Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 308-2017, 309-2017, 310-2017

eHealth Saskatchewan
University of Saskatchewan
Saskatchewan Health Authority

June 4, 2018

Summary: Through an audit, the Saskatoon Regional Health Authority (SRHA) determined that an employee of the College of Medicine at the University of Saskatchewan (U of S) had inappropriately accessed her mother's, a coworker's, and a deceased individual's personal health information in eHealth Saskatchewan's electronic Health Record (eHR) Viewer. The Information and Privacy Commissioner (IPC) made a number of findings and recommendations, including that eHealth, Saskatchewan Health Authority (SHA), and the U of S forward their investigation files to the Ministry of Justice, Public Prosecutions Division to allow prosecutors to further consider whether an offence has occurred and if charges should be laid under HIPA or any other statute.

I BACKGROUND

[1] In October 2017, the Saskatoon Regional Health Authority (SRHA) conducted an audit of a user's (Person X) accesses of personal health information in eHealth Saskatchewan's (eHealth) electronic Health Record (eHR) Viewer. The eHR Viewer enables users to access patient information such as the following:

- laboratory results,
- medication information,
- immunization information,
- discharge summaries,
- medical imaging reports,
- clinical encounters,
- structured medical records, and

- chronic disease information.

[2] SRHA determined that Person X, who was a clerical assistant at the University of Saskatchewan's (U of S) College of Medicine (the College), had inappropriately accessed her mother's personal health information through the eHR Viewer on numerous occasions. SRHA reported the matter to eHealth. eHealth determined that Person X had accessed her mother's personal health information on 38 distinct days for a total of 719 events between July 2017 and October 2017. In addition, SRHA and eHealth determined that Person X had also accessed two other individual's personal health information when those two individuals were not patients of the SRHA at the time that their personal health information was accessed. One was a co-worker of Person X and the other is an individual who has been deceased since 2003. There is no apparent relationship between Person X and the deceased individual.

[3] SRHA also reported the matter to the U of S' Privacy Officer. The U of S investigated the matter, including interviewing Person X. Person X indicated that she had accessed her mother's personal health information because she had concerns regarding the quality of care her mother was receiving. Further, Person X indicated she accessed a co-worker's personal health information because her co-worker had requested Person X to do so. As for the deceased individual, Person X indicated she did not recall the reason why she looked up that particular person's personal health information. She said that if a document such as a fax arrives at the department but it is not clear as to which physician the document is for, she will look up the patient to see which physician to whom she should route the document.

[4] It should be noted that SRHA was merged with the other regional health authorities in the province to form the Saskatchewan Health Authority (SHA) effective December 4, 2017. Therefore, SHA has inherited the responsibility for responding to this privacy breach.

Who is Person X?

[5] Person X was a clerical assistant within the College at the U of S.

[6] In an email dated January 19, 2018, the U of S indicated that Person X's job duties included providing clerical support to a physician who is a faculty member of the College but also had a clinical practice at the Royal University Hospital (RUH).

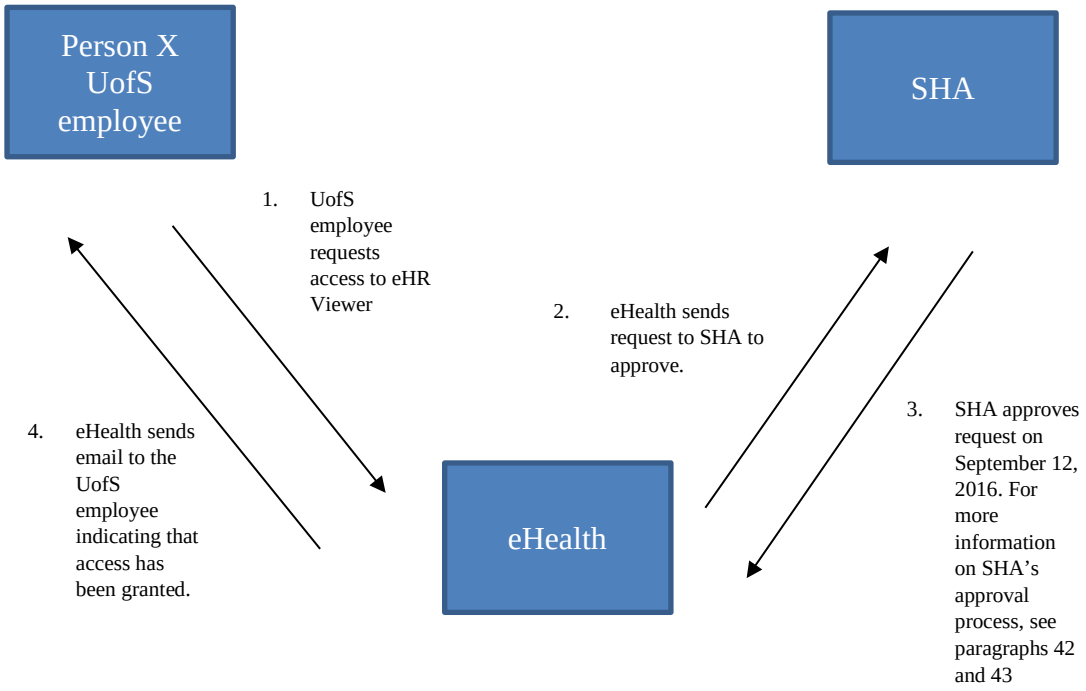
[7] Initially, at the beginning of my office's investigation, there was confusion over who was the employer of Person X. Based on the above, it appears that Person X is an employee of the U of S. However, she had to access personal health information of patients registered at the RUH to fulfill her job duties. The RUH was a part of the SRHA, now the SHA, not the U of S. If she is an employee of the U of S, then it is confusing as to why she had access to personal health information of patients of the SRHA. Further, to add to the confusion, she provided support to a physician who is a faculty member of the College but who is also a practitioner at the SRHA, now SHA. Therefore, there was question about whether or not Person X was in fact an employee of the physician. This confusion represents the lack of accountability for Person X's accesses to the eHR Viewer. Ultimately, as it will be discussed later in this report, my office determined that Person X is an employee of the U of S. She is no longer at the College but is still a U of S employee.

How did Person X gain access to the eHR Viewer?

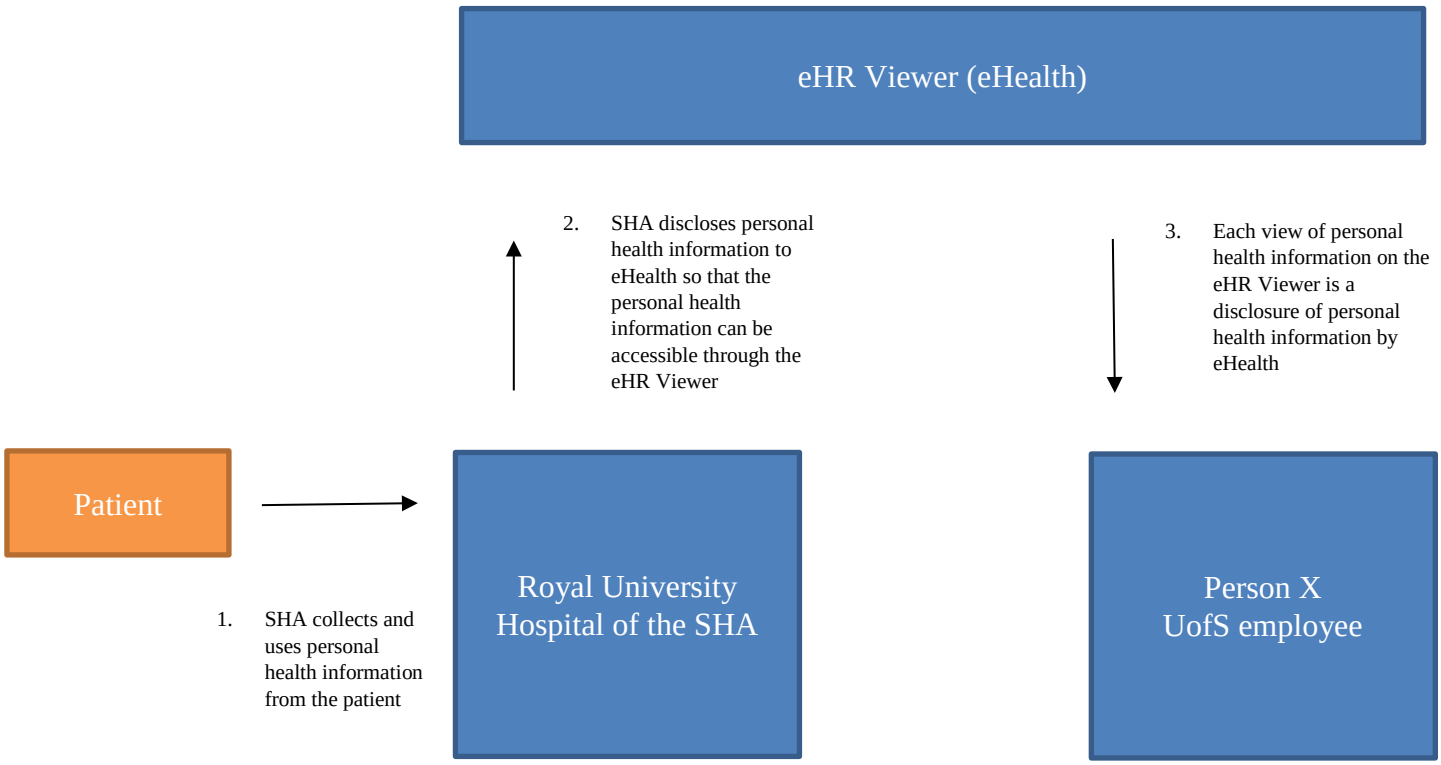
[8] In order for an individual to register for a user account to gain access to the eHR Viewer, he or she must register for a "myeHealth Account" at https://services.ehealthsask.ca/myehealth/pages/selfService/register.xhtml. He or she must then identify the "Authorized Provider Organization" (APO) with whom he or she is associated. An APO is an organization approved by eHealth to have access to personal health information stored within the electronic health record. Within each APO, there is an "Authorized Approver" that reviews applications for a user account. The Authorized Approver will then either approve or decline the application.

[9] In this case, on August 26, 2016, Person X applied for a user account to access the eHR Viewer through the SRHA. On September 12, 2016, SRHA's Authorized Approver approved Person X's application. On September 19, 2016, eHealth sent an email to Person

X indicating that she had been granted access to the eHR Viewer. Below is a diagram depicting how Person X gained user access to the eHR Viewer.



A diagram depicting the flow of information



II DISCUSSION OF THE ISSUES

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

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

[11] For the first element, there are two trustees present. eHealth is a trustee as defined by subsection 2(t)(i) of HIPA and SRHA, now SHA is a trustee as defined by subsection 2(t)(ii) of HIPA. The U of S is not a trustee under HIPA.

[12] For the second element, Person X viewed information such as medication and laboratory results. Such information qualifies as personal health information as defined by subsection 2(m) of HIPA.

[13] For the third element, individuals are registered as patients of the SRHA, now SHA. SHA collects and uses the personal health information for the purpose of providing care. I find that SRHA had, and now SHA, custody or control over personal health information.

[14] In addition, eHealth is responsible for creating a comprehensive health record with respect to individuals, pursuant to section 18.1 of HIPA. This comprehensive health record contains personal health information that is provided by trustees (including SHA) pursuant to subsection 18.1(2)(a) of HIPA, which can be viewed through the eHR Viewer. eHealth is a trustee that has custody and control of the personal health information within this comprehensive health record.

[15] I find that HIPA is engaged.

2. Is *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP) engaged?

[16] The U of S qualifies as a "local authority" as defined by subsection 2(f)(xi) of LA FOIP. LA FOIP deals with personal information, not personal health information. Subsection 23(1) of LA FOIP defines personal information as follows:

> 23(1) Subject to subsections (1.1) and (2), "personal information" means personal information about an identifiable individual that is recorded in any form, and includes:
>
> ...
>
> (c) information that relates to health care that has been received by the individual or to the health history of the individual;

[17] I also note that subsection 23(1.1) of LA FOIP provides that where a local authority is also a trustee under HIPA, "personal information" does not include information that constitutes personal health information under HIPA. Section 23(1.1) provides:

> 23(1.1) On and after the coming into force of subsections 4(3) and (6) of *The Health Information Protection Act*, with respect to a local authority that is a trustee as defined in that Act, "personal information" does not include information that constitutes personal health information as defined in that Act.

[18] Since the U of S is a local authority but not a trustee, I find that only LA FOIP is engaged but not HIPA.

3. Was there authority under HIPA or LA FOIP for Person X's access to her mother's, co-worker, and the deceased individual's information?

[19] eHealth is the trustee for the eHR Viewer. Whenever a user of the eHR views personal health information in the eHR Viewer, eHealth is disclosing personal health information. Personal health information must only be disclosed in accordance with HIPA. Otherwise, the disclosure would qualify as a privacy breach. I find that there was no authority under HIPA for Person X to access her mother's and coworker's personal health information in the eHR Viewer.

[20] Further, when a user uses information from the eHR Viewer, the view would qualify as a collection. Since Person X is an employee of the U of S, then I must determine if there was authority under LA FOIP for the viewing, or collection, of personal information under LA FOIP. The U of S is a local authority subject to LA FOIP. As such, the U of S must only collect personal information pursuant to section 24 of LA FOIP, which provides:

> 24 No local authority shall collect personal information unless the information is collected for a purpose that relates to an existing or proposed program or activity of the local authority.

[21] I find that there was no authority under LA FOIP for Person X to have collected personal information from the eHR Viewer regarding her mother. This is because the RUH is a part of the SHA. Patients register at the RUH to receive care. Therefore, the provision of care within the SHA is a program or activity of the SHA, not of the U of S.

[22] In its response to my office's draft report, the U of S disagreed with my office finding that there is no authority under LA FOIP for the collection of personal information. It asserted that it is a mistake of fact to find that the provision of health care is not a program or activity of the U of S and that the collection of health information is not authorized. It provided my office with a copy of an affiliation agreement it has with the SRHA, now the SHA. Under the affiliation agreement, there is a subsidiary agreement that was made effective

September 1, 2016. This subsidiary agreement explicitly states that the SRHA, has exclusive responsibility over and authority for patient care and treatment. Article 3 of the subsidiary agreement provides the following:

> The parties recognize that the RHA has exclusive responsibility over and authority for the care, treatment and safety of all patients in the RHA facilities, and for the RHA facilities, and that patient care responsibilities supersede all others.

[23] Based on the subsidiary agreement, the provision of care within the SHA is a program or activity of the SHA, and not the U of S. I find that there is no authority under LA FOIP for Person X to have collected her mother's personal information from the eHR Viewer.

4. Has this privacy breach been contained?

[24] To contain a breach is to recover personal information that may have been lost or stopping an unauthorized practice. In this case, to contain the privacy breach was to either suspend or terminate Person X's access to the eHR Viewer.

[25] eHealth indicated to my office that on October 26, 2017, SRHA had requested that Person X's access to the eHR Viewer be removed. eHealth complied with that request and revoked Person X's access that same day. Further, eHealth added Person X and Person X's mother to eHealth's "watch list". This means that if Person X accesses a patient eHR Viewer profile, eHealth's Privacy, Access and Patient Safety Unit will receive email notification of the access. It also means that if Person X's mother's eHR Viewer profile is accessed, the Privacy, Access and Patient Safety Unit will also receive email notification of the access.

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

5. Has notification been provided to affected individuals?

[27] Notifying affected individuals that her personal health information or personal information has been accessed inappropriately is important so that she can take necessary steps to protect herself. A notification should include the following elements:

- A description of what happened,
- A detailed description of the personal 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,
- Recognition of the impacts of the breach on affected individuals and an apology.

[28] In this case, there are three affected individuals: 1) Person X's mother, 2) Person X's co-worker, and 3) the deceased individual. For obvious reasons, the deceased individual was not notified of the privacy breach.

[29] As for Person X's mother, eHealth indicated that Person X's mother was made aware of the privacy breach when a client service representative (CSR) contacted the mother to seek consent into investigating Person X's concerns over the mother's care.

[30] For Person X's co-worker, eHealth indicated that the co-worker was already aware of Person X's viewing her personal health information.

[31] Unless there are compelling reasons not to do so, my office recommends that notification is sent to affected individuals. Therefore, I recommend that eHealth notify Person X's mother and co-worker of this privacy breach. The notification should have the elements listed at paragraph [27]. Even if Person X's mother and co-worker are aware of this privacy breach, a notification from eHealth would signal to both of them that such accesses are unauthorized by HIPA. If Person X's co-worker did indeed request that Person X access her personal health information in the eHR Viewer, the notification may discourage the co-worker from making such requests.

6. Did eHealth and SHA both meet its duty to protect pursuant to section 16 of HIPA?

[32] Section 16 of HIPA imposes a duty to protect personal health information upon trustees. Since both eHealth and SHA are trustees, both 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.

[33] In order to make a finding as to whether or not eHealth and SHA have met its duty to protect personal health information pursuant to section 16 of HIPA, I need to review the administrative safeguards that eHealth and SHA have in place to control access to the eHR Viewer. Paragraphs [34] to [44] are a description of safeguards each of the trustees has in place to protect personal health information in the eHR Viewer. Following the description is an analysis to determine if the duty to protect pursuant to section 16 of HIPA has been met.

a. eHealth

i. Joint Services/Access Policy (JSAP)

[34] The JSAP is an agreement between eHealth and APOs. APOs are provider organizations approved by eHealth to access or receive data stored within the Electronic Health Record. This includes data accessible through the eHR Viewer. A copy of the JSAP can be located on eHealth's website at https://www.ehealthsask.ca/services/ehr-viewer/Documents/eHR%20Viewer%20Joint%20Service%20and%20Access%20Policy.pdf.

[35] The JSAP sets out that eHealth is the trustee for the eHR Viewer, but it also outlines the responsibilities of the APOs. My understanding is that eHealth relies on APOs to review and approve/reject requests for user access to the eHR Viewer. According to the JSAP, APOs have a number of responsibilities, including:

- appointing an employee to be the Authorized Approver within the APO who is responsible to manage and designate users and user roles with the eHR Viewer (subsection 5.1.2 (b) of JSAP),
- ensuring all users that they authorize have completed the necessary training on how to use the eHR Viewer, privacy and security training, and have signed a confidentiality oath or agreement (subsections 5.1.2(g) and 5.1.2(h) of JSAP).

[36] Also, section 5.4 of the JSAP explicitly states that APOs and their authorized users are only to collect and use data on a need-to-know basis for an "Authorized Health Purpose", which is to support and or provide care to the patient to whom the information relates. Section 5.4 of the JSAP provides as follows:

> **Limiting Collection and Use.** The APOs and their authorized Users may only collect and use EHR Data from the EHR Viewer or Integration on a need-to-know basis for the Authorized Health Purpose as per section 5.2. The need-to-know must be supported by the User's relationship to the patient and the specific health services being provided. The APOs shall respect the user roles defined within the EHR Viewer or Integration.

ii. Training Resources for the eHR Viewer

[37] eHealth has made a number of training resources, including documents and videos, for users and Authorized Approvers for APOs on how to use the eHR Viewer available on its website. One training video entitled "Privacy and Security of the eHR Viewer" explicitly states that users are to only access the records of patients the user is directly providing care and treatment to, and they are not to access any other records for any other purpose. Further, the video highlights the offence provision within HIPA by stating that accessing PHI under false pretenses qualifies as a privacy breach and is punishable by a $50,000 fine and imprisonment.

[38] When a user is granted access to the eHR Viewer and logs into the eHR Viewer for the first time, the user must 'accept' the eHR Viewer Training Declaration. This declaration is to confirm that the user has reviewed the eHR training resources on eHealth's website.

[39] Further, the user must also accept the eHR JSAP agreement, which is an agreement where the user agrees to comply with the JSAP. Both the JSAP and the eHR JSAP agreement explicitly states that users must only collect and use personal health information for the sole purpose of supporting and providing a healthcare service to the individual to whom the information relates. The eHR JSAP agreement provides as follows:

> The eHR JSAP agreement must be accepted by users before they log into the eHR Viewer for the first time. It provides as follows:
>
> > By accessing the EHR Viewer you agree to comply with the EHR Joint Service/Access Policy.
> >
> > In this Policy you agree to:
> > - keep the personal health information accessed by you in strict confidence;
> > - collect and use the personal health information for the sole purpose of supporting or providing a healthcare service to the individual to whom the information relates;
> > - only access and use the personal health information on a strict need to know basis to support or provide the healthcare service;
> > - ensure appropriate safeguards are in place within the clinic or facility to protect the security and confidentiality of personal health information;
> > - with eHealth's assistance, ensure that the patient is aware of and has access to all available patient communication material about the eHealth Electronic Health Record Initiative and privacy and patient control options;
> > - allow the patient to have access to and to review their personal health information.

iii. Audits and the Electronic Provincial Privacy Audit and Monitoring (ePPAM) service

[40] eHealth has included an auditing feature in the eHR Viewer that tracks and logs access to personal health information. Section 5.10 of the JSAP provides as follows:

> **Audits.** Access to the EHR Data through the EHR Viewer or Integration will be tracked and logged to protect against inappropriate or improper access or use. Details relating to audit outcomes, reporting and review, including the eHealth Privacy Service's role in:
>
> (a) addressing patient requests for audits of access to their personal health information through the EHR Viewer or Integration; and
>
> (b) addressing requests from APOs for audit logs of their Users;
>
> will be determined by eHealth in its sole discretion.

[41] eHealth also provides the SHA with ePPAM, which is the ability to audit its own employees' access to personal health information in the eHR Viewer.

b. SHA

i. *Work standard – Applying for a Provincial eHR Viewer Account*

[42] As an APO, the SHA needs to have a procedure in place to review and approve/reject requests for access to the eHR Viewer. Prior to the merger of the health regions into the SHA on December 4, 2017, the SRHA had a work standard that described how its provisioned access to the eHR Viewer. It appears that even after the merger of the regional health authorities, this work standard is still being followed.

[43] According to this work standard, managers of departments/units are to instruct employees on how to apply for access to the eHR Viewer, which is a process described at paragraph [8]. Then, managers of departments/units are to send the employee's name, job title, department and facility to the SHA's Director of eHealth. The Director of eHealth will compare the employee's application for access to the eHR Viewer and validate it against the information she received from the managers of departments/units. If the information is validated, then employees are approved for access to the eHR Viewer.

ii. Audits

[44] SHA conducts audits on users' access to the eHR Viewer when it suspects that a user has inappropriately accessed personal health information. In this case, it was able to use the

audit function described at paragraphs [40] and [41] to conduct an audit on Person X's access to the eHR Viewer.

c. Does a gap exist in the safeguards that permitted this privacy breach?

[45] Even though eHealth and SHA have the above safeguards in place, I find that a gap in the safeguards is evident because Person X, an employee of the U of S, was granted user access to the eHR Viewer by the SRHA.

[46] SRHA's process for registering and gaining user access to the eHR Viewer is described at paragraphs [42] to [43]. Person X had registered for user access to the eHR Viewer through eHealth's website. Her manager at the U of S had contacted SRHA's Authorized Approver, to validate Person X's request for user access. Neither the U of S nor the SRHA were able to provide my office with a copy of the email sent by the U of S manager to SRHA's Authorized Approver. The U of S indicated that the manager may have contacted SRHA's Authorized Approver by telephone.

[47] Nothing prevents SHA from approving individuals who are not a SHA employee or contractor to access the eHR Viewer. However, this is a problematic practice since SHA is not able to hold non-employees accountable if they misuse their user privileges. Since Person X is not an employee of the SHA, it would be impossible for SHA to fulfill its responsibilities under the JSAP, including ensuring that Person X received appropriate training pursuant to subsection 5.1.2(g) of the JSAP and that she signed a confidentiality oath or agreement pursuant to subsection 5.1.2(h) of the JSAP. Further, since SHA is not Person X's employer, it is unable to discipline Person X for misusing her user privileges.

[48] I find that a gap in safeguards permitted SRHA (which is now a part of the SHA) to approve non-SRHA (or non-SHA) employees or contractors for access to the eHR Viewer. This gap prevented SRHA (and now SHA) from fulfilling its responsibilities under the JSAP.

[49] In its response to my office's draft report, SHA indicated that developing an agreement between it and the U of S that would outline the process of handling a privacy breach could help resolve the issue of the SHA not being able to hold a U of S employee responsible for

a privacy breach. I recommend that SHA work towards an agreement with the U of S so that the SHA can fulfill its responsibilities under the JSAP.

7. Are SHA and eHealth taking appropriate steps to prevent similar privacy breaches?

[50] SHA indicated that it has taken the following steps to prevent a similar privacy breach from occurring:

- Conducted an audit on Person X's access to the eHR Viewer, and
- Reported the inappropriate accesses made by Person X to eHealth and requested that eHealth remove Person X's access to the eHR Viewer.

[51] I find that the above steps are appropriate. In addition to the above steps, I recommend that SHA stop authorizing requests for user access from any person without an established relationship with the SHA. This would mean refusing requests from non-SHA employees, contractors or physicians that do not have practicing privileges granted to them by SHA. I recommend that SHA ensure that it has an established relationship with the person prior to approving the individual's request for user access to the eHR Viewer.

[52] I recommend that SHA review all the users it has approved to date and terminate the access of users who do not have an established relationship with the SHA. This would mean refusing requests from non-SHA employees, contractors or physicians that do not have practicing privileges granted to them by SHA.

[53] eHealth indicated that it has taken or will be taking the following steps to prevent a similar privacy breach from occurring:

- Removed Person X's access to the eHR Viewer,
- Are monitoring Person X's mother's eHR Viewer profile,
- Ensured that the eHealth Privacy, Access and Patient Safety Unit is notified if Person X regains access to the eHR Viewer,
- It is in the process of updating the JSAP to state users should not be viewing the personal health information of themselves, family members, friends, acquaintances, co-workers, public figures and any other person for purposes

unrelated to their duties. At the time of writing this report, the JSAP is being reviewed internally by eHealth.

- Placing a pop-up reminder to remind eHR Viewer users of the appropriate use of the eHR Viewer. Once the pop-up reminder is implemented, the next time a user logs in, he or she will receive the pop-up reminder and will need to accept the reminder in order to continue. eHealth will be tracking and logging the acceptance of the pop-up.

[54] I find that the above steps are appropriate. In addition to the above steps, I recommend that eHealth configure the eHealth Viewer to require users to review the training resources on its website and accept the eHR Viewer Training Declaration at least once a year. Also, I recommend that eHealth require users to review the JSAP and accept the eHR JSAP agreement once a year.

[55] Finally, in the course of this investigation, my office recommended that eHealth ensure that APOs are only approving its own employees or contractors prior to granting access to the eHR Viewer. In its response to my office's draft report, eHealth indicated that it relies on Authorized Approvers at APOs to only approve users who are employees or contractors. Therefore, eHealth is exploring options to remind Authorized Approvers that they should only approve users who are employees or contractors. One option eHealth is exploring is adding messaging in the communications Authorized Approvers receives when there is a new request for access and when they go to approve or reject requests. I commend eHealth's efforts. I recommend that eHealth implement such reminders.

8. Should U of S' College employees have access to the eHR Viewer?

[56] As I found earlier, the U of S is not a trustee under HIPA. Further, I found that the U of S does not have authority to collect personal information from eHR Viewer under LA FOIP. Therefore, I find that U of S' College employees who do not have an established relationship with the SHA (e.g. a non-SHA employee, contractor, or a physician with practicing privileges granted by SHA) should not have access to the eHR Viewer. It is alarming that Person X, as an employee of the U of S with no established relationship with the SHA, was accessing the eHR Viewer.

[57] The U of S indicated to my office that its College is undergoing restructuring that will result in the College having significantly fewer administrative staff providing support in a clinical setting. The restructuring will require members of the clinical faculty to be responsible for arranging for their own support staff. In other words, it would not be U of S employees who will be providing support to physicians in a clinical setting. I find this restructuring and requiring physicians (who are members of the clinical faculty) to arrange for their own support staff to be an appropriate change.

[58] As stated, the College will have significantly fewer administrative staff providing support in a clinical setting. This suggests that it will still have some of its employees accessing patient information and records. If this is the case, I recommend the U of S explore arrangements so that its clerical/administrative employees do not have access to patient records or access to the eHR Viewer. If its employees require access to the eHR Viewer, then those employees must have an established relationship with the APO (such as becoming an employee or contractor of the APO) prior to requesting access to the eHR Viewer. If the APO is the SHA, and the U of S employee needing access is a physician, then that physician should have practicing privileges granted by SHA prior to being given access to the eHR Viewer. This is so that the APO can hold the employee accountable if the employee/contractor/practitioner inappropriately accesses personal health information in the eHR Viewer.

[59] In its response to my office's draft report, SHA expressed concern over physicians being the APO and being their own Authorized Approver for the eHR Viewer. It said such a change would only shift the responsibility of snooping to physicians but not necessarily reduce or eliminate snooping. I appreciate SHA's concerns especially since it has a duty pursuant to section 16 of HIPA to protect the personal health information in its custody or control, which includes personal health information that is accessible through the eHR Viewer. My office, however, does not have control over how the U of S restructures itself or how physicians themselves arrange for their own administrative support staff. If physicians and their employees need to access personal health information in the custody or control of the SHA in the eHR Viewer, I recommend that the SHA explore the possibility of establishing agreements with physicians that they and their staff will access personal

health information in accordance with HIPA. The agreement should also establish that the physician will cooperate with an investigation by the SHA if the SHA detects a privacy breach and to follow any recommendations by the SHA to discipline administrative staff when caught inappropriately accessing personal health information. The agreement should also specify that the SHA may report the privacy breach to eHealth (if it involves the eHR Viewer), and to my office.

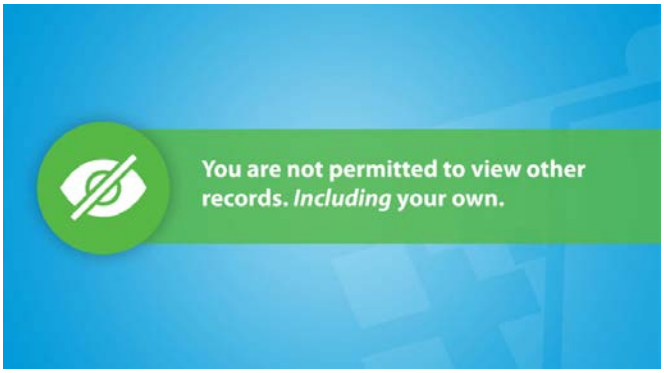
9. Do the offence provisions in HIPA apply to this matter?

[60] Accessing information stored within the eHR Viewer for reasons beyond performing job duties is inappropriate. If legitimate users of the eHR Viewer were permitted to access any person's personal health information without a need-to-know, then patients' trust in the confidentiality of their personal health information would be undermined. The consequences include individuals avoiding seeking treatment or care, or they may be compelled to withhold or falsify information. Upholding patients' trust means upholding the integrity of the health care system.

[61] Users of the eHR Viewer should not regard their access privileges as a perk to satisfy their own curiosity, to meet their own personal needs, or as a benefit or convenience to family, friends, and/or colleagues. Users of the eHR Viewer must still submit a formal access to information request pursuant to Part V of HIPA if they wish to receive access to personal health information – which is a right afforded to all Saskatchewan citizens under HIPA. Users of the eHR Viewer are not the winners of a two-tiered system where they can help themselves to any personal health information while others have to undertake the task of submitting a formal access to information request under HIPA to gain access to personal health information.

[62] As noted earlier, Person X accepted the eHR JSAP Agreement on April 12, 2017, which required Person X to only collect and use the personal health information for the sole purpose of supporting or providing a healthcare service to the individual to whom the information relates. Furthermore, Person X accepted the eHR Viewer Training Declaration that same day, which is confirmation she reviewed and completed the eHR Viewer training

resources on eHealth's website, which includes the "Privacy and Security of the eHR Viewer". At the 41 second mark of the video, the video's narration states that by agreeing to the JSAP, users are agreeing to only accessing the eHR Viewer records of patients who they are providing direct care and treatment to, and that users are not permitted to view anyone else's records, including their own. Below is a screenshot of the video, which is in plain language:



[63] According to the U of S, Person X asserted that she had the consent of both her mother and her colleague to access their information on the eHR Viewer. Person X accessed her mother's personal health information because she was concerned about the quality of care her mother was receiving. She accessed her colleague's personal health information because the colleague asked her to do so. I find that these two reasons suggests that Person X was not involved in providing a healthcare service to her mother or to her colleague. She accessed her mother and her colleague's personal health information even though she had agreed not to. She did it anyway.

[64] Further, at the one minute and 12 second mark, eHealth's video "Privacy and Security of the eHR Viewer" users are informed that unauthorized accesses to personal health information are considered privacy breaches and is punishable by a $50,000 fine and imprisonment. The following is a screenshot of the video, which is in plain language:

[65] Subsections 64(1) and 64(2) of HIPA provides as follows:

> 64(1) No person shall:
>
> > (a) knowingly contravene any provision of this Act or the regulations;
> > …
> > (f) obtain another person's personal health information by falsely representing that he or she is entitled to the information.
>
> 64(2) Every person who contravenes subsection (1) or (1.1) is guilty of an offence and is liable on summary conviction:
>
> > (a) in the case of an individual, to a fine of not more than $50,000, to imprisonment for not more than one year or to both; and
> >
> > (b) in the case of a corporation, to a fine of not more than $500,000.

[66] Even though Person X accepted and agreed to the JSAP and the eHR Viewer Training Declaration, she still accessed personal health information in the eHR Viewer without a legitimate need-to-know.

[67] I recommend that eHealth, SHA, and the U of S forward their investigation files to the Ministry of Justice, Public Prosecutions Division to allow prosecutors to further consider whether an offence has occurred and if charges should be laid under HIPA or any other statute.

III FINDINGS

[68] I find that HIPA is engaged.

[69] I find that LA FOIP is also engaged.

[70] I find that there was no authority under HIPA for Person X to have accessed her mother's or co-worker personal health information in the eHR Viewer.

[71] I find that there was no authority under LA FOIP for Person X to have the collected personal information from the eHR Viewer.

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

[73] I find that a gap in safeguards permitted SRHA (now SHA) to approve non-SHA employees or contractors for access to the eHR Viewer.

[74] I find that U of S' College employees who do not have an established relationship with the SHA (e.g. a non-SHA employee, contractor, or a physician with practicing privileges granted by SHA's Board of Directors) should not have access to the eHR Viewer.

[75] I find that eHealth has taken appropriate steps to prevent similar privacy breaches from occurring.

[76] I find that SHA has taken appropriate steps to help prevent similar privacy breaches from occurring.

IV RECOMMENDATIONS

[77] I recommend that eHealth notify Person X's mother and co-worker of this privacy breach. The notification should have the elements listed at paragraph [27].

[78] I recommend that eHealth configure the eHR Viewer to require users/managers to review the training resources on its website and accept the eHR Viewer Training Declaration at least once a year.

[79] I recommend that eHealth require users to review the JSAP and accept the eHR JSAP agreement once a year.

[80] I recommend that eHealth implement reminders to Authorized Approvers to only approver users that have an established relationship with the APO, such as being under the APO's employ or contract.

[81] I recommend that eHealth ban Person X from having access to the eHR Viewer indefinitely.

[82] I recommend that SHA works towards an agreement with the U of S so that it (the SHA) can fulfill its responsibilities under the JSAP, as described at paragraph [49].

[83] I recommend that SHA stop authorizing requests for user access from any person without an established relationship with the SHA. That is, non-SHA employees/contractors or physicians that do not have practicing privileges granted to them by SHA.

[84] I recommend that SHA review all the users it has approved to date and terminate the access of users who do not have an established relationship with the SHA. That is, non-SHA employees/contractors or physicians that do not have practicing privileges granted to them by SHA's Board of Directors.

[85] I recommend that SHA ensure that it has an established relationship with an individual (i.e., a SHA employee or contractor) prior to approving the individual's request for user access to the eHR Viewer.

[86] I recommend that the SHA explore the possibility of establishing agreements with physicians that they and their staff if they need to access personal health information in the custody or control over the SHA. The agreement should establish that physicians and their staff will access personal health information in accordance with HIPA. The agreement should also establish that the physician will cooperate with an investigation by the SHA if the SHA detects a privacy breach, and that the SHA may report the privacy breach to eHealth (if it involves the eHR Viewer), and to my office.

[87] I recommend the U of S explore arrangements so that its clerical/administrative employees do not have access to patient records or access to the eHR Viewer.

[88] I recommend that the U of S ensure that if its employees require access to the eHR Viewer, then those employee must have an established relationship with the APO. For example, resident physicians or medical faculty should have practicing privileges approved by SHA prior to requesting access to the eHR Viewer from the SHA. This is so that the SHA can hold the person accountable.

[89] I recommend that eHealth and SHA work together to increase their capacity to conduct audits not only on a reactive-basis but on a proactive and regular basis to prevent inappropriate accesses to personal health information stored on electronic systems.

[90] I recommend that eHealth, SHA, and the U of S forward their investigation files to the Ministry of Justice, Public Prosecutions Division to allow prosecutors to further consider whether an offence has occurred and if charges should be laid under HIPA or any other statute.

Dated at Regina, in the Province of Saskatchewan, this 4th day of June, 2018.

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