Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 206-2018, 207-2018, 208-2018, 214-2018

eHealth Saskatchewan and University of Saskatchewan

January 29, 2019

Summary: eHealth Saskatchewan (eHealth) detected that two medical residents at the Postgraduate Medical Education (PGME), a division of the College of Medicine at the University of Saskatchewan (U of S), had inappropriately accessed the personal health information within the eHealth's system, the Electronic Health Record Viewer (Viewer) for the purpose of a research project. Instead, the medical residents were supposed to access the personal health information in Saskatchewan Health Authority's electronic system, Sunrise Clinical Manager (SCM). eHealth proactively reported the privacy breaches to the Information and Privacy Commissioner (IPC). The IPC made a number of findings, including that a root cause of the privacy breaches is the researchers not knowing that SCM and the Viewer cannot be used interchangeably. The IPC made a number of recommendations including that the U of S continue its efforts in working with the PGME and the SHA in improving privacy training delivered to medical residents.

I BACKGROUND

[1] Two resident physicians, Dr. D and Dr. K, at the Postgraduate Medical Education (PGME), a division of the College of Medicine at the University of Saskatchewan (U of S), are members of a research project. The Principal Investigator of the research team submitted an application for operational approval from the former Saskatoon Health Region (now the Saskatchewan Health Authority). According to its application, the research project was to evaluate the treatment of a particular illness in tertiary hospitals in Saskatoon. The Principal Investigator sought access to the personal health information of one hundred patients testing positive for the particular illness stored in Saskatoon Health Region's electronic

system called Sunrise Clinical Manager (SCM) from the dates October 1, 2017 to May 31, 2018.

[2] Meanwhile, on April 6, 2018, a highway collision occurred 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 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 (the Viewer), to detect snooping.

[3] Then, on May 11, 2018, as a result of its monitoring, eHealth detected that the personal health information of one particular patient involved in the collision was accessed by the two resident physicians. In its investigation, eHealth determined that the two resident physicians had accessed personal health information of patients testing positive for the particular illness using the Viewer instead of SCM. eHealth determined the following:

- Dr. D had accessed the personal health information of 58 patients who tested positive for the particular illness within the Viewer for the purpose of the research project from January 3, 2018 to May 14, 2018. One of these patients was involved in the collision. Dr. D was having difficulties with her SCM account so she used the Viewer instead to gain access to the personal health information.

- Dr. K was returning from a leave of absence so her SCM account had not been reactivated. To gain access to personal health information, she used another physician's, Dr. S's (Dr. S), Viewer account. She accessed the personal health information of 15 patients who tested positive for the particular illness.

[4] For background, eHealth's electronic system, 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.

[5] The personal health information stored on the Viewer is retrieved from other organizations, including medical clinics or the Saskatchewan Health Authority. Whenever a user of the Viewer views personal health information on the Viewer, eHealth is *disclosing* personal health information to that particular user (or the user's employer). The user, who is usually an employee or contractor of an organization, would be *collecting* personal health information.

[6] Also, it should be noted in this background that all three physicians have their own Viewer accounts. According to information provided to my office by the U of S, medical residents apply directly to eHealth for access to the Viewer. As a part of the registration process, residents must select an organization. They are instructed to select PGME as their organization. Then, PGME becomes the "Authorized Approver" according to eHealth's Joint Services/Access Policy (JSAP). That is, PGME decides whether to approve or reject the resident physicians as users of the Viewer.

III DISCUSSION OF THE ISSUES

1. Is HIPA engaged?

[7] *The Health Information Protection Act* (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. Below is an analysis to see if these three elements are present and that HIPA is engaged.

[8] First, the Viewer enables users to view the information listed at paragraph [4]. 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;

[9] Second, 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;

[10] 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*.

[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?

[12] Privacy breaches occur when personal health information is collected, used, and/or disclosed without authority under HIPA. 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 the following:

- if eHealth had authority under HIPA to disclose personal health information through the Viewer to the two researchers, and
- if the researchers had authority to collect the personal health information from the Viewer.

[13] In the course of my office's investigation, SHA described the activities of the researchers as a quality project. The SHA advises it would have relied on subsection 27(4)(k)(ii) of HIPA to disclose personal health information to the researchers from SCM. However, my concern is the disclosure of personal health information by eHealth from its system, the Viewer. To be clear, beyond the scope of my office's investigation is:

- if the SHA had authority to disclose personal health information to the two researchers from its system SCM, and
- if the researchers had the authority to collect personal health information from the SCM.

[14] Dr. D and Dr. K accessed personal health information in the Viewer for the purpose of research. Subsection 29(1) of HIPA provides that a trustee, such as eHealth, may disclose personal health information for research purposes with the express consent of the subject individual. There is no evidence that the subject individuals provided express consent for the research. Therefore, subsection 29(1) of HIPA does not authorize eHealth to disclose personal health information.

[15] Where consent of subject individuals cannot be obtained, subsection 29(2) of HIPA sets out requirements that must be met by the trustee prior to disclosing personal health information. Subsection 29(2) of HIPA provides:

> 29(2) Where it is not reasonably practicable for the consent of the subject individual to be obtained, a trustee or designated archive may use or disclose personal health information for research purposes if:
>
> > (a) the research purposes cannot reasonably be accomplished using de-identified personal health information or other information;
> >
> > (b) reasonable steps are taken to protect the privacy of the subject individual by removing all personal health information that is not required for the purposes of the research;

> (c) in the opinion of the research ethics committee, the potential benefits of the research project clearly outweigh the potential risk to the privacy of the subject individual; and
>
> (d) all of the requirements set out in clauses (1)(a) to (c) are met.

[16] Since the researchers were supposed to obtain personal health information from the SHA's system, SCM, instead of the eHealth's Viewer, eHealth did not meet the requirements of subsection 29(2) of HIPA to disclose the personal health information. I find that privacy breaches occurred because there was no authority in HIPA for the disclosure of personal health information from the Viewer.

[17] Since there was no authority for the disclosure of personal health information from the Viewer, then I find there was no authority for the researchers to have collected the personal health information from the Viewer.

[18] I note that the Principal Investigator of the research team had sought operational approval from the SHA to conduct research using personal health information stored in SCM. Again, the scope of my office's investigation does not include analyzing whether or not the researchers had authority to collect personal health information from SCM.

3. Were the privacy breaches properly managed?

[19] When privacy breaches have 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.

[20] Below is an analysis of each step.

Step 1: Contain the breach

[21] The first step to 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.

[22] On May 16, 2018, eHealth suspended Dr. D, Dr. K, and Dr. Ss' Viewer accounts. On May 18, 2018, eHealth reactivated the accounts after the three physicians received privacy training from the U of S' College of Medicine.

[23] On May 31, 2018, Dr. D indicated to eHealth that she and Dr. K had deleted the personal health information they obtained from the Viewer. Further, the U of S confirmed to my office, in letters dated October 15, 2018, that both Dr. D and Dr. K deleted the personal health information they obtained from the Viewer.

[24] I find that eHealth has made efforts to contain the privacy breach.

[25] In the future, if eHealth determines a researcher (or any other person) has inappropriately obtained information from the Viewer, I recommend that eHealth require the researcher return to it the personal health information. This will enable eHealth to know precisely what personal health information was inappropriately obtained. Then, it should require the researcher to sign a written declaration indicating that he or she has deleted or destroyed all copies of the personal health information and no longer possesses a copy of the information in any form.

[26] Further, eHealth should also require the researcher to indicate whether he or she disseminated the information any further. If so, eHealth should make efforts to retrieve copies of the personal health information that may have been disseminated.

Step 2: Notify affected individuals

[27] 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.

[28] eHealth did not notify the affected individuals because Dr. D and Dr. K had approval to view the personal health information through other means. Therefore, eHealth's position is there was very little risk to the patients. Also, another reason why eHealth did not notify the affected individuals is that had Dr. D and Dr. K accessed the personal health information through the proper channels, then the access would have been authorized.

[29] I find that eHealth's reasons for not notifying the affected individuals inadequate. eHealth is the trustee of the Viewer. It has the duty to protect the personal health information. Maintaining the public's trust includes being transparent with affected individuals when their personal health information has been improperly accessed within the Viewer. As noted in the background, the following types of information can be accessed within the Viewer:

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

- Chronic disease information.

[30] Citizens are able to request an audit report from eHealth to see who has accessed their personal health information from the Viewer. Being upfront with the affected individuals that two researchers inappropriately accessed their personal health information and that eHealth has responded to the privacy breach is better than the affected individuals finding out about the privacy breach if and when they obtain their audit report.

[31] I recommend that eHealth notify the 58 individuals who had their personal health information accessed by Dr. D, and the 15 individuals who had their personal health information accessed by Dr. K through Dr. S's Viewer account. I also encourage eHealth to promote more prominently individuals' right to request access to their audit reports.

Step 3: Investigate the privacy breach

[32] The third step in 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.

[33] eHealth investigated the matter and determined the following:

- Dr. D was supposed to use her SCM research account to obtain personal health information of the 58 patients testing positive for the particular illness for the research project. However, she was having issues with SCM so she used the Viewer instead.

- Dr. K was returning from a leave so she was waiting to have her SCM research account reactivated. eHealth reported that while she waited to have her SCM research account reactivated, Dr. K used Dr. S's Viewer account to obtain personal health information of patients testing positive for the particular illness for the research project.

[34] The U of S also investigated this matter and determined the following:

- Dr. D had difficulty accessing her SCM research account. She assumed she could use SCM and the Viewer interchangeably so she used the Viewer. She indicates she now knows her assumption is incorrect and that the Viewer can only be used for direct patient care.

- Dr. K was on leave so her SCM research account and Viewer account were suspended. However, she had an impending deadline for a research project. Therefore, she used Dr. S's Viewer account.

- Dr. S did not know that the Viewer was not to be used for research. He knew that Dr. K had approval to access SCM for research. He did not know the difference between SCM and the Viewer so he shared his login information with Dr. K so she could gather data to meet her research deadline. He now realizes the difference between SCM and the Viewer and knows that the Viewer is not to be used for research purposes.

[35] Based on eHealth and the U of S' investigations, it appears that the root cause is not knowing that SCM and the Viewer cannot be used interchangeably. Further, in Dr. K and Dr. Ss' case, not understanding you cannot share logins and passwords appears to be a root cause.

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.

[37] As already noted, eHealth suspended the Viewer accounts of the three physicians until they received privacy training from the U of S' College of Medicine.

[38] Also, in its investigation report, eHealth would do the following:

1) Create acknowledgement to remind Viewer users of appropriate use. The user must agree to the acknowledgement the next time the user logs in.
2) Update the Viewer Joint Service/Access Policy and the Authorized Health Purpose.
3) Develop standard protocol for future high profile cases.
4) Develop a communication plan to educate Viewer users on appropriate collection, use and disclosure of Viewer data.

[39] I find that the above four steps for prevention are appropriate. I also recommend to eHealth the following:

a. 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.
b. Conduct regular monthly audits on Dr. D, Dr. K, and Dr. S to ensure they are using the Viewer in accordance with HIPA and the JSAP for a period of at least three years.
c. Develop a system of conducting random audits on resident physicians to ensure they are using the Viewer in accordance with HIPA and the JSAP.
d. Remove PGME as an Authorized Provider Organization.
e. Require medical residents to select the organization with which they are completing their residency as the Authorized Provider Organization, and not PGME. This is because the organization with which they are completing their resident has custody or control over the personal health information that the resident will manage, not PGME.

[40] The U of S indicated to my office that it will address the lack of understanding of the difference between SCM and the Viewer. In November 2018, the Privacy Officer met with PGME to discuss privacy in general and specific areas such as the Viewer. She has also met and intends to meet with SHA's Executive Director of Privacy and Health Information Management to discuss gaps and improvements in privacy training. I find that the U of S' efforts are appropriate. I recommend that the U of S continue its efforts in working with PGME and the SHA in improving privacy training delivered to medical residents.

IV FINDINGS

[41] I find that HIPA is engaged.

[42] I find that privacy breaches occurred because there was no authority for eHealth to have disclosed the personal health information because the doctors had no authority to collect it.

[43] I find there was no authority for the researchers to have collected the personal health information from the Viewer.

[44] I find that eHealth has made efforts to contain the privacy breach.

[45] I find that eHealth's reasons for not notifying the affected individuals to be inadequate.

[46] I find that a root cause of the privacy breaches is the researchers not knowing the SCM and the Viewer cannot be used interchangeably.

[47] I find that a root cause of some of the privacy breaches is Dr. K and Dr. S not understanding that you cannot share logins and passwords.

[48] I find that the action taken (or will be taken) by eHealth as described at paragraph [38] to be appropriate.

V RECOMMENDATIONS

[49] In the future, if eHealth determines a researcher (or any other person) has inappropriately obtained information from the Viewer, I recommend that eHealth:

- require the researcher return to it the personal health information,
- require the researcher to sign a written declaration indicating that he or she has deleted or destroyed all copies of the personal health information and no longer possesses a copy of the information in any form.

[50] I recommend that eHealth notify the 58 individuals who had their personal health information accessed by Dr. D, and the 15 individuals who had their personal health information accessed by Dr. K through Dr. S's Viewer account.

[51] I recommend to eHealth the following:

a. 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.

b. Conduct regular monthly audits on Dr. D, Dr. K, and Dr. S to ensure they are using the Viewer in accordance with HIPA and the JSAP for a period of at least three years.
c. Develop a system of conducting random audits on resident physicians to ensure they are using the Viewer in accordance with HIPA and the JSAP.
d. Remove PGME as an Authorized Provider Organization.
e. Require medical residents to select the organization with which they are completing their residency as the Authorized Provider Organization, and not PGME.

[52] I recommend that the U of S continue its efforts in working with PGME and the SHA in improving privacy training delivered to medical residents.

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

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