Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 203-2019, 214-2019, 257-2019

Saskatchewan Health Authority

October 28, 2020

Summary: The Saskatchewan Health Authority (SHA) investigated Dr. Ashwani Narang (Dr. Narang) and determined that Dr. Narang accessed personal health information in the electronic medical record (EMR) at the Rosetown Primary Care Centre (RPCC) without a professional need-to-know. The SHA proactively reported the privacy breach to the Commissioner. An affected individual also submitted a complaint to the Commissioner and requested that the Commissioner investigate Dr. Narang's accesses to the EMR. The Commissioner made a number of findings, including how *The Health Information Protection Act* did not authorize Dr. Narang's accesses to the EMR and that the SHA's notification of the privacy breaches to the affected individuals did not provide a complete accounting of what occurred. The Commissioner made a number of recommendations, including that the SHA send a revised notification letter to affected individuals and that the SHA conduct monthly audits of Dr. Narang's accesses to the EMR for at least three years.

I BACKGROUND

[1] The relationship between the Rosetown Primary Care Centre (RPCC), the Town of Rosetown (the Town), and the Saskatchewan Health Authority (SHA) was established in 2013 and is complex. First, the building that houses the RPCC was made possible by the Town and the Rural Municipality of St. Andrews No. 287. The staff at the RPCC, such as medical office assistants, are employed by the Town. The physicians are contracted by the SHA. The equipment at the RPCC, including the electronic medical record (EMR), are provided by the SHA. Based on their contracts with the SHA, a portion of the cost associated with the operation of the EMR is billed monthly to the physicians. Further, all staff and physicians at the RPCC all have SHA email addresses and accounts.

[2] In 2013, Dr. Olawale Igbekoyi (Dr. Igbekoyi or "Dr. Franklin") and Dr. Amrish Ramiah (Dr. Ramiah) both signed contracts with the former Heartland Regional Health Authority (HRHA) to provide physician services and other primary health services on behalf of the HRHA. They both also participated in the Saskatchewan Medical Association EMR program that provided incentives for physicians to implement an EMR. The HRHA worked with the RPCC to ensure all of the program requirements were met. This included each Dr. Franklin and Dr. Ramiah signing two separate agreements with the HRHA: 1) *Single Trustee Policy for EMR System at Rosetown Primary Care Clinic,* and 2) *Information Sharing and Clinic Exit Agreement*.

[3] In April of 2018, Dr. Ramiah left the RPCC. In September of 2018, through the Saskatchewan International Physician Practice Assessment (SIPPA) program, Dr. Ashwani Narang (Dr. Narang) joined the RPCC under the supervision of Dr. J.C. Cooper. When Dr. Narang began at the RPCC, Dr. Narang signed a contract with the SHA to provide physician services and other primary health services on behalf of the SHA. However, the SHA did not review the two agreements described in the preceding paragraph with Dr. Igbekoyi nor did the SHA ask Dr. Narang to sign either agreement.

[4] In April of 2019, based on comments made by Dr. Narang, Town employees at the RPCC became suspicious that Dr. Narang had been accessing patients' personal health information in the EMR without a need-to-know. Therefore, an audit into Dr. Narang's activity in the EMR was conducted. The audit revealed that Dr. Narang not only accessed the Town employees' personal health information in the EMR, but also the personal health information of individuals who were not Dr. Narang's patients.

[5] The SHA conducted an investigation into the matter. As part of its investigation, the SHA met with Dr. Narang to ask about the accesses to the patient records in the EMR. Dr. Narang was given a two week period to go into the patient records so that they could refresh their memory as to why they had accessed the patient records. At the conclusion of its investigation, the SHA determined that Dr. Narang had accessed at least 20 individuals'

personal health information without a need-to-know under *The Health Information Protection Act* (HIPA).

[6] In letters dated June 25, 2019, the SHA notified the affected individuals. The letter did not identify Dr. Narang as the snooper. Instead, SHA's letter indicated the snooper was, "an individual at Rosetown Primary Care Centre, who was not involved in your medical care". As a result, any person working at the RPCC, whether as a Town employee or as a SHA contractor, could have been assumed to have been the snooper.

[7] On June 26, 2019, the SHA proactively reported the privacy breach to my office. It reported that a physician at the RPCC had accessed 20 patients' personal health information in the RPCC's EMR without a professional need-to-know. In its initial reporting of the privacy breach to my office, the SHA did not identify the physician to my office.

[8] My office learned the identity of the physician when it received a letter dated July 2, 2019, from Dr. Narang's lawyer. They indicated that Dr. Narang was proactively reporting a privacy breach to my office. In that letter, Dr. Narang's lawyer expressed concerns over an audit that led to the SHA investigating Dr. Narang's access to certain patients' personal health information. Both Dr. Narang and their lawyer requested that my office review the audit and the SHA's investigation.

[9] Since the SHA had already proactively reported to my office, my office advised Dr. Narang's lawyer that we would accept the July 2, 2019 letter as Dr. Narang's representations for the purposes of my office's investigation.

[10] Then, in an email dated July 10, 2019, Dr. Narang's lawyer asserted that they believed that trusteeship lies both with the SHA and Dr. Narang. Dr. Narang's lawyer asserted that it would be appropriate for each party to self-report the privacy breaches. Dr. Narang's lawyer indicated that the letter dated July 2, 2019, does not contain the full extent of Dr. Narang's representations to my office. Dr. Narang's lawyer indicated they were, "requesting further information from SHA for purposes of putting together a detailed response".

[11] My office indicated that if Dr. Narang wished to provide further representations, that they should do so by August 2, 2019. Further, my office indicated that it could not provide an advance ruling on the matter of trusteeship.

[12] However, to resolve the issue of who is the trustee with custody or control over the personal health information in the EMR at the RPCC, my office determined that it should invite both the SHA and Dr. Narang to provide representations on the issue. In other words, who is the trustee with custody or control over the personal health information in the EMR at the Clinic – the SHA, Dr. Narang, or both? Therefore, on July 18, 2019, my office sent emails to both the SHA and Dr. Narang requesting submissions on the issue of trusteeship. My office requested the submissions be provided by August 19, 2019.

[13] Dr. Narang's lawyer provided a submission on August 19, 2019. At the end of the letter, Dr. Narang's lawyer concluded that their understanding is that Dr. Narang will be required to provide information at a future point in time regarding the patients involved in the audit into the EMR.

[14] On August 7, 2020, my office requested Dr. Narang's lawyer provide my office with Dr. Narang's reasons for accessing the patients' personal health information in the EMR. On September 11, 2020, my office received the requested information from Dr. Narang's lawyer.

Complaint from an affected individual

[15] As noted earlier, the SHA had sent letters dated June 25, 2019, to 20 individuals whose personal health information was accessed by Dr. Narang. One of the individuals submitted a complaint to my office regarding this matter. This individual (the Complainant) was one of the Town employees working at the RPCC. Dr. Narang had accessed their personal health information and the personal health information of their family members.

[16] The Complainant, as an administrator of the EMR, conducted the audit and reported this matter to the SHA. The SHA undertook an investigation and the Complainant assisted the SHA in its investigation into the matter.

[17] However, the Complainant raised concerns with my office on how the SHA handled this matter, including the letter it sent to individuals on June 25, 2019. As noted earlier, the SHA did not identify Dr. Narang as the snooper, but its letter said that, "an individual at Rosetown Primary Health Centre, who was not involved in your medical care". This ambiguity resulted in any person working at the RPCC, whether as a Town employee or as an SHA contractor, could have been assumed to have been the snooper. This also resulted in the Complainant and another Town employee working at the RPCC to respond to calls from the individuals affected by Dr. Narang's actions, some of whom were angry after receiving the SHA letters.

[18] The Complainant highlighted the lack of accountability of Dr. Narang. They indicated that as far they were aware, Dr. Narang had not admitted to any wrongdoing or ever offered any apology for their actions. Personally, the Complainant indicated that Dr. Narang had not addressed the matter with them. The Complainant also indicated they were advised by the SHA's Privacy Director that the SHA would not be disciplining Dr. Narang since Dr. Narang was a contractor and not an SHA employee.

[19] Finally, the Complainant described how this matter had strained the working relationships at the RPCC and that it had personal consequences for the Complainant since their family members' personal health information had also been accessed by Dr. Narang without a need-to-know.

Charge by the Council of the College of Physicians and Surgeons of Saskatchewan

[20] The Council of the College of Physicians and Surgeons of Saskatchewan (CPSS) laid a charge against Dr. Narang on September 26, 2020. The charge is as follows:

The Council of the College of Physicians and Surgeons directs that, pursuant to section 47.5 of *The Medical Profession Act, 1981*, the Discipline Committee hear the following charge against Dr. Ashwani Narang:

> You Dr. Ashwani Narang are guilty of unbecoming, improper, unprofessional, or discreditable conduct contrary to the provisions of section 46(o) and/or section 46(p) of *The Medical Profession Act, 1981*, S.S. 1980-81, c. M-10.1, and/or bylaw 8.1(b)(viii), and/or paragraph 31 and/or paragraph 32 and/or paragraph 33 of the Code of Ethics contained in bylaw 7.1 of the bylaws of the College of Physicians and Surgeons of Saskatchewan. The evidence that will be led in support of this charge will include some or all of the following:
>
> 1. During the period December 1, 2018 to March 31, 2019, you accessed the personal health information of a number of individuals (referred to as "the individuals") through the electronic medical record of the Rosetown & District Primary Care Centre;
> 2. At the time of accessing those records, you did not have a physician-patient relationship with the individuals.
> 3. You accessed the personal health information of the individuals without their consent.
> 4. You accessed the personal health information of the individuals without a legitimate need to know the information, and/or you failed to exercise due diligence to ensure you had a legitimate need to know the individuals' personal health information that you accessed.

II DISCUSSION OF THE ISSUES

1. Who is the trustee with custody or control over the personal health information in the EMR?

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

[22] Subsection 2(m) of HIPA defines "personal health information" as follows:

> **2** In this Act:
> ...
> (m) **"personal health information"** means, with respect to an individual, whether living or deceased:

> (i) information with respect to the physical or mental health of the individual;
>
> (ii) information with respect to any health service provided to the individual;
>
> (iii) information with respect to the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual;
>
> (iv) information that is collected:
>
> (A) in the course of providing health services to the individual; or
>
> (B) incidentally to the provision of health services to the individual; or
>
> (v) registration information;

[23] I find that information contained within an EMR would qualify as "personal health information" as defined by subsection 2(m) of HIPA.

[24] Subsection 2(t) of HIPA defines "trustee" as follows:

> **2** In this Act:
> ...
> (t) **"trustee"** means any of the following that have custody or control of personal health information:
> ...
> (ii) the provincial health authority or a health care organization;
> ...
> (xii) a person, other than an employee of a trustee, who is:
>
> (A) a health professional licensed or registered pursuant to an Act for which the minister is responsible;
> ...
> (xiv) a person, other than an employee of a trustee, who or body that provides a health service pursuant to an agreement with another trustee;

[25] The SHA, as the provincial health authority defined by subsection 1-2 of *The Provincial Health Authority Act*, qualifies as a "trustee" pursuant to subsection 2(t)(ii) of HIPA. I should note that subsection 3-2 of *The Provincial Health Authority Act*, provides that the

HRHA has been amalgamated with 11 other health regions to continue as the provincial health authority. This will be relevant later on in this Report.

[26] Dr. Narang's lawyer asserted that Dr. Narang qualifies as a "trustee" pursuant to subsection 2(t)(xii)(A) of HIPA. If Dr. Narang is indeed a trustee pursuant to this particular provision of HIPA, then Dr. Narang must not be an employee of the SHA.

[27] The SHA qualifies as a "local authority" as defined by subsection 2(f)(xiii) of *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP):

> **2** In this Act:
>
> ...
>
> (f) **"local authority"** means:
>
> ...
>
> (xiii) the provincial health authority or an affiliate, as defined in *The Provincial Health Authority Act*;

[28] Dr. Narang's lawyer asserted that Dr. Narang is not an employee of the SHA. The term "employee" is defined by subsection 2(b.1) of LA FOIP as follows:

> **2** In this Act:
>
> ...
>
> (b.1) **"employee"** means an individual employed by a local authority and includes an individual retained under a contract to perform services for the local authority;

[29] The SHA has a contract with Dr. Narang that provides that Dr. Narang is to provide services on behalf of the SHA at the Clinic. Therefore, for the purposes of LA FOIP and for HIPA, I find that Dr. Narang is an "employee" of the SHA. Since Dr. Narang is an employee of the SHA, I find that Dr. Narang is not a trustee pursuant to subsection 2(t)(xii)(A) of HIPA.

[30] I note however that section 5.1 of Dr. Narang's contract with the SHA provides that Dr. Narang is not to be deemed an employee of the SHA for any purpose. It says:

> 5.1 The Contractor is an independent Contractor and shall not be deemed to be an employee of the SHA for any purpose.

[31] This provision within the contract between Dr. Narang with the SHA does not trump LA FOIP or HIPA. If there is any confusion if Dr. Narang is an employee for the purposes of LA FOIP or HIPA, I recommend that the SHA amend its contract with Dr. Narang and any other physician. The amendment should be clear that the physician qualifies as an employee for the purposes of LA FOIP and HIPA.

[32] Dr. Narang's lawyer also cited the agreement entitled *Information Sharing and Clinic Exit Agreement* to support their argument that Dr. Narang is a trustee. This agreement provides:

> 2. Trusteeship.
>
> i) HHR will be in control of who uses the PHI in the single database within the EMR System and will accept the responsibilities of a Trustee under HIPA for the PHI in the database.
>
> ii) The Physician documenting, using or sharing the PHI will accept the responsibilities of a Trustee (Physician-Trustee) under HIPA for the PHI in the database.

[33] The wording of the above provision is confusing as it implies that both the HRHA (now the SHA) and physician are trustees of the personal health information in the EMR. An individual or an organization cannot contract its way into becoming a trustee. I note that the only reference to control is that by the HRHA, not any physician. Even if the agreement provided that Dr. Narang is a "Physician-Trustee", I do not find that Dr. Narang qualifies as a trustee as defined by subsection 2(t) of HIPA. I recommend that the SHA amend the wording of this agreement so that it is clear that the SHA is the trustee with custody or control of the personal health information in the EMR. I also recommend that the SHA amend the agreement so that it sets out the consequences for a physician that breaches HIPA. Physicians should be made aware of the offense provisions set out in HIPA.

[34] In previous reports, my office defined the term "custody" as physical possession with a measure of control. Further, "control" refers to the authority of an organization to manage, even partially, what is done with a record. To demonstrate that it has custody and control over the personal health information in the EMR, the SHA provided my office with the following:

- A license and services agreement between the 1) Optimed Software, the supplier of the EMR, and 2) the Heartland Health Region, Rosetown & District Primary Care Centre, and the Town of Rosetown, collectively referred to as the "Client".

- Schedule 8 of an Electronic Medical Record Solution Agreement between the "Eligible Physician" (Dr. Igbekoyi) and the "Supplier" (Optimed). This agreement is dated February 26, 2013.

[35] Based on a review of the above, I find that it is the HRHA (and now the SHA) has custody or control over the personal health information. As such, I find that the SHA is the trustee with custody or control over the personal health information in the EMR.

[36] Finally, even if I had found that Dr. Narang was a trustee with custody or control over the personal health information in the EMR, HIPA would still apply to this matter. That is, Dr. Narang should only be accessing personal health information in accordance with HIPA. I will continue with my analysis to determine if breaches have occurred.

2. Did privacy breaches occur?

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

[38] When an employee or contractor accesses personal health information, my office considers that as a "use" of personal health information. Subsection 2(u) of HIPA defines "use" as:

> **2** In this Act:
> ...
> (u) **"use"** includes reference to or manipulation of personal health information by the trustee that has custody or control of the information, but does not include disclosure to another person or trustee.

[39] Further, subsection 23(1) of HIPA establishes the need-to-know principle, 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.

[40] Finally, section 26 of HIPA provides when a trustee (or its employees) can use personal health information:

> **26**(1) A trustee shall not use personal health information in the custody or control of the trustee except with the consent of the subject individual or in accordance with this section.
>
> (2) A trustee may use personal health information:
>
> (a) for a purpose for which the information may be disclosed by the trustee pursuant to section 27, 28 or 29;
>
> (b) for the purposes of de-identifying the personal health information;
>
> (c) for a purpose that will primarily benefit the subject individual; or
>
> (d) for a prescribed purpose.

SHA

[41] Following investigating Dr. Narang's accesses in the RPCC's EMR, the SHA reported to my office that it was unable to establish that Dr. Narang had a professional need-to-know the personal health information of the 20 affected individuals. For example, it noted that Dr. Narang had accessed the personal health information of seven individuals of a family for a personal reason. The SHA also asserted that Dr. Narang acknowledged that curiosity contributed to Dr. Narang viewing the personal health information of an SHA employee and a relative of the SHA employee. For the remaining 11 patients, the SHA said Dr. Narang did not provide a reason for accessing the personal health information of those patients. The SHA indicated that Dr. Narang only provided a list of possible reasons for access to the personal health information. As such, the SHA was not able to determine a professional need-to-know for the accesses.

Dr. Narang

[42] Dr. Narang's lawyer identified two circumstances in which Dr. Narang accessed personal health information in the EMR for unauthorized reasons, but asserted that the other accesses were either authorized or due to "technical issues".

a. Unauthorized accesses acknowledged by Dr. Narang

[43] The first of two circumstances in which Dr. Narang's lawyer acknowledged there was unauthorized access to personal health information is when Dr. Narang accessed the personal health information of seven individuals from the same family for a personal reason, which was also reported to my office by the SHA (described above). Dr. Narang's lawyer indicated that Dr. Narang has apologized to the family.

[44] The second circumstance is when Dr. Narang had accessed one other individual's personal health information in order to raise concerns with RPCC staff regarding scheduling practices. Dr. Narang acknowledged that they should not have accessed the individual's personal health information for this reason.

[45] Based on the above, I find that privacy breaches have occurred since personal health information was used for purposes not authorized by HIPA.

[46] Next, I will consider the reasons offered by Dr. Narang's lawyer for Dr. Narang's accesses to other individuals' personal health information.

b. Reasons for other accesses by Dr. Narang

[47] Dr. Narang's lawyer provided reasons why Dr. Narang accessed other personal health information in the EMR, including:

i. Taking on Dr. Ramiah's former patients;

ii. Technical issues that led to Dr. Narang accessing patients' personal health information unintentionally;

iii. Dr. Narang provided care to the patient; and

iv. Dr. Narang was assisting Dr. Franklin.

[48] Below, I will describe Dr. Narang's explanations for each of these other accesses.

i. Taking on Dr. Ramiah's former patients

[49] Dr. Narang's lawyer indicated to my office that Dr. Narang was told that they would be taking on the patients previously seen by Dr. Ramiah. In their letter dated September 11, 2020, Dr. Narang's lawyer said:

> As discussed above, on joining the Clinic, Dr. Narang was told he was responsible for taking over patients previously seen by Dr. Ramiah. Dr. Narang was not provided with a list of Dr. Ramiah's patients; rather, **he was instructed by Clinic staff, including the Clinic Manager, to use the Clinic EMR to identify and review Dr. Ramiah's patients and see if they required follow-up. Dr. Narang would review these charts whenever time permitted. He understood that he should review incoming labs and investigations for Dr. Ramiah's patients, and he could access and open the "Patient Information" tab in the Clinic EMR to determine whether he was assuming care for the patient from Dr. Ramiah or whether the patient had already transferred his or her care to Dr. Franklin on another family physician.**
> …
> Laboratory and investigation results for many of Dr. Ramiah's former patients were directed to Dr. Narang, even though he had yet to see the patients and he did not know their medical history. Dr. Narang would follow the above-noted process; he would review the laboratory and investigation results and other PHI in the Clinic EMR to ensure continuity of care. Logistically-speaking, when the Clinic received laboratory and investigation results for these patients, Dr. Narang was alerted via his inbox in the Clinic EMR. From his inbox, Dr. Narang would link to the laboratory or investigation results and access the patient's other PHI in the Clinic EMR. SHA was advised by Accuro that there is no audit information available for Dr. Narang's inbox in the Clinic EMR. In other words, there is no way to determine whether Dr. Narang was prompted to access a patient's PHI because he received laboratory or investigation results for the patient in his EMR inbox.
>
> [Emphasis added]

[50] Based on the above, Dr. Narang's lawyer argued that Dr. Narang accessed personal health information for two reasons: 1) to identify Dr. Ramiah's patients and see if they required follow-up, "whenever time permitted", or 2) they would be prompted to access personal health information after receiving laboratory and investigation reports for Dr. Ramiah's patients.

[51] Based on information provided to my office by Dr. Narang's lawyer, Dr. Narang accessed the personal health information of the Complainant, two members of the Complainant's

family, a politician, and an SHA employee and the SHA employee's relative for the first reason described in the preceding paragraph. For these six individuals, it does not appear that Dr. Narang was prompted by a laboratory or investigation result to access their personal health information. Instead, Dr. Narang's lawyer explained that Dr. Narang accessed these individuals' personal health information to determine if these individuals were a patient of Dr. Ramiah and if these individuals should be "recalled for follow-up". Dr. Narang's lawyer asserted that subsection 26(2)(c) of HIPA would authorize such accesses because "the access purpose will primarily benefit the subject individual". I disagree that subsection 26(2)(c) of HIPA would authorize such accesses. Even if Dr. Ramiah remained at the RPCC and had provided care to these six individuals, Dr. Ramiah themself would not have had the authority under HIPA to access these six individual's personal health information in the EMR unless there was an need-to-know pursuant to subsection 23(1) of HIPA. Physicians do not have a static entitlement to patients' personal health information. As such, Dr. Narang, who hadn't provided care to these six individuals in the past, would certainly not have authority to access these six patients unless there was a demonstrable need-to-know. What is troubling is one of these six individuals was the Complainant. The Complainant worked in close proximity to Dr. Narang. If Dr. Narang was trying to determine if the Complainant was Dr. Ramiah's patient in the past, then Dr. Narang should have asked the Complainant directly. Further, according to the guideline entitled *Guideline: Treating Employees* established by the CPSS, physicians are discouraged from treating their co-workers. Not only was Dr. Narang's access to the Complainant's personal health information not authorized by HIPA, the access was against CPSS' guideline.

[52] It does not appear that Dr. Narang accessed the personal health information of the six individuals described at paragraph [51] for a purpose that will primarily benefit the subject individual. As such, I find that subsection 26(2)(c) of HIPA, nor any other, authorized Dr. Narang's access to these six individuals' personal health information.

ii. Technical issues that led to Dr. Narang accessing patients' personal health information unintentionally

[53] Dr. Narang's lawyer indicated that "technical issues" may have led to Dr. Narang accessing seven patients' personal health information inadvertently. These seven individuals include an SHA employee, a relative of the SHA employee, and one of the medical office assistants. In their letter dated September 11, 2019, Dr. Narang's lawyer described these technical issues as follows:

- The SHA provided Dr. Narang with a laptop that had not been properly maintained and was in very poor condition; and
- The RPCC's internet connection was "inadequate", which causes problems when accessing the RPCC's EMR. Dr. Narang encountered "a significant time lag" when they used they EMR. There were delays when they clicked on links or scrolled on pages; they would end up navigating to parts of the EMR that they had not intended.

[54] Dr. Narang's lawyer pointed out, in their letter dated September 11, 2020, that the EMR has an "autofill" feature. As a user types characters of a person's last name into the search field in the EMR, the EMR will begin to "autofill" the search field with names corresponding to the typed characters. Dr. Narang's lawyer indicated that if a user accidentally hit enter or clicked on the wrong autofill name, the user can end up accessing the wrong patient chart. They asserted that while the autofill feature is sometimes helpful, it can be problematic when combined with technical issues. Dr. Narang's lawyer identified examples of how legitimate patients of Dr. Narang's had the same or similar last name of the individuals whose personal health information that Dr. Narang inadvertently accessed.

[55] It is difficult to establish precisely what occurred when Dr. Narang accessed these seven individuals' personal health information in the EMR. However, based on a review of the audit log related to the seven individuals, it is also difficult to believe that all accesses were inadvertent due to "technical issues". For example, the audit log showed nine "activities" occurred on the SHA employee's profile on January 28, 2019, over the course of 26 seconds *after* Dr. Narang had viewed a patient of the same last name. If Dr. Narang already had the correct patient's profile already displayed on the EMR, it is difficult to understand why Dr. Narang used the autofill feature of the search function in the EMR to have "accidentally" searched the SHA employee's profile. Similarly, on March 10, 2019, the audit log showed that five activities occurred on the SHA employee's profile over the

course of 12 seconds *after* Dr. Narang had viewed the personal health information of a patient of the same last name. Again, if Dr. Narang had the correct patient's personal health information displayed on the EMR, then it is difficult to understand how the "autofill" feature of the search function contributed to Dr. Narang accidentally pulling up the SHA employee's profile. Also on March 10, 2019, the audit log shows that Dr. Narang viewed the personal health information of a relative of the SHA employee with the same last name *after* Dr. Narang had viewed the personal health information of the patient with the same last name. The audit log showed that five "activities" over 23 seconds occurred on the SHA employee's relative's profile in the EMR.

[56] Further, the audit log showed that Dr. Narang accessed the personal health information of another individual (Individual A) on December 2, 2018, without an apparent need-to-know. There were five activities that occurred over the course of 51 seconds on Individual A's profile in the EMR. Dr. Narang's lawyer asserted that it is likely due to "technical issues" for this inadvertent access. However, Individual A's last name is not the same or even similar to the names of the patients whose personal health information Dr. Narang accessed prior to and after to accessing this particular Individual A's personal health information. Therefore, the autofill feature would not have contributed to this inadvertent access. It is also difficult to conceive how an inadequate Internet connection would have contributed to this inadvertent access as well.

[57] Whether or not technical issues contributed to Dr. Narang's accesses, I find that HIPA does not authorize access to patient's personal health information due to "technical issues". I find that Dr. Narang has not established that there was a professional need-to-know the personal health information for the seven individuals. As such, I find that privacy breaches occurred.

iii. Dr. Narang had provided care to the patient

[58] Dr. Narang's lawyer identified that one individual attended an appointment with Dr. Narang on November 30, 2018, for whom Dr. Narang ordered bloodwork. Dr. Narang's lawyer explained that accesses to this patient's personal health information in December

2018, was either related to the appointment (i.e. updating notes on the patient) or the bloodwork results would have been directed to Dr. Narang. I find that such accesses to the individual's personal health information in the EMR are authorized by subsection 23(1) of HIPA.

iv. Dr. Narang was assisting Dr. Franklin

[59] Dr. Narang accessed an individual's personal health information on March 10, 2019. Dr. Narang was unable to recall the reason for accesses to this patient's personal health information on March 10, 2019. Dr. Narang's lawyer suggested that since this individual had an appointment with Dr. Franklin on February 26, 2019, it is possible that the medical office assistants sought assistance from Dr. Narang about the patient if Dr. Franklin was unavailable. Similarly, there were other instances in which Dr. Narang believed they may have accessed another individual's personal health information because the individual was scheduled to see Dr. Franklin on March 13, 2019, but Dr. Franklin was on call at the hospital that day. Certainly, if Dr. Narang is accessing patient's personal health information in the EMR to provide physician services, I find this access to be on a need-to-know basis pursuant to subsection 23(1) of HIPA. Later in this Report, in the "Plan for prevention" section, I will describe the steps Dr. Narang is taking to account for such accesses.

[60] In another case, a consultation report for a particular patient was sent to RPCC on January 28, 2019. The audit log showed that the consultation report was initially assigned to Dr. Narang. As a result, Dr. Narang accessed the patient's personal health information on January 29, 2019 and January 30, 2019. Then consultation was subsequently transferred by a medical office assistant to Dr. Franklin on January 30, 2019. I find that Dr. Narang accessing the patient's personal health information was on a need-to-know basis pursuant to subsection 23(1) of HIPA, because they were prompted to do so because of receiving the consultation report.

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

[61] My office's resource, *Privacy Breach Investigation Questionnaire* (June 23, 2020), suggests trustee organizations take the following four best practice steps when responding to a privacy breach:

1. Contain the breach;
2. Notify affected individuals;
3. Investigating the breach;
4. Plan for prevention.

[62] I will analyze these steps below.

Contain the breach

[63] When a privacy breach has or may have occurred, a trustee organization should take immediate steps to confirm and contain the breach. Depending on the nature of the breach, this can include stopping the unauthorized practice, recovering the records, shutting down the breached system, revoking access privileges or correcting security vulnerabilities.

[64] As noted earlier, the SHA provided Dr. Narang with a two-week period to access the EMR so that they could refresh their memory as to why they had accessed certain patients' personal health information. Dr. Narang was no longer able to access Dr. Franklin's billing, schedule or day sheet. I find that the SHA has taken steps to contain the breach.

[65] However, I recommend that when the SHA has grounds to believe an individual is inappropriately accessing personal health information, that the SHA immediately suspend the individual's access to the EMR instead of giving them another two weeks of access to the EMR. I recommend that the SHA explore other options of having the individual account for their accesses to the EMR. This can include giving the individual printed copies of audit logs and other printed documents to assist the individual to jog their memories of why they may have accessed patients' personal health information.

Notify affected individuals

[66] Notifying an individual that their personal health information has been inappropriately accessed or disclosed is important for a number of reasons. Not only do individuals have a right to know, they need to know in order to protect themselves from potential harm that may result from the inappropriate disclosure. Unless there is a compelling reason not to, trustee organizations should always provide notification.

[67] The SHA provided notification of the unauthorized accesses to affected individuals. However, it merely described the snooper as, "an individual at Rosetown Primary Health Centre, who was not involved in your medical care" in the letter. This resulted in the Complainant and other employees and contractor(s) at the RPCC bearing the consequences of Dr. Narang's snooping.

[68] My office's position is that an individual who has snooped should have a diminished expectation of privacy. Their identities and the disciplinary action taken against them should be revealed to affected individuals. The impact of a privacy breach is not standard and flat. Learning that a best friend, business partner, estranged spouse, co-worker, boss, neighbour, or a stranger snooped upon one's personal health information has different implications for individuals. Affected individuals are in the best position to understand the impacts of a privacy breach upon themselves. Knowing the identity of the snooper provides affected individuals with information to assess the harm that may result from having their privacy invaded. In my Investigation Report 100-2015, I cited the former Ontario Information and Privacy Commissioner's Investigation Report HO-010 that provided that aggrieved individuals have a right to a complete accounting of what has occurred. Aggrieved individuals will not find closure regarding the incident unless all the details of the investigation have been disclosed. Receiving general assurances that "the incident has been dealt with appropriately" falls far short of the level of disclosure that is required. Further, publicly identifying the snooper and the disciplinary action taken against the snooper would be a strong deterrent for other employees and contractors.

[69] In this case, the SHA's letters to affected individuals did not identify Dr. Narang nor did it identify any disciplinary action taken against them. It also provided the general assurance

that the SHA will, "continually strive to make improvements to our processes to better protect the privacy of our patients, client and residents".

[70] I find that the SHA's notification letters to affected individuals does not provide the complete accounting to affected individuals that is required for individuals to find closure regarding the snooping committed by Dr. Narang.

[71] I recommend that the SHA send another letter to the affected individuals that identifies Dr. Narang as the snooper. The letter should also identify the disciplinary actions, if any, taken against Dr. Narang. Further, it should identify concrete actions taken by the SHA to prevent future incidents of snooping. For example, it should provide details of whether Dr. Narang's access to personal health information was restricted, what training Dr. Narang has undertaken so that they understand the requirements of HIPA, and how often Dr. Narang is audited. The letter should also include instructions to individuals on how they can submit a formal access to information request under HIPA for access to their personal health information in the EMR, including the audit logs of who may have accessed their personal health information. The letter should include the contact information of an SHA employee who can answer questions about this matter. Since some time has elapsed since it was discovered that Dr. Narang has snooped into the EMR, I recognize that the RPCC may not have the current contact information of affected individuals. As such, if the SHA does not have the current contact information for any of the affected individuals, then I recommend that the SHA post its notification of this privacy breach to its website for a period of at least 30 days. To ensure the greatest chance of affected individuals receiving the notification via the SHA's website, I recommend that the SHA post the notification to a webpage of the SHA's website that receives a lot of traffic. This can include its "News Releases" page at https://www.saskhealthauthority.ca/news/releases.

Investigate the breach

[72] Investigating the privacy breach to identify the root cause is key to understanding what happened and to prevent similar privacy breaches in the future.

[73] The SHA determined the privacy breaches were likely intentionally committed by Dr. Narang. During its investigation, the SHA found that Dr. Narang demonstrated a strong awareness of HIPA and the need-to-know principle. The SHA indicated that Dr. Narang was aware of the fact that eHealth Saskatchewan's Electronic Health Record Viewer (eHR Viewer) was monitored and audited. SHA indicated that Dr. Narang was not aware that the "health information at the Rosetown Primary Care Centre was audited". The SHA indicated that an audit of the Patient Archiving and Communication System (PACS) found that Dr. Narang had not accessed any of the affected individuals' personal health information within that system. In contrast though, the SHA indicated to my office that it appeared that Dr. Narang was not aware that the "health information" at the RPCC was audited. Therefore, SHA suggested that if Dr. Narang was aware of auditing done on the EMR, perhaps Dr. Narang would not have snooped.

[74] Earlier, I summarized the SHA's investigation findings into why Dr. Narang accessed personal health information in the EMR, so I will not repeat them here. However, in its investigation, the SHA identified gaps in its safeguards. Namely, it had not required Dr. Narang to sign the *Information Sharing and Clinic Exit Agreement* or the *Single Trustee Policy for EMR System at Rosetown Primary Health Care Centre* when Dr. Narang joined the RPCC in September of 2018. The former agreement was between the HRHA and the physicians who signed the agreement. As described and discussed earlier, this agreement confusingly implies that both the HRHA and the physician are trustees under HIPA for the personal health information in the EMR. This agreement also specifies how physicians are to maintain records in accordance with the requirements of the CPSS and HIPA, to use/disclose personal health information in accordance with HIPA, and to work together to ensure HIPA compliance. It also provides details of how records are to be managed, should a physician leave the RPCC. The latter agreement specifies that the personal health information in the EMR is in the custody and control of the HRHA and it requires that all users access the EMR for "authorized health purposes" specified in the agreement. Not requiring Dr. Narang to review and sign these agreements when Dr. Narang first joined the RPCC likely contributed to these privacy breaches. Without requiring Dr. Narang to review and sign these agreements, the SHA did not communicate its expectations to Dr. Narang.

Submission of Dr. Narang's lawyer

[75] Earlier, I summarized Dr. Narang's reasons for accessing the personal health information in the EMR. I will not repeat them here. However, I should note that in their letter dated September 11, 2020, Dr. Narang's lawyer indicated that Dr. Narang was surprised by SHA's statement that Dr. Narang accessed the SHA employee's personal health information due to curiosity. Dr. Narang thought they made it clear that curiosity was not the reason they accessed any patient charts.

[76] Besides the two circumstances in which Dr. Narang admitted that they should not have accessed personal health information in the EMR, Dr. Narang's reasons for accessing patient charts are as follows:

1) Technical issues;
2) Lack of privacy training; and
3) Lack of training on the EMR through the SIPPA program.

[77] In the "Plan for prevention" section below, I will summarize the steps Dr. Narang has taken to address these reasons. I will also summarize the SHA's plan for prevention.

Plan for prevention

[78] At risk is patients' trust in Dr. Narang, the RPCC, and the SHA to manage their personal health information in a privacy-respectful manner. Implementing a plan for prevention is important to restore patients' trust and confidence in the delivery of health care. Preventing future breaches means implementing measures to prevent similar breaches from occurring in the future. This could include implementing policies and procedures that help reduce the likelihood of the same or similar types of breaches from occurring in the future.

SHA's plan for prevention

[79] In its investigation report, the SHA indicated that the physicians at the RPCC now only have access to their own schedules in the EMR.

[80] It also said it has discussed the two agreements, *Information Sharing and Clinic Exit Agreement* and the *Single Trustee Policy for EMR System at Rosetown Primary Health Care Centre* with Dr. Narang. However, it indicated that Dr. Narang signed one agreement but not the other. Dr. Narang's lawyer clarified that Dr. Narang signed the former agreement, but not the latter one. Earlier, I had recommended that the SHA amend the *Information Sharing and Clinic Exit Agreement*. I recommend that once the SHA amends the agreement, that it require Dr. Narang to review and sign this agreement.

[81] Dr. Narang should be given the chance to review the *Single Trustee Policy for EMR System at Rosetown Primary Health Care Centre* agreement and to ask questions about the agreement prior to signing it. However, if Dr. Narang refuses to sign the agreement, then the SHA should take action to protect its personal health information. In other words, without Dr. Narang's cooperation, the SHA should not allow Dr. Narang to have access to personal health information in the EMR. I recommend that the SHA require Dr. Narang to sign the *Single Trustee Policy for EMR System at Rosetown Primary Health Care Centre*. If Dr. Narang refuses to sign the agreement, then the SHA should disable Dr. Narang's access to the EMR.

[82] The SHA indicated it would conduct "regular audits of accesses to the personal health information at the Clinic". It did not define what it meant by "regular" audits. In previous investigation reports, I have recommended that physicians who have snooped should be audited monthly for a period of three years so that trustees can ensure they are accessing personal health information for need-to-know purposes in accordance with subsection 23(1) of HIPA. If Dr. Narang has access to the EMR, then I recommend that the SHA conduct monthly audits of Dr. Narang's accesses to the EMR for at least three years. If any audit reveals that Dr. Narang is accessing personal health information inappropriately, I recommend that their user privileges to the EMR be suspended. The SHA should report the matter to both my office and to the CPSS.

[83] The SHA also indicated it is exploring ways for physicians to receive the same privacy training that SHA employees are required to receive. I recommend that SHA implement procedures so that no physicians are given access to the EMR without having received HIPA training. Further, the SHA should require physicians, its employees/contractors, and Town employees at the RPCC to take annual HIPA training. If physicians, employees/contractors, or Town employees at the RPCC do not take the annual HIPA training, their access to personal health information (whether it be electronic or hard copy) should be suspended until the training is completed.

[84] Finally, I recommend that the SHA require agreements to be signed by any individual who accesses the EMR. This would include not only SHA employees and contractors, but also medical office assistants who may not be SHA employees but are instead employees of municipalities such as the Town. These agreements should set out the consequences that will occur if the individuals breach the privacy of patients.

Steps taken by Dr. Narang

[85] According to the letter dated September 11, 2020, from Dr. Narang's lawyer, Dr. Narang is enrolled in a course called "HIPA – Diagnosis Privacy". This course is offered by the Division of Continuing Medical Education at the University of Saskatchewan. Further, Dr. Narang completed an in-person Medical Record Keeping course at the University of Toronto in May of 2019. Dr. Narang's lawyer indicated that since taking this course, Dr. Narang has been documenting whenever they access the EMR for patients usually seen by Dr. Franklin or another family physician.

[86] I commend Dr. Narang for taking these steps in increasing their knowledge of HIPA and taking practical steps to account for their accesses to personal health information in the EMR. I recommend that Dr. Narang continue to seek opportunities to increase their knowledge of HIPA. This would include cooperating and complying with the SHA's safeguards. If they have questions, concerns, or suggestions on how to improve safeguards, they should raise them with the SHA's Privacy Officer.

III FINDINGS

[87] I find that the SHA qualifies as the "trustee" as defined by subsection 2(t)(ii) of HIPA and a "local authority" pursuant to subsection 2(f)(xiii) of LA FOIP.

[88] For the purposes of LA FOIP and HIPA, I find that Dr. Narang is an "employee" of the SHA and not a trustee.

[89] I find that the SHA is the trustee with custody or control over the personal health information in the EMR.

[90] I find that privacy breaches occurred when Dr. Narang accessed certain patients' personal health information in the EMR without a need-to-know.

[91] I find that the SHA has taken steps to contain the breach.

[92] I find that the SHA's notification letters to affected individuals do not provide the complete accounting to affected individuals that is required for individuals to find closure regarding the snooping committed by Dr. Narang.

[93] I find that the SHA has investigated the privacy breaches and identified gaps in its safeguards.

IV RECOMMENDATIONS

[94] I recommend that the SHA amend its contract with Dr. Narang (and with any other physician) so that it is clear.

[95] I recommend that the SHA amend the wording of the agreement entitled *Information Sharing and Clinic Exit Agreement* so that it is clear that the SHA is the trustee of the personal health information in the EMR.

[96] I recommend that the SHA amend the *Information Sharing and Clinic Exit Agreement* so that it sets out the consequences for a physician that breaches HIPA.

[97] I recommend that once the SHA has amended the wording in the agreement entitled *Information Sharing and Clinic Exit Agreement*, that it require Dr. Narang to review and sign it.

[98] I recommend that when the SHA has grounds to believe an individual is inappropriately accessing personal health information, that the SHA immediately suspend the individual's access to the EMR instead of giving them another two weeks of access to the EMR.

[99] I recommend that the SHA explore other options of having the individual account for their accesses to the EMR instead of giving them access to the EMR for a two-week period. This can include giving the individual printed copies of audit logs and other printed documents to assist the individual to jog their memories of why they may have accessed patients' personal health information.

[100] I recommend that the SHA send another letter to the affected individuals as described at paragraph [71].

[101] I recommend that the SHA post its notification of the privacy breaches to its website for a period of at least 30 days as described at paragraph [71].

[102] I recommend that SHA require Dr. Narang to sign the *Single Trustee Policy for EMR System at Rosetown Primary Health Care Centre*.

[103] If Dr. Narang refuses to sign either the *Information Sharing and Clinic Exit Agreement* (once it has been amended) or the *Single Trustee Policy for EMR Systems at Rosetown Primary Health Care Centre*, that the SHA disable Dr. Narang's access to the EMR.

[104] If Dr. Narang has access to the EMR, then I recommend that the SHA conduct monthly audits of Dr. Narang's accesses to the EMR for at least three years. If any audit reveals

that Dr. Narang is accessing personal health information inappropriately, I recommend that their user privileges to the EMR be suspended. The SHA should report the matter to both my office and to the CPSS.

[105] I recommend that SHA implement procedures so that no physicians are given access to the EMR without having received HIPA training and having signed the amended *Information Sharing and Clinic Exit Agreement* and the *Single Trustee Policy for EMR Systems at Rosetown Primary Health Care Centre*.

[106] I recommend that the SHA require agreements to be signed by any individual who accesses the EMR. This would include not only SHA employees and contractors, but also medical office assistants who may not be SHA employees but employees of municipalities such as the Town. These agreements should set out the consequences that will occur if the individuals breach the privacy of patients.

[107] I recommend that the SHA require physicians, its employees/contractors, and Town employees at the RPCC to take annual HIPA training. If physicians, employees, contractors, or Town employees at the RPCC do not take the annual HIPA training, their access to personal health information (whether it be electronic or hard copy) should be suspended until the training is complete.

Dated at Regina, in the Province of Saskatchewan, this 28th day of October, 2020.

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