Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 108-2024

Dr. Siva Karunakaran
(Prairie Internal Medicine Specialists)

September 20, 2024

Summary: The Complainant raised concerns with eHealth Saskatchewan (eHealth) regarding certain accesses to their personal health information in the eHR Viewer by the Office Manager at Prairie Internal Medicine Specialists (the Clinic). eHealth investigated the matter and determined that the accesses by the Clinic Office Manager were inappropriate. eHealth suggested that the Complainant raise their concerns with Dr. Siva Karunakaran (Dr. Karunakaran) at the Clinic. The Complainant did not receive a response from Dr. Karunakaran. Therefore, the Complainant requested that the Commissioner conduct an investigation. The Commissioner made a number of findings, including that privacy breaches occurred when the Office Manager accessed the Complainant's personal health information in the eHR Viewer and that the Office Manager ought to have known that accessing the Complainant's personal health information was inappropriate. The Commissioner also found that the root cause of the privacy breach was when the Office Manager disregarded office policies, procedures and training. The Commissioner made a number of recommendations, including recommending that Dr. Karunakaran and eHealth forward their investigation files to the Ministry of Justice and Attorney General, Public Prosecutions Division, to allow prosecutors to further consider whether an offence has occurred and if charges should be laid under HIPA or any other statute.

I BACKGROUND

[1] According to eHealth Saskatchewan's (eHealth) website, the eHR Viewer is a secure website that authorized health care providers can use to access patient information.

[2] eHealth logs accesses to the eHR Viewer by health care providers. Patients are able to contact eHealth and request a copy of an audit report to see who has accessed their personal health information. In this case, the Complainant did just that. After reviewing the audit report, they became concerned over accesses to their personal health information by the Office Manager at Prairie Internal Medicine Specialists (Clinic). The audit report showed that the Office Manager accessed the Complainant's personal health information on the following dates:

- 28 times on April 21, 2021 (accesses were from 7:56 a.m. to 4:51 p.m.),
- 5 times on April 22, 2021 (accesses were at 9:50 a.m.), and
- 4 times on August 10, 2022 (accesses were from 4:38 p.m. to 4:39 p.m.).

[3] The Complainant raised their concerns with eHealth. eHealth conducted an investigation.

[4] In a letter dated November 29, 2022, eHealth informed the Complainant of the results of its investigation. eHealth said:

> This letter is in follow-up to your concern regarding certain audit events on your eHR Viewer audit report. **I regret to inform you that during this investigation we identified that all of the eHR Viewer events in question were inappropriate accesses to your personal health information.**
>
> …
> Access to the eHR Viewer is subject to the eHR Viewer Joint Services and Access Policy. This policy states that the eHR Viewer is to be used only for the purpose of supporting or providing care to the patient to whom the information and to whom the healthcare provider is providing current health services. All employees at the clinic, including [name of the Office Manager], have bene reminded of this and we have been reassured this will not happen again. eHealth Saskatchewan will continue to audit and monitor their use of the eHR Viewer.
>
> [Emphasis added]

[5] eHealth recommended to the Complainant that they raise their concerns with Dr. Siva Karunakaran (Dr. Karunakaran) at the Clinic.

[6] On March 7, 2024, the Complainant addressed a letter to Dr. Karunakaran and dropped it off at the Clinic. The Complainant described that they were upset over the privacy breach. The Complainant said that they sought "legal action to be taken against [name of Office Manager]". The Complainant asked Dr. Karunakaran to respond within 30 days. Dr. Karunakaran did not respond within 30 days.

[7] On April 3, 2024, the Complainant contacted my office. On April 8, 2024, the Complainant confirmed that they were requesting that my office undertake an investigation into this matter.

[8] On May 15, 2024, my office notified both the Complainant and Dr. Karunakaran that my office would be undertaking an investigation.

[9] In a letter dated July 19, 2024, a lawyer representing Dr. Karunakaran provided a letter in response to my office's notice.

II DISCUSSION OF THE ISSUES

1. Do I have jurisdiction?

[10] *The Health Information Protection Act* (HIPA) is engaged when three elements are present: 1) a trustee, 2) personal health information, and 3) the trustee has custody or control over the personal health information. Below is an analysis to determine if HIPA is engaged. If so, then I would have jurisdiction to conduct this investigation.

1) Trustee

[11] Subsection 2(1)(t) of HIPA defines "trustee" as follows:

> **2**(1) In this Act:
>
> ...
> (t) **"trustee"** means any of the following that have custody or control of personal health information:

> ...
> (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;
> …
> ...
> (xv) any other prescribed person, body or class of persons or bodies;

[12] I note that subsection 4(b) of *The Health Information Protection Regulations, 2023* (HIPA Regulations) provides:

> **4** For the purposes of subclause 2(1)(t)(xv) of the Act, the following are prescribed as trustees:
>
> ...
> (b) every person who owns or operates a privately-owned facility in or from which health services are provided by a health professional;

[13] According to the Clinic's entity profile report on ISC's Corporate Registry, the proprietor of Prairie Internal Medical Specialist is (101258413) MNK Management Ltd. According to the entity profile report on ISC's Corporate Registry, there are three shareholders for (101258413) MNK Management's Ltd, one of which is Dr. Karunakaran.

[14] Dr. Karunakaran is licensed pursuant to *The Medical Profession Act, 1981*. As such, I find that Dr. Karunakaran qualifies as a trustee pursuant to subsection 2(1)(t)(xii)(A) and 2(1)(t)(xv) of HIPA and subsection 4(b) of the HIPA Regulations.

2) Personal health information

[15] The audit report produced by eHealth includes a column entitled "Event Description", which describes the information viewed by the Office Manager. The event descriptions are as follows:

- View Patient Summary,
- View Patient Lab Summary,

- View Clinical Encounters,
- View Clinical Document,
- View Patient Lab Details,
- View Medical Imaging Report Event, and
- View Patient Prescription Profile.

[16] Such information qualifies as "personal health information" as defined by subsections 2(1)(m)(i), (iii) and (iv) of HIPA, which provide as follows:

> **2**(1) 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;
> …
> (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;
>
> …
> (v) registration information;

3) Custody or control of the personal health information

[17] Subsection 2(1) of the HIPA Regulations define "employee" as follows:

> 2(1) In these regulations:
> ...
> **"employee"** means:
>
> (a) an individual:
>
> (i) who is employed by a trustee, including an individual retained under a contract to perform services for the trustee; and
>
> (ii) who has access to personal health information;

[18] When an employee at the Clinic views personal health information from the eHR Viewer, that view is a collection of personal health information. Therefore, I find that Dr. Karunakaran, as a shareholder of (101258413) MNK Management LTD., has custody and control over the personal health information at issue.

[19] Since all three elements are present, HIPA is engaged. Therefore, I find that I have jurisdiction to undertake this investigation.

2. Did a privacy breach occur?

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

[21] The need-to-know principle is the principle that trustees and their employees should only collect, use, or disclose necessary for the diagnosis, treatment or care of an individual or other purposes authorized by HIPA. The need-to-know principle is enshrined in section 23 of HIPA as follows:

> **23**(1) A trustee shall collect, use or disclose only the personal health information that is reasonably necessary for the purpose for which it is being collected, used or disclosed.
>
> (2) A trustee must establish policies and procedures to restrict access by the trustee's employees to an individual's personal health information that is not required by the employee to carry out the purpose for which the information was collected or to carry out a purpose authorized pursuant to this Act.
>
> …
> (4) A trustee must, where practicable, use or disclose only de-identified personal health information if it will serve the purpose.

[22] Further, section 24 of HIPA restricts the collection of personal health information by trustees. It provides:

> **24**(1) A trustee shall ensure that the primary purpose for collecting personal health information is for the purposes of a program, activity or service of the trustee that can reasonably be expected to benefit the subject individual.
>
> (2) A trustee may collect personal health information for a secondary purpose if the secondary purpose is consistent with any of the purposes for which personal health information may be disclosed pursuant to section 27, 28 or 29.
>
> (3) Nothing in this Act prohibits the collection of personal health information where that collection is authorized by another Act or by a regulation made pursuant to another Act.
>
> (4) A trustee may collect personal health information for any purpose with the consent of the subject individual.

[23] In the letter dated July 19, 2024 to my office, Dr. Karunakaran's lawyer indicated that the Complainant has never received treatment at the Clinic. The Complainant also stated this to my office. As such, the accesses by the Office Manager at the Clinic were not in accordance with sections 23 or 24 of HIPA. Therefore, I find that privacy breaches occurred when the Office Manager at the Clinic accessed the Complainant's personal health information without the authority to do so.

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

[24] In circumstances where I have found that a privacy breach (or breaches) has occurred, my office's investigation will focus on whether the trustee (or trustees) have properly responded to the privacy breaches.

[25] As set out in section 5-4 of my office's *Rules of Procedure* and my office's *Privacy Breach Guidelines for Health Trustees*, my office determines whether the trustee properly responded to the privacy breach by analyzing the trustee's efforts to:

- Contain the breach (as soon as possible);
- Notify affected individuals (as soon as possible);
- Investigate the privacy breach; and
- Prevent future breaches.

Contain the breach (as soon as possible)

[26] Upon learning that a privacy breach has occurred, steps should be taken to immediately contain the breach. Depending on the nature of the breach, this can include:

- Stopping the unauthorized practice;
- Recovering the records;
- Shutting down the system that has been breached;
- Revoking access privileges; and
- Correcting weaknesses in physical security.

(*Privacy Breach Guidelines for Health Trustees*, p. 3)

[27] Dr. Karunakaran's lawyer indicated that Dr. Karunakaran was unaware of the privacy breaches until being notified by eHealth "in or around the summer of 2022." At that point, the Office Manager's access to the eHR Viewer was revoked for a period of approximately six months. Once the access privileges were reinstated, the Office Manager was subject to random audits, "each of which was returned without issue", according to Dr. Karunakaran's lawyer.

[28] The revocation of the Office Manager's access to the eHR Viewer is evidence that Dr. Karunakaran made efforts to prevent the Office Manager from continuing to breach the Complainant's (or anyone else's) personal health information. Dr. Karanukaran should have also taken steps to determine if the Office Manager had disseminated the Complainant's personal health information when they viewed it and, if so, taken steps to recover it. This could have been accomplished by:

1) interviewing the Office Manager and asking what they did with the Complainant's personal health information;
2) reviewing the Office Manager's work email account on or around the days the unauthorized accesses occurred;

3) reviewing the Office Manager's work phone on or around the days the unauthorized access occurred; and/or

4) reviewing printer logs on or around the days the unauthorized accesses occurred to determine if the Office Manager had printed the Complainant's personal health information.

[29] Based on this, I find that Dr. Karunakaran should have taken further steps to contain the privacy breach.

[30] I recommend within 30 days of the issuance of this Investigation Report that Dr. Karunakaran take the steps outlined at paragraph [28] to determine if the Office Manager disclosed the Complainant's personal health information any further. If so, I recommend that Dr. Karunakaran take steps to recover/contain the Complainant's personal health information as much as possible. Dr. Karunakaran should inform my office and the Complainant of the results of efforts to further recover/contain the Complainant's personal health information within 30 days of issuance of this Investigation Report.

Notify affected individuals (as soon as possible)

[31] It is best practice to inform affected individuals when their personal health information has been a part of a privacy breach (*Privacy Breach Guidelines for Health Trustees*, p. 3). This is an important step so that the trustee can identify possible risks to the affected individuals and to inform them of steps they can take to protect themselves.

[32] However, in this case, the affected individual is the Complainant. They were the one who discovered the privacy breach and notified Dr. Karunakaran of the unauthorized accesses to their personal health information. Therefore, Dr. Karunakaran did not have to notify the Complainant and make them aware of the privacy breach. Nevertheless, Dr. Karunakaran's lawyer indicated that Dr. Karunakaran had spoken to and apologized to the Complainant, including providing reassurance to the Complainant that a similar incident would not occur again.

Investigate the privacy breach

[33] When considering why a privacy breach occurred, a trustee should reflect on the root causes, or what led to the breach occurring. It is an important step in mitigating the risk of a future breach of a similar nature from occurring (*Privacy Breach Guidelines for Health Trustees*, p. 5).

[34] Dr. Karunakaran's lawyer indicated that the Office Manager initially explained that the Clinic occasionally receives referrals and/or medical information intended for physicians who do not practice at the clinic. The Office Manager stated that they accessed the Complainant's personal health information in August 2022 in order to identify the physician to whom they (the Office Manager) should forward correspondence they had received in error. In response to the Office Manager's explanation, Dr. Karunakaran instructed the Office Manager to return incorrectly addressed referrals and/or medical information to the original sender, and to not access the eHR Viewer for this reason.

[35] However, regarding the accesses in April 2021, Dr. Karunakaran was able to determine that the Complainant has a connection to a friend of the Office Manager's family member. Dr. Karunakaran believes that at around the time of the breach, the Complainant was giving birth to a child. Dr. Karunakaran believes that the Office Manager accessed the Complainant's personal health information for the purpose of obtaining information about the birth of the Complainant's child.

[36] Dr. Karunakaran's lawyer indicated that the Clinic developed a manual, *The Privacy and Security Policies Manual*, in July 2016:

> The Privacy and Security Policies Manual (the "Policy Manual") was developed by the Clinic in July 2016. Dr. Karunakaran was familiar with it prior to this incident and advises all staff at the Clinic were required to review and acknowledge it prior to commencing employment. [Name of Office Manager] indicated she was familiar with the Policy Manual; however, her actions clearly contradicted it.

[37] Dr. Karunakaran's lawyer provided my office with a copy of *The Privacy and Security Policies Manual* (Policy Manual). The Policy Manual includes several policies authored by the Office Manager, including:

- Responsibilities of the Privacy Officer and the Officer Manager;
- Obligations of Health Professionals, Employees, Medical Students and Residents;
- Privacy and Security Awareness, Education and Training;
- Accuracy and Integrity;
- Identified Purpose and Openness;
- Challenging Compliance;
- Ceasing to be a Physician at Prairie Internal Medicine Specialists;
- Patient Access to Own Record;
- Amending Patient Record Upon Request;
- Authorized Representatives Who Make Decision on Behalf of Patients;
- Collection;
- Use;
- Disclosure;
- Managing Patient Consent and Masking in the EMR;
- Agreements;
- Management of Breaches;
- Business Continuity and Disaster Recovery Plan;
- Retention, Storage and Destruction of Paper Records;
- Scanning and Destruction of Paper Records;
- Backups and Storage;
- User Account Management;
- Auditing;

- Destruction of Office Equipment and Medical Devices Retaining Personal Health Information;
- General Security Software; and
- Security of the Office.

[38] Earlier, I had noted that when an employee at the Clinic views personal health information from the eHR Viewer, that view is a collection of personal health information. I note that the section entitled "Collection" in the Policy Manual provides as follows:

> Prairie Internal Medicine Specialists collects only the personal health information that is reasonably necessary to provide care and treatment to benefit its patients.

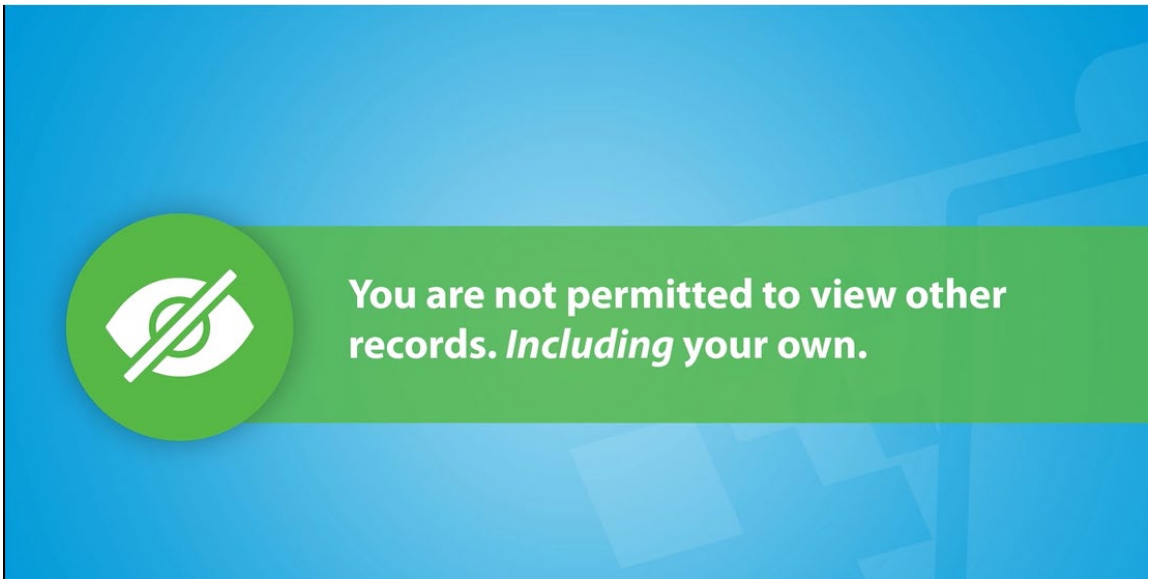
[39] The policy also cites sections 6, 19, 20, 23, 24, 25, 27, 28 and 29 of HIPA as the "legislative reference" for the policy.

[40] I also note that the policy entitled "Management of Breaches" outlines the penalties of unintentional and willful breaches of privacy as follows:

> 16.1. Users who unintentionally collect, use, access or disclose personal health information without authorization are subject to all or any of the following:
>
> - further privacy training
> - loss of privileges to use the [electronic medical record]
> - suspension without pay for one day
> - dismissal
>
> 16.2. Users who willfully collect, use, access or disclose personal health information without authorization are subject to all or any of the following:
>
> - further privacy training
> - loss of privileges to use the [electronic medical record]
> - suspension without pay for up to five days
> - dismissal

[41] Since the Office Manager was the author of the policies in the Policy Manual, then they ought to have been aware that snooping upon the Complainant's personal health information was inappropriate.

[42] Further, as noted in eHealth's letter dated November 29, 2022 to the Complainant, eHealth noted that all users of the eHR Viewer are subject to the eHR Viewer Joint Services and Access Policy. When registering for access privileges to the eHR Viewer, users are required to view the eHR Viewer Privacy Video. At the 41 second mark, the video clearly states that by agreeing to the JSAP, users agree to only access the records of patients to whom they are providing care or treatment to. Users are not to access other records, including their own:



[43] At the one minute and 12 second mark, the video provides that it is an offence under HIPA to access the eHR under false pretenses or where they are not authorized to do so. Doing so qualifies as a privacy breach and is punishable by a fine up to $50,000 and imprisonment of up to one year:

[44] While proper policies, procedures and training is effective at minimizing and preventing future privacy breaches in some cases, the root cause is not the lack of policies, procedures and training. Rather, the Office Manager ought to have known that repeatedly accessing the eHR Viewer was inappropriate, and so I find the root cause of the privacy breach is that the Office Manager disregarded office policies, procedures and training.

[45] I note that Dr. Karunakaran's lawyer's letter dated July 19, 2024, said that patient safety or care would unlikely be affected:

> It is unlikely that patient safety or care will be adversely affected by this breach. There is no foreseeable risk to public health or safety.

[46] I disagree. When users of the eHR Viewer use the system for illegitimate purposes, patients' trust in the health care system, including their own health care provider, is adversely affected. In my office's Investigation Report 308-2017, 309-2017, 310-2017, I explained the consequences of users of the eHR Viewer accessing information inappropriately:

> [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.

[47] Unfortunately, my office continues to investigate inappropriate accesses to the eHR Viewer and other systems containing patient information, including my recent Investigation Report 168-2024, 177-2024, 178-2024, 179-2024. In that investigation, my office found that the privacy of 114 people was breached when one user of the eHR Viewer misused their access privileges to satisfy their own personal curiosity. In another investigation, my office had found that healthcare workers had even gone as far as altering medical records, such as the case in Investigation Report H-2013-001. Altered records could no doubt affect the care or treatment a person receives.

[48] I caution anyone who believes that snooping does not adversely affect patient safety or care. It does.

Prevent future breaches

[49] The most important part of responding to a privacy breach is to implement measures to prevent future breaches from occurring (*Privacy Breach Guidelines for Health Trustees*, p. 6). Prevention steps include strategies such as adding/enhancing safeguards, providing additional training, monitoring or auditing systems and users, and providing additional training.

[50] In the letter dated July 19, 2024, Dr. Karunakaran's lawyer said:

> [Office Manager's name]'s access to eHealth Saskatchewan was suspended for approximately six months and [they] received one-on-one training from Dr. Karunakaran regarding proper privacy policies and procedures. It was important to Dr. Karunakaran to ensure [name of Office Manager] understood the severity of [their] actions and the consequences of the privacy breach.
>
> The Clinic is taking the following actions to prevent further privacy breaches:

- reviewing and updating all existing privacy policies and procedures at the Clinic;

- ensuring signed copies of all confidentiality agreements between the Clinic and its staff are obtained and kept on record;

- coordinating with the Saskatchewan Medical Association for the review of the updated privacy policies and procedures, as well as the implementation of further privacy policies and procedures; and

- developing initial and ongoing privacy training for all physicians and staff members of the Clinic.

The Clinic will meet with the Clinical Advisor for the Saskatchewan Medical Association ("SMA") in the near future to develop and review updated and further privacy policies and procedures. It is anticipated that these privacy policies and procedures will be implemented within 30 days of meeting with the SMA.

[51] Suspending the Officer Manager's access to the eHR Viewer, and then monitoring their access once reinstated, was a positive step taken by eHealth. It is also positive that Dr. Karunakaran provided some additional training to the Office Manager – this is a step I would expect Dr. Karunakaran to have taken.

[52] What is troubling about the inappropriate accesses by the Office Manager, however, is that they were well-aware that accessing the Complainant's personal health information was not authorized by HIPA but did so anyway. Afterall, the Office Manager was the author of the clinic's privacy policies. While eHealth and Dr. Karunakaran took some steps to address the root cause, I find they should do more.

[53] Subsections 64(1) and (2) of HIPA provides:

64(1) No person shall:

(a) knowingly contravene any provision of this Act or the regulations;

(2) Every person who contravenes subsection (1) or (1.1) is guilty of an offence and is liable on summary conviction:

(a) in the case of an individual, to a fine of not more than $50,000, to imprisonment for not more than one year or to both; and

(b) in the case of a corporation, to a fine of not more than $500,000.

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

[55] I also recommend that Dr. Karunakaran contact eHealth to establish a plan to conduct random user audits of all employees at the Clinic on an ongoing basis to ensure all employees at the Clinic are accessing the eHR Viewer in accordance with HIPA.

[56] If the Office Manager continues to have access to the eHR Viewer, I recommend that eHealth continue to audit this individual indefinitely. This includes if they work at the Clinic or at any other place that requires them to have access to the eHR Viewer.

III FINDINGS

[57] I find that I have jurisdiction to undertake this investigation.

[58] I find that privacy breaches occurred when the Office Manager at the Clinic accessed the Complainant's personal health information without the authority to do so.

[59] I find that Dr. Karunakaran should have taken further steps to contain the privacy breach.

[60] I find the root cause of the privacy breach is that the Office Manager disregarded office policies, procedures and training.

[61] While eHealth and Dr. Karunakaran took some steps to address the root cause, I find they should do more.

IV RECOMMENDATIONS

[62] I recommend within 30 days of the issuance of this Investigation Report that Dr. Karunakaran take the steps outlined at paragraph [28] to determine if the Office Manager disclosed the Complainant's personal health information any further. If so, I recommend that Dr. Karunakaran take steps to recover/contain the Complainant's personal health information as much as possible. Dr. Karunakaran should inform my office and the Complainant of the results of efforts to further recover/contain the Complainant's personal health information within 30 days of issuance of this Investigation Report.

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

[64] I recommend that Dr. Karunakaran contact eHealth to establish a plan to conduct random user audits of all employees at the Clinic on an ongoing basis to ensure all employees at the Clinic are accessing the eHR Viewer in accordance with HIPA.

[65] If the Office Manager has access to the eHR Viewer, I recommend that eHealth continues to audit this individual indefinitely. This includes if they work at the Clinic or at any other place that requires them to have access to the eHR Viewer.

Dated at Regina, in the Province of Saskatchewan, this 20th day of September, 2024.

Ronald J. Kruzeniski, K.C.
A/Saskatchewan Information and Privacy Commissioner