Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 082-2025[1]

eHealth Saskatchewan

-and-

Dr. Yang Zhan (Regina Cardiology Clinic)

-and-

Danniela Morgan

PART 2 – PRIVACY BREACH IN 2024/2025

April 8, 2026

Summary: In November of 2020, Ms. Danniela Morgan was hired by eHealth Saskatchewan (eHealth) as a Registry Administrator. Ms. Morgan was provided access to two electronic health database systems: (1) Panorama; (2) Panorama COVID Quick Entry (CQE); and one application - the Shared Client Index Enterprise Viewer (SCI). Ms. Morgan worked at eHealth until October 2021. Ms. Morgan's access to the three electronic health systems was terminated on her last day with eHealth, October 1, 2021.

eHealth conducted its own investigation into Ms. Morgan's activities for the period of 2020-2021 when she was employed solely by eHealth. The results of that investigation forms the basis of *Investigation Report 166-2025 (Part 1)*. eHealth determined that Ms. Morgan had committed a privacy breach by snooping on the personal health information of 6 individuals while employed by eHealth from November 2020 to October 2021.

[1] The other investigation file numbers associated with the investigation are 138-2025, 139-2025, 140-2025.

In August 2024, Danniela Morgan signed an employment contract with Dr. Yang Zhan (Dr. Zhan) to work at Dr. Zhan's clinic, the Regina Cardiology Clinic. On September 9, 2024, Ms. Morgan was charged with several *Criminal Code* offences that included one count of fraud over $5,000, one count of fraud under $5,000, two counts of identity theft and two counts of identity fraud. In October 2024, she was granted unsupervised access to the eHealth Saskatchewan (eHealth) web-based electronic health record (eHR) Viewer while working for Dr. Zhan. Upon being granted access to the eHR Viewer, Ms. Morgan made unauthorized accesses of personal health information without a legitimate need-to-know basis. Ms. Morgan left Dr. Zhan's employ in February 2025 but continued to have access to the eHR Viewer because Dr. Zhan failed to revoke her access on the last day of her employment. Ms. Morgan continued to access personal health information in the eHR Viewer until April 2025 when an affected individual contacted eHealth with concerns respecting the illegitimate access of their personal health information. eHealth immediately revoked Ms. Morgan's access to the eHR Viewer. With the assistance of Dr. Zhan, eHealth then investigated further and determined that Ms. Morgan had accessed the personal health information of 23 individuals as well as her own personal health information in the eHR Viewer without the need to know requirement. OIPC undertook an investigation and made several findings in this case, including that the privacy breach occurred because of Ms. Morgan's willful actions as a rogue employee.

The privacy breach involving Dr. Zhan's clinic is covered by this *Investigation Report 082-2025 (Part 2)*. However, because the snooper in these two matters, Danniela Morgan, is the same person, *Investigation Report 166-2025 (Part 1)* and *Investigation Report 082-2025 (Part 2)* we are treating this case as one continuous snooping violation of *HIPA* over a period of many years and so the two Investigation Reports should be read together.

In this case, the Commissioner recommended that:

(1) Dr. Zhan ensure that he has in place written policies and procedures regarding annual privacy training for staff, routine audits and the revocation of access to both the EMR and eHR Viewer upon the termination of an employee's employment;

(2) Dr. Zhan offer credit monitoring to the affected individuals for a minimum of five years;

(3) eHealth agree to forbid Danniela Morgan future access to any clinical system containing personal health information systems;

(4) eHealth continue in its efforts to update its *User Access Recertification Policy*;

(5) eHealth implement a process for eHR Viewer user access recertification;

(6) eHealth implement a proactive audit and monitoring program for the eHR Viewer; and

(7) This matter be conveyed to the Attorney General of Saskatchewan for an opinion with respect to the prosecution of Danniela Morgan for the willful violation of *HIPA* pursuant to section 64(4) of *HIPA*.

TABLE OF CONTENTS

I BACKGROUND

[1] The eHealth Saskatchewan (eHealth) electronic health record (eHR Viewer) is a secure website for authorized health care workers and provides access to patient personal health information in this province.[2] Organizations seeking access to the eHR Viewer must complete the *eHealth Saskatchewan Organization Approval Request Form*[3] prior to receiving designation as an "Approved Organization." Approved Organizations must identify at least one individual within the organization as an "Authorized Approver." Authorized Approvers receive email requests from members of the organization who require access to the eHR Viewer ("Users"). Upon approval by the Authorized Approver, Users are allowed to access to the eHR Viewer to carry out their job duties.

[2] On November 30, 2017, an employee of the Regina General Hospital, Danniela Morgan, was provided access to the eHR Viewer as a User.[4] When she first logged into the system, she had to accept the *eHR Viewer Joint Services/Access Policy* (JSAP) *Acknowledgements* (*eHR Viewer JSAP Acknowledgements*). The *eHR Viewer JSAP Acknowledgements* sets out the rules in which she was to use the eHR Viewer, including the provision that she only access personal health information on a need-to-know basis. Ms. Morgan's access to the eHR Viewer in connection with the Regina General Hospital terminated on April 5, 2018.

[3] On July 18, 2023, Dr. Yang Zhan (Dr. Zhan) of Dr. Yang Zhan Medical Prof Corp (publicly known as Regina Cardiology Clinic) submitted an *eHealth Saskatchewan Organization Approval Request Form* to eHealth to become an Approved Organization. Dr. Zhan identified himself as the Authorized Approver.

---

[2] *eHealth Viewer*. eHealth Saskatchewan: https://www.ehealthsask.ca/services/ehr-viewer/Pages/default.aspx

[3] *eHealth Saskatchewan Organization Approval Request Form*. eHealth Saskatchewan: https://www.ehealthsask.ca/forms/Forms/eHealthSaskatchewanOrganizationApprovalRequestForm-%20Nov%202023.pdf.

[4] The Regina General Hospital is a facility of the Saskatchewan Health Authority.

[4] On August 30, 2024, Danniela Morgan commenced employment with Dr. Zhan as a Medical Office Assistant at the Regina Cardiology Clinic.

[5] On September 9, 2024, Regina Police Service issued a public news release indicating that Danniela Morgan had been charged with several offences contrary to the *Criminal Code*:[5] one count of fraud over $5,000 [section 380(1)(a)], two counts of fraud under $5,000 [section 380(1)(b)], two counts of identity theft [section 402.2(1)] and two counts of identity fraud [section 403(1)(a)].[6]

[6] On October 29, 2024, eHealth's Access Management Services (AMS) Unit processed a request from Dr. Zhan's employee, Danniela Morgan, for access to the eHR Viewer under Dr. Yang Zhan Medical Prof Corp.

[7] On October 30, 2024, Dr. Zhan, as an Authorized Approver, approved Danniela Morgan's access to the eHR Viewer. Danniela Morgan had already accepted the *eHR Viewer JSAP Acknowledgements* in 2017, so she did not have to re-accept the acknowledgements when logging into the eHR Viewer in October of 2024.

[8] Also on October 30, 2024, Danniela Morgan began accessing the eHR Viewer in an unsupervised capacity which is questionable in light of the nature of the criminal charges two months prior. She accessed the personal health information of 23 individuals, including her own personal health information, without the requisite need-to-know precondition as required by *The Health Information and Protection Act* (*HIPA*).[7]

[9] Commencing on January 19, 2025, eHealth required all users of the eHR Viewer to accept an updated version of the *eHR Viewer JSAP Acknowledgements* at their next login. eHealth

[5] *Criminal Code*, RSC 1985, c. C-46, as amended.

[6] *Female Faces Fraud Charges.* Regina Police Service (September 9, 2024).

[7] *The Health Information Protection Act*, S.S. 1999 c. H-0.021, as amended.

required all users to have to read and accept the updated acknowledgements. The updated acknowledgements read:

> Your use of the eHR Viewer is subject to *The Health Information Protection Act* (HIPA) and the eHR Viewer Joint Services/Access Policy (JSAP). Before accessing the eHR Viewer you must read the JSAP which is available on the eHealth Saskatchewan website.
>
> The eHR Viewer is ONLY to be used on a need-to-know basis to access personal health information (PHI) of individuals who are currently in your care. Access MUST be limited to the minimum amount of information needed to provide or support the individual's health care service.
>
> By clicking accept below, you agree to be bound by the terms and conditions of the JSAP. Any violations may result in removal of your eHR Viewer access privileges. Remember:
>
> - Your actions in the eHR Viewer are audited and monitored.
> - You are NOT permitted to access your own PHI.
> - You are not permitted to access PHI about:
>   - your spouse,
>   - family members,
>   - friends,
>   - acquaintances,
>   - co-workers,
>   - public figures, or
>   - any other person you are not providing health services to.
> - You cannot use the eHR Viewer to access PHI for curiosity, billing, quality improvement or research (even if approved by a Research Ethics Board).
> - You cannot use the eHR Viewer to check up on a patient's condition or to follow-up on a patient that is no longer in your care.
> - Do not share your password with others. You are responsible for all activities conducted under your user account.

[10] On January 20, 2025, Ms. Morgan logged into the eHR Viewer and accepted eHealth's new and revised *eHR Viewer JSAP Acknowledgements.* Ms. Morgan acknowledged that as a user, she would only access the personal health information of all Saskatchewan residents on a need-to-know basis.

[11] Regardless, Ms. Morgan continued to access personal health information in the eHR Viewer of several residents of Saskatchewan, including her own, without the requisite need-to know.

[12] Ms. Morgan's last day of employment at Dr. Zhan's office was February 7, 2025. Dr. Zhan failed to revoke her access to the eHR Viewer. Since the eHR Viewer is web-based, Ms. Morgan continued to access personal health information in the eHR Viewer up to and including March 6, 2025.

[13] On April 11, 2025, a resident of Saskatchewan contacted eHealth to report concerns that someone accessed their personal health information. On that same day, eHealth ran an audit report and identified "trigger events" that suggested Ms. Morgan had accessed personal health information inappropriately. eHealth revoked Ms. Morgan's user access to the eHR Viewer on this date.

[14] Also on April 11, 2025, eHealth contacted Dr. Zhan. Dr. Zhan co-operated with eHealth to identify which of Ms. Morgan's accesses to the eHR Viewer were legitimate and which were not. Dr. Zhan identified various patient profiles that were accessed by Ms. Morgan that were not his patients. Any patient information accessed by Ms. Morgan after February 7, 2025 was easily identified as illegitimate accesses.

[15] In total, it was determined that Ms. Morgan accessed the personal health information of 23 individuals without the requisite need-to-know precondition as required by *HIPA*.

[16] On April 21, 2025, eHealth proactively reported this privacy breach to the Office of the Saskatchewan Information and Privacy Commissioner (OIPC).

[17] On May 2, 2025, and May 8, 2025, eHealth sent notices to affected individuals. Several affected individuals contacted eHealth with their concerns.

[18] On June 6, 2025, this office received complaints from two of the 23 affected individuals.

[19] On August 14, 2025, OIPC notified eHealth, Dr. Zhan, Ms. Morgan and the two affected individuals that OIPC would be undertaking an investigation.

[20] On September 12, 2025, eHealth provided a submission to OIPC.

[21] On September 19, 2025, legal counsel for Dr. Zhan provided a submission to OIPC.

[22] On September 22, 2025, Ms. Morgan provided a submission to OIPC.

II DISCUSSION OF THE ISSUES

1. Jurisdiction

a. HIPA

[23] *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.

i. First element – trustees

[24] eHealth qualifies as a trustee pursuant to section 2(1)(t)(i) of *HIPA*.

[25] Dr. Zhan qualifies as a trustee pursuant to sections 2(1)(t)(xii)(A), 2(1)(xv) of *HIPA* and section 4(b) of *The Health Information Protection Regulations*.[8]

[8] *The Health Information Protection Regulations, 2023*, RRS c H-0.021 Reg 2 (effective August 1, 2023), as amended by Saskatchewan Regulations 68/2023.

ii. Second element – personal health information

[26] At issue is the information accessible via the eHR Viewer. Through the eHR Viewer, users can view the following categories of medical information that is logged with respect to the residents of Saskatchewan:[9]

- Laboratory Results;
- Medical Imaging Reports;
- Clinical Documents;
- Hospital Visits;
- Surgical appointments;
- Medication information;
- Immunization information;
- Chronic Disease Management Information.

[27] This medical information qualifies as "personal health information as defined by section 2(1)(m):[10]

> **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;
>
> (ii) information with respect to any health service provided to the individual;
>
> ...
> (iv) information that is collected:
>
> (A) in the course of providing health services to the individual; or

[9] *Available information and updates to the eHR Viewer*. eHealth Saskatchewan: https://www.ehealthsask.ca/services/ehr-viewer/Pages/Notifications.aspx.

[10] This office has previously found that information accessible via the eHR Viewer qualifies as personal health information as defined by section 2(1)(m) of *HIPA*: Investigation Report 290-2024, 007-2025 at paragraph [9], Investigation Report 108-2024 at paragraph [16], and Investigation Report 168-2024 at paragraph [8].

(B) incidentally to the provision of health services to the individual; or

(v) registration information;

iii. Third element - Do the trustees have custody and/or control over the personal health information?

[28] "Custody" is the physical possession of a record by a trustee combined with a measure of control. "Control" connotes authority. Personal health information is under the control of a trustee when the trustee has authority to manage the information, including restricting, regulating and administering its use, disclosure or disposition. Custody is not a requirement for control to be present.[11]

A. eHealth

[29] eHealth provided OIPC with a copy of the *eHR Viewer and Integration Joint Services/Access Policy (Data Access Agreement)* (*eHR Viewer JSAP*), which is the eHealth policy that governs how information within the eHR Viewer is to be accessed. The *eHR Viewer JSAP* provides that custody and control of this information remains at all times with eHealth:

> eHealth (the Ministry as trustee for PIP) will have custody and control of and make decisions regarding the use and disclosure of the EHR Data.

[30] We accept that eHealth has custody and control over the personal health information in the eHR Viewer.

B. Dr. Zhan

[31] When Dr. Zhan, or one of his employees[12], views personal health information through the eHR Viewer, *HIPA* designates that "view" as a "collection" of personal health information

[11] OIPC Investigation Report 036-2025 at paragraph [25].

[12] *Supra,* footnote 8. The regulations define "employee" as:

by Dr. Zhan.[13] As such, the information viewed by Ms. Morgan is simultaneously in the custody and control of Dr. Zhan and eHealth. The third element is met.

[32] Since both eHealth and Dr. Zhan have custody and control over the personal health information at issue, *HIPA* is engaged. OIPC has jurisdiction to undertake this investigation pursuant to the authority afforded by *HIPA*.

2. Did privacy a breach occur?

[33] A privacy breach occurs when personal health information is collected, used and/or disclosed without authority under *HIPA*.[14] Privacy breaches can also occur when personal health information is not appropriately safeguarded which is also the case here.[15]

[34] Earlier, OIPC noted that when Dr. Zhan or one his employees views personal health information in the eHR Viewer, that view qualifies as a collection of personal health information.

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; or

(b) an individual who, with the authorization of a trustee, acts on behalf of the trustee with respect to personal health information and for the purposes of the trustee, and not for the individual's own purposes, whether or not the individual has the authority to bind the trustee, is paid by the trustee or is remunerated by the trustee;

[13] Section 2(1)(b) of *HIPA* defines "collect" as: **"collect"** means to gather, *obtain access to*, *acquire*, receive or *obtain* personal health information from any source by any means;

[14] *Supra*, footnote 11 at paragraph [36].

[15] OIPC Investigation Report 015-2025 at paragraph [25].

[35] Section 23 of *HIPA* requires that a trustee only collect personal health information in accordance with the "need-to-know" principle. The need-to-know principle provides that trustees, and trustee employees, should only collect, use and/or disclose what is necessary for diagnosis, treatment or care of an individual or other purposes authorized by *HIPA*. Section 23 of *HIPA* provides, in part:

> **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.

[36] Further, section 24 of *HIPA* restricts the collection of personal health information by trustees as follows:

> **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.

[37] eHealth indicated it ran an audit report and identified "trigger events", such as same last-name look-ups and late-night views. It then requested Dr. Zhan to review the trigger events to determine if the views were of his patients. Dr. Zhan reviewed the list and identified 23 individuals who were not patients at his clinic. eHealth noted that these individuals

included Ms. Morgans's alleged partner, individuals who lived at the same address as the alleged partner, the officer who had arrested Ms. Morgan on the criminal matter, and the officer's spouse. Dr. Zhan indicated to eHealth that Ms. Morgan's last day under his employ was February 7, 2025, so any access on the part of Ms. Morgan to patient health information after that day clearly contravened the need-to-know principle.

[38] For Ms. Morgan to have accessed personal health information on the "need-to-know" basis in this case, the personal health information must be attributable to the patients of Dr. Zhan and as the result of Dr. Zhan's treatment of those patients. Since Ms. Morgan accessed her own personal health information and that of 23 individuals who were not the patients of Dr. Zhan without a need-to-know precondition, we conclude a sizeable privacy breach occurred.

3. Did eHealth and Dr. Zhan respond appropriately to the privacy breach?

[39] The analysis of a trustee's response to a privacy breach involves several factors. The considerations include:

a. Was the breach contained;
b. Were the affected individuals notified;
c. Was the breach investigated; and
d. Were appropriate steps taken to prevent future breaches.

a. Containment of the Breach

[40] Upon learning that a privacy breach occurred, a trustee should immediately take steps to contain the breach. These steps will depend entirely on the nature of the breach, but they include:[16]

- Stopping the unauthorized practice.
- Recovering the records.
- Shutting down the system that was breached.

[16] *Supra*, footnote 11 at paragraph [52].

- Revoking access to personal health information.
- Correcting weaknesses in physical security.

[41] This office applies a standard of reasonableness to assess the containment of a breach. The trustee must demonstrate that it reasonably reduced the magnitude of the breach and the resulting risk to affected individuals.[17]

[42] On April 11, 2025, eHealth revoked Ms. Morgan's access to the eHR Viewer. This is the date that eHealth learned of the privacy breach as well the fact that Ms. Morgan no longer worked for Dr. Zhan. As such, eHealth took immediate steps to contain this privacy breach. Later in this Investigation Report, we acknowledge that eHealth also added Ms. Morgan's name to its Service Desks' watchlist which forwards any future request on the part of Ms. Morgan for access to the Privacy, Access and Patient Safety Unity of eHealth for careful review.

[43] In the case of Dr. Zhan, the hiring took place on August 30, 2024, and we understand that the presumption of innocence applies to Ms. Morgan when she was charged with the criminal offences on September 9, 2024. However, the charges are of such a concern (fraud, identity theft and identity fraud), that common sense would have required supervision or monitoring of her access to the eHR Viewer when she was granted access to the database on October 30, 2024. No one can dispute that the eHR Viewer database presents as a tempting warehouse of sensitive information of all residents of Saskatchewan and should be jealously protected from those who are even suspected of fraud and identity theft.

[44] Sadly, we have to observe that Dr. Zhan was nothing short of negligent in failing to not only supervise Ms. Morgan's access to the eHR Viewer in the month following the criminal charges, but in abdicating his duty of trust to the people of Saskatchewan by failing to revoke Ms. Morgan's access to the eHR Viewer when she left his employ on February 7,

[17] OIPC Investigation Report 253-2024 at paragraph [23].

2025. As noted above, it was eHealth that finally revoked the access on April 11, 2025, some two months later.

b. Notification of Affected Individuals

[45] Best practice demands that trustees inform affected individuals as soon as possible when personal health information has been breached. This is an obvious and crucial step that invokes the principles of fairness. Affected individuals must be informed of the possible risks so they can take any remedial steps they deem necessary to protect themselves. An effective notice should include:[18]

- A general description of what happened.
- A detailed description of the personal health information involved (e.g., name, medical record, prescriptions, health services number, credit card information, etc.).
- A description of the types of harm that may possibly come 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 change a health services number).
- Contact information of an individual within the organization who can answer questions and provide information.
- A notice that individuals have a right to complain to the OIPC.
- Recognition of the impacts of the breach on affected individuals and an apology.

[46] eHealth notified 22 of 23 affected individuals of the privacy breach. The 23rd affected individual was not notified because they were deceased at the time of discovery of the breach. eHealth customized each letter to provide an overview of their personal health information as accessed by Ms. Morgan. eHealth also enclosed audit reports with each

[18] OIPC Investigation Report 168-2024 at paragraph [73].

letter to outline each occasion of a snoop access event, what information was accessed and the dates and times of each snoop access event.

[47] The notice letters also included advice to each individual to check their health record for any information that does not belong to them on their *MySaskHealthRecord*.[19] The letters included an apology as well as contact information of a Senior Privacy Analyst at eHealth in the event of questions. The notice letters informed the individuals of the right to complain to OIPC and the contact information for this office.

[48] Before this health privacy breach ever occurred, on September 9, 2024, Ms. Morgan was charged with fraud over $5,000, fraud under $5,000, two counts of identity theft and two counts of identity fraud. Since those charges are still extant, both eHealth and Dr. Zhan should have notified the affected individuals of the risk of identity theft and fraud in connection with this breach. Because of the willful violations of *HIPA* while under the watch of Dr. Zhan, we recommend that he offer credit monitoring to the affected individuals for a minimum of five years.[20]

c. Investigation of the breach

[49] Once the breach has been contained and appropriate notification has occurred, the trustee should conduct an internal investigation. The investigation should address the incident on a systemic basis and should include a root cause analysis. A root cause analysis should include a consideration of section 16 of *HIPA*, which sets out the trustee's duty to protect personal health information, which 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;

[19] *MySaskHealthRecord*, eHealth Saskatchewan: https://www.ehealthsask.ca/MySaskHealthRecord/MySaskHealthRecord.

[20] OIPC Investigation Report 009-2020 at paragraph [105]

(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.

[50] At the conclusion of its investigation, the trustee should understand the root cause of the breach with an eye to future prevention.[21] We have surmised the following as the root causes that that led and enabled Danniela Morgan to gain unauthorized accesses to personal health information. We have already noted that Dr. Zhan failed to monitor Ms. Morgan's access to the eHR Viewer upon her acceptance of employment at his clinic in the face of disturbing criminal charges one month later. To this failure we add:

i. Dr. Zhan failed to contact eHealth to terminate Ms. Morgan's access to the eHR Viewer

[51] Dr. Zhan signed the *eHealth Saskatchewan Organization Approval Request Form*[22] for his clinic to become an "Approved Organization" with access to the eHR Viewer. On that form, Dr. Zhan identified himself as the "Authorized Approver". As an Authorized Approver, Dr. Zhan's responsibilities included managing and deleting privileges for user account access for the organization. As an authorized approver, Dr. Zhan warranted that he had assumed the following responsibilities:

Authorized Approvers are responsible for ensuring that:

- Users complete the training available on the eHR Viewer Program Page as well as have read and understand their roles and responsibilities.
- Additions, deletions and changes in privileges for user account access is managed for the organization.

[21] *Supra,* footnote 18 at paragraphs [83] to [84].

[22] *Supra*, footnote 3.

- User access is audited on a regular basis.

[52] Dr. Zhan failed to notify eHealth when Ms. Morgan's employment with his clinic terminated. In his submission, Dr. Zhan explained that Ms. Morgan's access to the clinic's electronic medical record (EMR) was revoked immediately upon her leaving his employ on **February 7, 2025**. Surprisingly, Dr. Zhan failed to grasp that his clinic's EMR is not the same beast as the province's eHR Viewer. That is, by simply revoking access to his clinic's EMR and by not informing eHealth of the termination of employment of Ms. Morgan, Dr. Zhan allowed her to continue to access the eHR Viewer until **April 11, 2025** when eHealth finally terminated the access.

ii. Auditing

[53] OIPC and eHealth co-authored the resource *Audit and Monitoring Guidelines for Trustees.*[23] This document provides guidance to trustees in the establishment of a proactive auditing and monitoring program. The auditing of users' access to personal health information in electronic databases is a technical safeguard that enables trustees to speedily identify inappropriate access. It can also act as a deterrent to unauthorized access.[24]

[54] Dr. Zhan did not have auditing processes in place prior to this matter. Had there been such a feature in place, it is likely that Ms. Morgan's unauthorized accesses in the eHR Viewer would have been detected.

[55] Trustees may also request audit reports of their employees from eHealth. These audit reports show the personal health information that has been accessed by their employees. Trustees may then review to determine if the accesses were legitimate or not.

[23] *Audit and Monitoring Guidelines for Trustees*. OIPC and eHealth Saskatchewan: Audit and Monitoring Guidelines for Trustees | OIPC.

[24] OIPC Investigation Report 155-2025 at paragraph [56].

[56] eHealth conceded that a proactive audit and monitoring program would have assisted in the detection of this Snooper much earlier.

iii. eHealth User Access Recertification

[57] At the time of Ms. Morgan's unauthorized accesses, eHealth had formulated the *User Access Recertification Policy*. This policy requires eHealth to send a list of the current users to the appropriate trustee of the eHR Viewer to confirm valid access. While this policy existed, the procedure to recertify eHR Viewer users had not been implemented at the material time. Had the policy been implemented, Ms. Morgan's accesses to the eHR Viewer may have been caught soon after she left the employment with Dr. Zhan.

iv. Ms. Morgan's own actions

[58] Even if trustees have established reasonable administrative, technical and physical safeguards, it is important to determine if Ms. Morgan purposefully bypassed such safeguards in her unauthorized quest to snoop the personal health information of innocent victims.

[59] Ms. Morgan filed a submission with this office. She listed several reasons maintaining her innocence in the face of the allegations of unauthorized accesses to personal health information in the eHR Viewer. Below is a table that outlines her statements followed by the reasons that illustrated why her submissions are wrong in law and fact:

Ms. Morgan's Submissions	**OIPC Response**
"I was not provided with formal training or instructions regarding PHI handling under *The Health Information Protection Act* (*HIPA*) or related provincial legislation."	Ms. Morgan first accepted the *eHR Viewer JSAP Acknowledgements* in 2017 as an employee at the Regina General Hospital as well as on January 20, 2025, while as an employee of Dr. Zhan. *She knew and acknowledged as early as 2017 that personal health information is only to be accessed on a need-to-know basis.*

"I did not receive an employee handbook, nor was I asked to sign a confidentiality agreement."	Ms. Morgan signed an employment contract on August 30, 2024, between herself and Dr. Zhan and his clinic. Clauses 22 to 30 of the employment contract outlined that Ms. Morgan was to maintain the confidentiality of personal health information. Specifically, clause 23 outlined that Ms. Morgan agreed not to divulge, reveal, report or use, any confidential information as a result of being an employee of Dr. Zhan's clinic.
"Individual accounts were not assigned initially to her" so she "could not confirm whether all activity attributed to her credentials were performed" by her.	The *eHR Viewer JSAP Acknowledgements* explicitly stated that the user was not to share their unique password with others. The password and access to the system came with the acknowledgement that the user is responsible for all activities conducted under the user's personal account. Ms. Morgan accepted and acknowledged this agreement. Therefore, she was responsible for all activities conducted under her personal account and she was later audited on this account.
Ms. Morgan maintained she only accessed "patient information…in response to direct requests from patients, family members, or caregivers seeking support or clarification regarding care."	Dr. Zhan determined that Ms. Morgan accessed the personal health information of 23 individuals who were not patients of the clinic. As an aggravating feature to this set of facts, Ms. Morgan continued to access personal health information in the eHR Viewer *after* her employment at Dr. Zhan's clinic was terminated.

[60] Ms. Morgan's submissions lack credibility. We conclude that the violation of *HIPA* was willful in this case. We note that since the personal health information of the arresting

officer and their spouse were snooped upon – there was an element of willful and premeditated intent in this matter that is deeply disturbing.

d. Prevention of future breaches

[61] Prevention of future breaches is perhaps the most important step in responding to a privacy breach. A privacy breach cannot be undone but trustees can take concrete measures to prevent similar breaches in the future.[25]

i. Dr. Zhan

[62] In the spirit of preventive measures, Dr. Zhan has now implemented verbal training to his frontline staff regarding appropriate and inappropriate access of eHealth information. Further, he has commenced mandatory annual privacy training and will use the *eHR Viewer JSAP* as a resource to implement this privacy training as soon as possible.

[63] Dr. Zhan has committed to routine audits of frontline staff on the 1st and 15th of every month. These audits will include reviewing the personal information and personal health information accessed by staff. We commend him on these efforts.

[64] Further, Dr. Zhan confirms that he now understands that revoking access to the clinic's EMR is not the same as revoking access to the eHR Viewer. He indicated he will revoke access to both the EMR and the eHR Viewer upon the termination/end of any employee's employment in the future.

[65] Dr. Zhan should ensure that he has written policies and procedures available for all staff regarding annual privacy training, routine audits and the revocation of access to both the EMR and eHR Viewer upon the termination of an employees' employment.

ii. eHealth

[25] OIPC Investigation Report 193-2024 at paragraph [137].

[66] To prevent similar privacy breaches, eHealth has added Danniela Morgan's name to its Service Desks' watchlist. Any future requests for her to have access to provincial clinical health systems in Saskatchewan will be forwarded to the Privacy, Access and Patient Safety Unit of eHealth for careful review. From a privacy standpoint, this office recommends that Ms. Morgan has forfeited her ability to ever be granted access to future clinical systems containing personal health information of the people of Saskatchewan.

[67] eHealth also committed to several improvements for the future: (1) it is in the process of updating its *User Access Recertification Policy* and that it would implement a process for eHR Viewer user access recertification; and (2) it is looking at implementing a proactive audit and monitoring program for the eHR Viewer. Such a program will be necessary to ensure the protection of personal health information as our province's health care system evolves to increasingly rely on electronic system to deliver health care.

4. Section 64 of *HIPA*

[68] It is necessary to consider the merit of a referral of this matter to the Attorney General of Saskatchewan. It is crucial to ensure justice for the vulnerable citizens of Saskatchewan whose personal health information has been subjected to unauthorized access. It is also crucial to maintain trust and ensure the inviolability of health services of this province.

[69] In the publication *Detecting and Deterring Unauthorized Access to Personal Health Information*, the former Information and Privacy Commissioner of Ontario, Brian Beamish, advocated for an increase in prosecutions of those who access personal health information without the requisite need-to-know principle.[26]

[70] In Saskatchewan, individuals who are responsible for a violation under *HIPA* could be subject to the offense provisions in section 64 of *HIPA*. In this case, section 64 of *HIPA* requires consideration:

[26] *Detecting and Deterring Unauthorized Access to Personal Health Information* at page 9. Information and Privacy Commissioner of Ontario. January 2015.

> **64**(1) No person shall:
>
> (a) knowingly contravene any provision of this Act or the regulations;
>
> ...
> (3.2) An individual who is an employee of or in the service of a trustee and who wilfully accesses or uses or directs another person to access or use personal health information that is not reasonably required by that individual to carry out a purpose authorized pursuant to this Act is guilty of an offence and is liable on summary conviction to a fine of not more than $50,000, to imprisonment for not more than one year or to both, whether or not the trustee has been prosecuted or convicted.
>
> …
> (4) No prosecution shall be commenced pursuant to this section except with the express consent of the Attorney General of Saskatchewan.
>
> (5) No prosecution shall be commenced pursuant to this section after the expiration of two years after the date of the discovery of the alleged offence.

[71] For sections 64(1)(a) and (3.2) of *HIPA* to apply, the contravention would have to be proven to have been willful and committed with full knowledge. This office defines these terms as follows:[27]

> - A person who acts *knowingly* understands that the social harm will almost certainly be a consequence of the action but acts with other motives and does not care about whether the social harm occurs.
>
> - A voluntary act becomes *willful*, in law, only when it involves conscious wrong or evil purpose on the part of the actor, or at least inexcusable carelessness, whether the act is right or wrong.
>
> [Emphasis added]

[72] Based on the findings made in this Investigation Report, Danniela Morgan willfully and knowingly violated *HIPA* in this matter.

[73] This office has identified several factors that must be considered when consent is sought from the Attorney General for a prosecution of a matter of this nature. We list those factors

[27] *Supra*, footnote 25 at paragraph [154].

here: (1) overall strength of the case; (2) public interest in a prosecution; (3) harm to the community; (4) number of complaints from community; and (5) available litigation resources.[28]

[74] We find that most factors listed above can be adequately addressed by the factual matrix of this case. We are certain that this is a strong case especially since Ms. Morgan chose to snoop on the personal health information of her arresting officer with the Regina Police Service and that of their spouse. The mental element displayed by Ms. Morgan in connection with this case is aggravated by the fact that Ms. Morgan continued to snoop on the personal health information of individuals after she left the employ of Dr. Zhan. The element of willful intent to violate *HIPA* is without question. There can be no doubt that there is a public interest in this case and concern in connection with the nature of the outstanding criminal charges. The harm to the community is obvious and our office received complaints from two of the 22 violated individuals in this matter. One of the violated individuals is no longer around to complain.

[75] In the past, this office has publicly named those who willfully commit a personal health privacy breach. We have a duty to denounce the actions of Ms. Morgan and to reflect the community's adoption of a zero tolerance for violations of *HIPA*.[29] In publicly naming Danniela Morgan, we hope to increase awareness among health employers of the need to maintain vigilance with the provincial personal health information databases and the primacy of protecting personal health information in Saskatchewan.[30]

[28] OIPC Investigation Report 103-2025 at paragraph [80].

[29] *Supra,* footnote 24 at paragraph [78].

[30] *Stebner v Canadian Broadcasting Corporation*, 2019 SKQB 91 stands for the principle of the inherent right of this office to identify a willful snooper. In that case Danyliuk J. of the Saskatchewan Queen's Bench (as it then was) dismissed an application for injunctive relief and further dismissed an application for a publication ban at paragraphs [164] to [167] of that decision.

III FINDINGS

[76] eHealth and Dr. Zhan, as trustees, have custody and control over the personal health information at issue. As such, *HIPA* is engaged.

[77] OIPC has jurisdiction to undertake this investigation under the authority afforded under *HIPA*.

[78] Danniela Morgan committed a privacy breach when she accessed personal health information without a need-to-know basis.

[79] eHealth took steps to contain the privacy breach by revoking Danniela Morgan's access to the eHR Viewer, including registering her name on the eHealth Service Desks' watchlist to be forwarded to the Privacy, Access and Patient Safety Unity of eHealth for careful review.

[80] eHealth notified the affected individuals of the privacy breach but should have included information with respect to the nature of the risks involved.

[81] The root causes that enabled Ms. Morgan included:

(1) Dr. Zhan failed to monitor Danniela Morgan's access to the eHR Viewer and he failed to terminate her access to the eHR Viewer upon the termination of her employment with his clinic;

(2) Dr. Zhan did not have an auditing process in place so Ms. Morgan's unauthorized accesses went undetected;

(3) eHealth did not have a proactive audit and monitoring program in place so Ms. Morgan's unauthorized accesses went undetected;

(4) eHealth had not fully implemented a procedure to routinely recertify users of the eHR Viewer. Had it been implemented, Ms. Morgan's continued unauthorized access to the eHR Viewer beyond her last day of employment with Dr. Zhan's clinic may have been caught sooner; and

(5) Danniela Morgan willfully and intentionally violated the need to know principle associated with *HIPA*.

IV RECOMMENDATIONS

[82] I recommend that Dr. Zhan offer credit monitoring to the affected individuals for a minimum of five years.

[83] I recommend that Dr. Zhan ensure that he has written policies and procedures in place regarding annual privacy training for staff, routine audits and the revocation of access to both the EMR and eHR Viewer upon the termination of an employees' employment.

[84] I recommend that eHealth forbid future access to any clinical personal health information systems in Saskatchewan to Danniela Morgan.

[85] I recommend that eHealth continue updating its *User Access Recertification Policy*.[31]

[86] I recommend that eHealth implement a process for eHR Viewer user access recertification.

[87] I recommend that eHealth implement a proactive audit and monitoring program for the eHR Viewer.

[88] I recommend that this matter be conveyed to the Attorney General of Saskatchewan for an opinion with respect to the prosecution of Danniela Morgan for the willful violation of *HIPA* pursuant to section 64(4) of *HIPA*.

[31] OIPC will not attach timelines to this recommendation because eHealth is a demonstrated and commendable citizen when it comes to privacy matters. However, we note that if there are future violations involving this policy and its lack of implementation, we may have to submit to the imposition of timelines in the future.

Dated at Regina, in the Province of Saskatchewan, this 8th day of April, 2026.

Grace Hession David
Saskatchewan Information and Privacy Commissioner