a two-month window to complete the training and quizzes. The two month-window should allow them to plan and schedule when to complete the training and quizzes in a timely manner.

[159] I recommend that eHealth conduct regular monthly audits of Dr. D's, Dr. M's, Dr. R's, Dr. L's, and Dr. F's accesses to the Viewer for at least three years to ensure compliance. If eHealth finds any of them inappropriately accessing the Viewer, I recommend that eHealth disable their account. I also recommend eHealth report any inappropriate activity to my office and to the College of Physicians and Surgeons of Saskatchewan.

[160] I recommend that the Humboldt Clinic cooperate and assist eHealth with the auditing of Dr. D's accesses to the Viewer.

[161] I recommend that eHealth remove PGME as an APO and to no longer require medical residents to select PGME as the organization with which to be associated when registering for access to the Viewer. eHealth should require medical residents to select the organization with which they are completing their residency.

[162] I recommend that eHealth end the practice of approving physicians directly through eHS Physicians.

[163] I recommend that eHealth require organizations to be approved as an APO before its physicians can be approved as users.

[164] As a part of the approval process for organizations to become APOs, I recommend that eHealth develop a checklist of specific safeguards that the JSAP requires the potential APOs to have in place. This would include:

- customized privacy policies and procedures that address access to and personal health information collected from the eHR Viewer;
- a privacy officer;
- HIPA compliant technical safeguards on all devices that will be used to access the Viewer;
- annual HIPA training for all employees;
- a procedure to ensure all approved users of the viewer have taken eHealth training on an annual basis; and
- HIPA compliant physical safeguards.

[165] I recommend that eHealth have all existing APOs complete and sign the checklist within one year.

[166] I recommend that eHealth require APOs to sign and submit the checklist annually.

[167] I recommend that eHealth continue to undertake its own investigations instead of relying on other organizations such as CPSS to undertake investigations into privacy breaches.

[168] I recommend that eHealth continue to follow the process outlined in the JSAP for approving non-physicians.

[169] I recommend that eHealth use the ePPAM Service to regularly audit the physicians in these cases to ensure they are accessing the Viewer legitimately for a period of at least three years.

[170] I recommend that eHealth proactively conduct random audits on users of the Viewer to ensure they are complying with HIPA.

[171] I recommend that the Ministry of Health amend the HIPA Regulations to reflect paragraph [138].

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

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