Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 065-2021, 068-2021, 069-2021, 073-2021

Saskatchewan Health Authority

October 26, 2021

Summary: In October of 2020, the Commissioner issued Investigation Report 203-2019, 214-2019, 257-2019 on the Saskatchewan Health Authority (SHA) regarding Dr. Ashwani Narang's (Dr. Narang) snooping of personal health information of 20 individuals in the electronic medical record (EMR) at the Rosetown Primary Care Centre (RPCC). After issuing the report, four more affected individuals came forward and submitted complaints to the Commissioner. They requested that he investigate the matter. The Commissioner undertook new investigations pursuant to section 52(d) of *The Health Information Protection Act* (HIPA). The Commissioner made a number of findings including that the lack of HIPA training provided by the SHA likely contributed to Dr. Narang inappropriately accessing the Complainants' personal health information. The Commissioner made a number of recommendations including that the SHA suspend Dr. Narang's access to the EMR until the SHA has communicated its expectations to Dr. Narang on how he is to manage personal health information in accordance with HIPA, he has demonstrated the understanding of such expectations and has agreed to conduct himself accordingly. This includes requiring him to receive HIPA training from the SHA, and signing a revised version of the *Information Sharing and Clinic Exit Agreement* (which should include the consequences for a physician that breaches HIPA).

I BACKGROUND

[1] On June 26, 2019, the Saskatchewan Health Authority (SHA) proactively reported a privacy breach to my office. It reported that a physician at the Rosetown Primary Care Centre (RPCC) had accessed 20 patients' personal health information in the RPCC's electronic medical record (EMR) without a professional need-to-know.

[2] Then, in letters dated July 2, 2019 and July 10, 2019, the physician's lawyer contacted my office indicating that the physician, Dr. Ashwani Narang (Dr. Narang), was proactively reporting a privacy breach to my office. The lawyer asserted that trusteeship for the patients' personal health information lies with both the SHA and Dr. Narang.

[3] Finally, on July 4, 2019, my office received a complaint from an affected individual that a physician, Dr. Narang, had inappropriately accessed their personal health information. This affected individual was an employee at the RPCC.

[4] My office undertook an investigation. I issued Investigation Report 203-2019, 214-2019, 257-2019 on October 28, 2020. I made a number of findings in that investigation, including that the SHA, not Dr. Narang, was the trustee with custody or control over the personal health information in the EMR at the RPCC. It should be noted that throughout this Investigation Report, I will be referencing the previous Investigation Report 203-2019, 214-2019, 257-2019.

[5] In my Investigation Report 203-2019, 214-2019, 257-2019, I noted that seven individuals whom Dr. Narang snooped upon were members of a family.

[6] In March of 2021, four of the seven members of the family submitted complaints to my office. These four members are part of a nuclear family (herein referred to as Complainants, or Complainant Z, Complainant Y, Complainant X, and Complainant W). The remaining three are extended family members. The Complainants requested they be given an opportunity to provide their perspective on this matter. I determined that I would undertake new investigations into this matter pursuant to section 52(d) of *The Health Information Protection Act* (HIPA):

> **52** The commissioner may:
>
> ...
>
> (d) from time to time, carry out investigations with respect to personal health information in the custody or control of trustees to ensure compliance with this Act;

[7] Pursuant to Part 7 of my office's *Rules of Procedure*, it is normal procedure for my office to notify the Complainants and the trustee that my office is undertaking an investigation. This matter was no different especially since my office previously found that it was the SHA, and not Dr. Narang, that was the trustee of the personal health information at issue. Therefore, on April 6, 2021, my office notified the Complainants and the SHA that it would be undertaking investigations into this matter.

The Complainants' perspective

[8] At paragraph [43] of my Investigation Report 203-2019, 214-2019, 257-2019, I noted that Dr. Narang's lawyer had indicated to my office that Dr. Narang accessed the personal health information of seven members of the same family for a personal reason. Dr. Narang's lawyer also indicated that Dr. Narang apologized to the family. However, the Complainants asserted that Dr. Narang had not apologized to them, but had only apologized to one extended family member.

[9] According to the Complainants, the following occurred:

- One of the Complainants (Complainant Z) was the schoolmate of a member of Dr. Narang's family (Person A).
- Some time between January 23, 2019 and January 27, 2019, Person A attended the Complainants' home then left. Some time between 10:00pm and 10:30pm in the evening, Complainant Z went to Dr. Narang's home to return school material to Person A.
- On January 31, 2019, Person A attended the Complainants' home again and remained there for less than an hour before leaving. Soon after, Dr. Narang, Dr. Narang's spouse, and Person A returned to the Complainants' home. A discussion occurred between two of the Complainants and Dr. Narang, Dr. Narang's spouse, and Person A.

[10] In June of 2019, three of the four Complainants received letters from the SHA indicating that their "personal health information was inappropriately viewed by an individual at the Rosetown Primary Health Care Centre who was not involved in your medical care". In November 2019, the fourth Complainant received a similar letter from the SHA.

[11] The Complainants provided my office with a copy of an apology letter dated August 7, 2019 from Dr. Narang that was addressed to an extended family member. In the letter, Dr. Narang indicated that the reason for accessing the extended family member's personal health information in "January 2019" (no specific date provided) was out of concern for Person A's whereabouts. Dr. Narang indicated that Person A may have been with a person with the same last name as the extended family member (Complainant Z). Therefore, Dr. Narang asserted he accessed records to locate Complainant Z's address. Dr. Narang asserted he only knew Complainant Z's last name at the time and he believed he accessed the extended family member's medical records during the search.

[12] The Complainants provided my office with audit reports that showed the dates and times in which Dr. Narang accessed their personal health information in the RPCC's EMR. Below is a table that details these accesses:

Date	Time in which information was accessed	# of times the chart was accessed	# of times the "Medical Summary" was accessed
Complainant Z			
January 23, 2019	22:08:42 to 22:39:48	4	5
January 31, 2019	19:48:59 to 19:50:04	4	4
May 20, 2019	12:47:40 to 12:47:46	2	2
Complainant Y			
January 23, 2019	22:11:04 to 22:11:12	2	2
January 31, 2019	19:49:18 to 19:49:52	3	3
May 20, 2019	12:48:29 to 12:48:29	1	1
Complainant X			
January 23, 2019	22:11:42 to 22:11:52	2	2
January 31, 2019	19:50:15 to 19:50:19	2	2
May 20, 2019	12:49:05 to 12:49:06	1	1
Complainant W			

January 23, 2019	22:12:17 to 22:13:03	3	3

[13] Dr. Narang's accesses to the Complainants' personal health information on January 23, 2019 and January 31, 2019 appear to coincide with the times in which interactions occurred between Complainant Z, Person A, and Dr. Narang. Of the four Complainants, Dr. Narang had the greatest interest in Complainant Z based on the number of times Dr. Narang accessed Complainant Z's personal health information.

[14] The Complainants expressed concern over Dr. Narang's accesses to their personal health information for Dr. Narang's own personal reasons. They expressed an unsettling feeling of wondering why Dr. Narang would access their personal health information and what he may do with such information.

[15] I note that the accesses on May 20, 2019 appear to be a part of the SHA's investigation process, as I had noted at paragraph [5] of my Investigation Report 203-2019, 214-2019, 257-2019.

II DISCUSSION OF THE ISSUES

1. Do I have jurisdiction?

[16] HIPA is only engaged if three elements are present: 1) there must be a trustee within the meaning of section 2(t) of HIPA; 2) there must also be personal health information within the meaning of section 2(m) of HIPA; and 3) the personal health information must be in the custody or control of the trustee.

[17] At paragraphs [21] to [36] of my Investigation Report 203-2019, 214-2019, 257-2019, I found:

- that the SHA qualifies as a trustee pursuant to section 2(t)(ii) of HIPA;
- that the information in RPCC's EMR qualifies as personal health information pursuant to section 2(m) of HIPA; and

- that the personal health information in the EMR is within the custody or control of the SHA.

[18] The circumstances are the same in this investigation. As such, I find that HIPA applies to this matter and I have jurisdiction to conduct this investigation.

2. Did privacy breaches occur?

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

[20] When personal health information is accessed by an employee or a contractor of the SHA, such accesses qualify as a "use" of personal health information. Section 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.

[21] Section 23(1) of HIPA provides that trustees should be using personal health information on a need-to-know basis:

> **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.

[22] 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.

[23] My office learned of different reasons given by Dr. Narang for accessing the Complainants' personal health information. To the SHA, Dr. Narang indicated that he accessed the Complainants' personal health information in the EMR for the purposes of having a complete family history for an individual patient. When my office inquired with the SHA which family member was Dr. Narang's patient, the SHA said Dr. Narang did not indicate which family member was the "original patient". The SHA stated that it was not able to establish that Dr. Narang had a professional need-to-know to access any of the family members' personal health information.

[24] In contrast, and as described earlier in this Report, there was an apology letter written by Dr. Narang to one of the extended family members. Dr. Narang explained how he was concerned for Person A's whereabouts and therefore accessed information in the EMR to locate Complainant Z's address. Since he was only aware of Complainant Z's last name, Dr. Narang ended up accessing the extended family member's personal health information.

[25] Given that Dr. Narang provided different reasons for accessing the Complainants' personal health information, Dr. Narang's credibility is questionable. First, since the SHA was unable to establish that Dr. Narang had a professional need-to-know, I can conclude that none of the Complainants or extended family members were patients of Dr. Narang. Furthermore, even if a Complainant or an extended family member was a patient of Dr. Narang's, HIPA would not authorize Dr. Narang to snoop through the EMR for the purposes of having a complete family history of a patient. Second, I summarized the number of times Dr. Narang accessed each of the Complainants' personal health information in the EMR. If he was merely seeking an address, he would not have needed to access each Complainants' chart and medical summaries multiple times. Nevertheless,

HIPA also does not authorize Dr. Narang to snoop through personal health information for the purposes of seeking the address for a personal reason. As I have said in my previous Investigation Report 308-2017, 309-2017, 310-2017 regarding eHealth's electronic Health Record (eHR Viewer), I emphasized how accessing patients' personal health information for personal reasons undermines the integrity of the health care system:

> [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.

[26] The same principle applies to users of an EMR. Physicians and any other user of an EMR should not regard themselves as above the law. They must still comply with HIPA.

[27] As I noted in Investigation Report 203-2019, 214-2019, 257-2019, the Council of the College of Physicians and Surgeons of Saskatchewan (CPSS) laid a charge against Dr. Narang on September 26, 2020 for accessing personal health information without a legitimate need-to-know. The charge was as follows:

> 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.

[28] After the hearing on September 17, 2021, the Council of the CPSS imposed penalties upon Dr. Narang, including a 3-month suspension commencing on September 20, 2021 and a requirement that Dr. Narang complete a course on medical ethics and professionalism within six months.

[29] Based on: (1) the SHA's finding that there was no professional need-to-know to access the family members' personal health information, (2) Dr. Narang's apology letter to the extended family member, and (3) the Council of the CPSS' charge and penalties imposed upon Dr. Narang, I find that privacy breaches occurred. There was no authority under HIPA for Dr. Narang to have accessed the Complainants' personal health information.

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

[30] In the resource, *Privacy Breach Guidelines for Trustees* (updated September 2020) (Privacy Breach Guidelines), my office recommends four steps to be taken when a trustee discovers a privacy breach. The four steps are:

1. Contain the breach
2. Notification
3. Investigate the breach
4. Prevent future breaches

[31] Below is an analysis to determine if the SHA responded appropriately to the privacy breach based on these four steps.

Contain the breach

[32] To contain a breach is to ensure that personal health information is no longer at risk. This may involve:

- stopping the unauthorized practice
- recovering the records
- shutting down the system that was breached
- revoking access to personal health information
- correcting weaknesses in physical security

(Privacy Breach Guidelines, p. 3)

[33] In Investigation Report 203-2019, 214-2019, 257-2019, I noted that when the SHA first learned that Dr. Narang may have been accessing individuals' personal health information inappropriately, it had asked Dr. Narang to access the individuals' personal health information in the EMR over the course of a two-week period. The SHA did this so that Dr. Narang could refresh his memory as to why he had accessed certain individuals' personal health information. The SHA did not revoke Dr. Narang's access to the EMR. The SHA explained that Dr. Narang needed continued access to the EMR for the purposes of providing patient care; however, the SHA adjusted the EMR so that physicians could only access their own schedule only since it had found that Dr. Narang had accessed the schedule of the other physician at RPCC.

[34] In Investigation Report 203-2019, 214-2019, 257-2019, I had recommended that when the SHA has grounds to believe an individual is inappropriately accessing personal health information, that the SHA should immediately suspend the individual's access to the EMR instead of giving them another two weeks of access. I recommended that the SHA explore other options of having the individual account for their access to the EMR. This could

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. In a letter dated December 15, 2020, the SHA indicated that it would comply with my office's recommendation.

[35] In the course of this current investigation, the SHA indicated that it was auditing Dr. Narang's use of the EMR on a quarterly basis and it has not discovered any further inappropriate accesses.

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

Notification

[37] It is best practice to notify affected individuals of the privacy breach so that they can determine how they have been impacted and take steps to protect themselves. An effective notification should include the following:

- A description of the breach (a general description of what happened)
- A detailed description of the personal health information involved (e.g. name, credit card numbers, medical records, financial information, etc.)
- A description of possible types of harm that may come to them as a result of the privacy breach
- Steps taken and planned to mitigate the harm and to prevent future breaches
- If necessary, advice on actions the individual can take to further mitigate the risk of harm and protect themselves (e.g. how to contact credit reporting agencies, how to change a health services number or driver's license number, etc.)
- Contact information of an individual within your organization who can answer questions and provide further information
- A notice that individuals have a right to complain to my office (provide contact information)
- Recognition of the impacts of the breach on affected individuals and, an apology

(Privacy Breach Guidelines, p. 4)

[38] Initially, the SHA provided a notification letter to affected individuals that did not identify Dr. Narang as the person who accessed their personal health information inappropriately. Therefore, in my Investigation Report 203-2019, 214-2019, 257-2019, I recommended that the SHA send another letter to affected individuals that identifies: (1) Dr. Narang as the person who accessed their personal health information inappropriately, (2) the disciplinary actions, if any, taken against Dr. Narang, and (3) concrete actions taken by the SHA to prevent future incidents of snooping. The SHA sent letters to affected individuals in March of 2021 that identified Dr. Narang as the snooper; however, the letter did not provide detail of any actions, disciplinary or otherwise, to prevent future incidents of snooping. The letter apologized for "any inconvenience" that the privacy breach may have caused and said that the SHA strives to makes improvements to protect privacy. The letter said:

> Further to my letter dated June 2019, the Saskatchewan Health Authority (SHA) has chosen to send a second letter to those patients whose electronic medical record was viewed by an individual working in the Rosetown Primary Health Care Clinic without a professional need-to-know. In my original letter, we did not name the individual who committed the privacy breach, and that was an error on our part. The individual involved in this privacy breach was Dr. A. Narang.
>
> We sincerely apologize that this has happened, and are sorry for any inconvenience that this breach of privacy has caused you. The Saskatchewan Health Authority takes privacy breaches very seriously, and we continually strive to make improvements to our processes to better protect the privacy of our patients, clients and residents.

[39] As described in the background of this Report, the Complainants expressed concern over why Dr. Narang would access their personal health information and what he may do with such information. This signals to me that the Complainants' trust in the SHA maintaining the confidentiality of their personal health information has been undermined.

[40] In past reports, I have said that affected individuals have a right to a complete accounting of what has occurred in order to find closure. General assurances such as the SHA taking privacy breaches "very seriously" falls short of what is needed to restore and ensure patients' trust in the SHA to provide effective healthcare. The SHA should be informing affected individuals of the steps taken to deter Dr. Narang (and others) from snooping in

the future to demonstrate how it has taken the privacy breach "very seriously". For example, in the course of this investigation, the SHA informed my office that it had reported Dr. Narang to CPSS over this matter. I would recommend that the SHA include such detail in their letters to affected individuals in the future. That would demonstrate to affected individuals that the SHA has taken the privacy breach "very seriously" since Dr. Narang would be held accountable for his actions by his professional regulatory body. Such action by the SHA could deter Dr. Narang from snooping in the future. Further, revealing this step taken by the SHA would also deter other employees or contractors at the SHA from snooping. Such concrete detail would assure affected individuals the SHA does indeed take privacy breaches "very seriously" and are looking out for their patients. Otherwise, without such information, affected individuals may hesitate or resist seeking healthcare from the SHA in the future. The SHA cannot deliver effective healthcare without patients' trust and confidence.

[41] As part of an effective notice to affected individuals, the trustee should be providing a description of possible types of harm that may come to them as a result of the privacy breach. The SHA's letters to the Complainants did not detail possible harms including the loss of trust in the SHA to maintain the confidentiality of their personal health information. Alarmingly, based on what was provided to my office, the SHA seemed to demonstrate it did not understand the seriousness of breaching the Complainants' personal health information or the possible harm that may come to them as a result of the privacy breach. During investigations, my office asks trustees to fill out a form called *Privacy Breach Investigation Questionnaire for Public Bodies*. In filling out this questionnaire, the SHA stated that the risk to the patient is "low" since it believed that the snooping wasn't for any "malicious purpose". It said:

> The risk to the patients from this privacy breach is low. Dr. Narang stated that he accessed the records of this family for the purposes of having a complete family history for an individual patient. **We do not feel that the information was reviewed for any malicious purpose.**
>
> [Emphasis added]

[42] As I have already analyzed earlier, Dr. Narang reporting to the SHA that he accessed the Complainants' personal health information to have a complete family history for an individual patient contrasts with the reason that Dr. Narang stated in his apology letter to an extended family member. The SHA is not in a position to evaluate whether a snooper's motives were "malicious" or not. Only affected individuals are in the position to determine how snooping impacts them. Snooping is serious and jeopardizes patients' trust in the SHA.

[43] While I find that the SHA has notified the affected individuals, I find its notification letters to be inadequate. I recommend that the SHA amend its practices so that it offers details of actions taken by the SHA to prevent future privacy breaches in its notification letters.

Investigation

[44] Investigating the privacy breach to identify the root cause(s) is key to understanding what happened and to prevent similar privacy breaches in the future. Below are some key questions to ask during a privacy breach investigation:

- When and how did your organization learn of the privacy breach?
- What occurred?
- How did the privacy breach occur?
- What is the applicable legislation and what specific sections are engaged?
- What safeguards, policies, and procedures were in place at the time of the privacy breach?
- Was the duty to protect met?
- Who are the affected individuals?

(Privacy Breach Guidelines, p. 5)

[45] As described in my Investigation Report 203-2019, 214-2019, 257-2019, employees at the RPCC became suspicious that Dr. Narang was accessing personal health information without a professional need-to-know based on comments he was making. As an

administrator of the EMR, an employee at the RPCC conducted an audit of Dr. Narang's accesses and then reported Dr. Narang's snooping to the SHA. Then, the SHA conducted an investigation into the matter and was unable to establish that Dr. Narang had a professional need-to-know to access the personal health information of the affected individuals. In other words, HIPA did not authorize Dr. Narang's accesses to the affected individuals' personal health information, including the Complainants' in this case.

[46] Section 16 of HIPA sets out the duty of trustees to protect personal health information. Section 16 of HIPA provides:

> **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.

[47] Failure to have adequate safeguards pursuant to section 16 of HIPA means there is a greatly increased risk that patients' personal health information will fail to be protected from exposure from those without a legitimate need-to-know that personal health information. Below, I will discuss the following safeguards: (1) *Information Sharing and Clinic Exit Agreement* and *Single Trustee Policy for EMR System at Rosetown Primary Health Care Centre*, (2) privacy training, and (3) auditing.

(1) Information Sharing and Clinic Exit Agreement and *Single Trustee Policy for EMR System at Rosetown Primary Health Care Centre*

a. *Information Sharing and Clinic Exit Agreement*

[48] In Investigation Report 203-2019, 214-2019, 257-2019, I recommended that the SHA amend the wording in the *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 at the RPCC. Further, I recommended that the SHA amend the wording so that it sets out the consequences for a physician that breaches HIPA. In response, the SHA indicated it would comply with my recommendations. In the course of this investigation, the SHA advised that Dr. Narang signed the former version of this agreement. However, it advised my office that due to the pandemic, the *Information Sharing and Clinic Exit Agreement* had not been reviewed and updated. However, the SHA's Director of Privacy met with primary care directors and the SHA's senior contract specialist in July of 2021 and the SHA has a plan to review and revise the agreement in September of 2021. The SHA did note that due to the nature of the relationship between the SHA, the RPCC, and the Town of Rosetown, the review and revision of the agreement may not be complete by the end of September 2021.

[49] I recommend that the SHA prioritize the review and revision of the *Information Sharing and Clinic Exit Agreement*. As I had mentioned earlier, Dr. Narang was suspended by the Council of the CPSS for a period of three months commencing on September 20, 2021. I recommend that the SHA suspend Dr. Narang's access to the EMR and require Dr. Narang to sign the revised *Information Sharing and Clinic Exit Agreement* prior to being given access to the EMR again.

b. Single Trustee Policy for EMR System at Rosetown Primary Health Care Centre

[50] In Investigation Report 203-2019, 214-2019, 257-2019, I recommended that the SHA require Dr. Narang to sign the *Single Trustee Policy for EMR System at Rosetown Primary Health Care Centre*. In response, the SHA agreed to comply with that recommendation and provided my office with a copy of the agreement signed by Dr. Narang, dated July 6, 2021.

(2) Privacy Training

[51] In Investigation Report 203-2019, 214-2019, 257-2019, it was noted that Dr. Narang did not receive HIPA training through the SHA. Therefore, I had recommended that the SHA implement procedures so that no physicians are given access to the EMR without having received HIPA training. In response, the SHA indicated that it was working with its physician leadership on privacy training for physicians who practice in the SHA and when that training will be delivered (e.g. prior to being given access to the EMR). In the course of this investigation, the SHA indicated that it will require physicians to complete SHA's privacy training module. However, it said due to the ongoing work regarding COVID-19, the SHA had not begun this work. The SHA indicated that it expected to be ready to engage physicians in privacy training in the 2022-2023 fiscal year. The SHA noted that Dr. Narang had received privacy training through the Saskatchewan International Physicians Practice Assessment (SIPPA) program and the Saskatchewan Medical Association.

[52] I find that the lack of HIPA training provided by the SHA has likely contributed to Dr. Narang inappropriately accessing the Complainants' personal health information in the EMR.

[53] I recommend that physicians are not given access to the EMR without having received HIPA training by the SHA first and having signed the revised *Information Sharing and Clinic Exit Agreement* and the *Single Trustee Policy for EMR Systems at Rosetown Primary Health Care Centre*. Further, I recommend that the SHA require physicians to receive annual HIPA training. Should physicians fail to take the annual HIPA training, then their access to personal health information (whether it be electronic or hard copy) should be suspended until the training is complete.

(3) Auditing

[54] As noted in Investigation Report 203-2019, 214-2019, 257-2019, Dr. Narang was aware that eHealth's eHR Viewer was monitored and audited. However, he was not aware that the EMR at the RPCC was audited. The SHA had suggested that if Dr. Narang was aware that the EMR was audited, then perhaps Dr. Narang would not have snooped. I had recommended to the SHA that it conduct monthly audits of Dr. Narang's accesses to the

EMR for a period of three years. If the SHA detected any inappropriate accesses, then the SHA should suspend Dr. Narang's access to the EMR as well as report the matter to both the CPSS and to my office. In response, the SHA indicated that it had been auditing Dr. Narang's access to the EMR on a quarterly basis and would continue to do so for a period of three years. It said it was also conducting random audits on all EMR users as part of its standard practice. It said it would report any inappropriate accesses to both my office and to the CPSS. However, it said it would not suspend Dr. Narang's access to the EMR as that would be a risk to patient care.

[55] I would argue that any inappropriate accesses of personal health information by any physician (or any other user of the EMR) is a risk to patient care. As my office had documented in Investigation Report H-2013-001, employees of the former Regina Qu'Appelle Regional Health Authority accessed electronic information systems and entered false information into patients' charts. Inaccurate and false information threatens the basis in which healthcare providers can make appropriate decisions about a patient's care and can lead to undesired outcomes, including fatal ones. Allowing a snooper to have continued access to personal health information means patient care continues to be at risk.

[56] I recommend that if the SHA detects any inappropriate accesses by any user of the EMR, that it swiftly suspend the user's access to the EMR until the SHA can complete an investigation into the matter and implement appropriate safeguards to protect the integrity and accuracy of the personal health information, including the information that was snooped upon.

Prevent future breaches

[57] Prevention is perhaps one of the most important steps. A privacy breach cannot be undone, but a trustee can learn from one and improve its practices. To avoid future breaches, the trustee should formulate a prevention plan. Some changes that are needed may have revealed themselves during the investigation phase. For example, deficient policies or procedures, a weakness in the system, a lack of accountability measures or a lack of training.

[58] The following are some questions a trustee should consider when completing this step in responding to a privacy breach:

- Can the trustee create or make changes to policies and procedures relevant to this privacy breach?
- Are additional safeguards needed?
- Is additional training needed?
- Should a practice be stopped?

(Privacy Breach Guidelines, p. 6)

[59] In this Report, I have already described the prevention measures taken by the SHA, including the SHA's plan to review and revise the *Information Sharing and Clinic Exit Agreement* as well as having Dr. Narang sign the *Single Trustee Policy for EMR System*. I have made recommendations regarding the prevention measures taken by the SHA as well.

[60] However, I want to emphasize the importance of the SHA communicating its expectations to Dr. Narang on how he is to manage personal health information in accordance with HIPA. This includes the SHA providing him with HIPA training and requiring him to sign a revised version of the *Information Sharing and Clinic Exit Agreement*, which should include communicating the consequences for a physician that breaches HIPA. Dr. Narang (and all other physicians) should be made aware of the offense provisions set out in HIPA. Until Dr. Narang has demonstrated his understanding of HIPA and the SHA's expectations and has agreed to conduct himself accordingly, I recommend that Dr. Narang's access to the EMR be suspended.

III FINDINGS

[61] I find that HIPA applies to this matter and I have jurisdiction to conduct this investigation.

[62] I find that privacy breaches occurred.

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

[64] While I find that the SHA has notified the affected individuals, I find its notification letters to be inadequate.

[65] I find that the lack of HIPA training provided by the SHA likely contributed to Dr. Narang inappropriately accessing the Complainants' personal health information in the EMR.

IV RECOMMENDATIONS

[66] I recommend that the SHA amend its practices so that it offers details of actions taken by the SHA to prevent future privacy breaches in its notification letters to individuals who are affected by privacy breaches.

[67] I recommend that the SHA prioritize the review and revision of the *Information Sharing and Clinic Exit Agreement*.

[68] I recommend that the SHA suspend Dr. Narang's access to the EMR and require Dr. Narang to sign the revised *Information Sharing and Clinic Exit Agreement* prior to being given access to the EMR again.

[69] I recommend that physicians not be given access to the EMR without having received HIPA training from the SHA and having signed the revised *Information Sharing and Clinic Exit Agreement* and the *Single Trustee Policy for EMR Systems at Rosetown Primary Health Care Centre*.

[70] I recommend that the SHA require physicians to receive annual HIPA training. Should physicians fail to 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.

[71] I recommend that if the SHA detects any inappropriate accesses by any user of the EMR, that it swiftly suspend the user's access to the EMR until it can complete an investigation into the matter and implement appropriate safeguards to protect the integrity and accuracy of the personal health information, including the information that was snooped upon.

[72] I recommend that the SHA communicate its expectations to Dr. Narang on how he is to manage personal health information in accordance with HIPA. This includes the SHA providing him with HIPA training and requiring him to sign a revised version of the *Information Sharing and Clinic Exit Agreement*, which should include communicating the consequences for a physician that breaches HIPA. Dr. Narang (and all other physicians) should be made aware of the offense provisions set out in HIPA.

[73] Until Dr. Narang has demonstrated his understanding of HIPA and the SHA's expectations and has agreed to conduct himself accordingly, I recommend that Dr. Narang's access to the EMR be suspended.

Dated at Regina, in the Province of Saskatchewan, this 26th day of October, 2021.

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