Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 166-2025[1]

eHealth Saskatchewan

-and-

Ministry of Health

-and-

Danniela Morgan

PART 1 – PRIVACY BREACH IN 2020/2021

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.

In October 2024, Ms. Morgan was hired by Dr. Yang Zhan (Dr. Zhan) to work at Dr. Zhan's clinic, the Regina Cardiology Clinic, as a Medical Office Assistant. 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. 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 worked at the Regina Cardiology Clinic until February 7, 2025. It was not until April of 2025

[1] The other OIPC file numbers associated with this matter are 193-2025 and 263-2025.

when a complaint by a concerned individual led to the discovery that Ms. Morgan had snooped on personal health information of 23 citizens of Saskatchewan in the eHR Viewer while under the employ of Dr. Zhan. That matter forms the basis of *Investigation Report 082-2025 (Part 2)*.

As a result of that discovery, 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 this *Investigation Report 166-2025 (Part 1)*. eHealth determined that Ms. Morgan had committed a privacy breach by snooping on the personal health information of six individuals while employed by eHealth from November 2020 to October 2021.

eHealth proactively reported the privacy breach to the Office of the Saskatchewan Information and Privacy Commissioner (OIPC). As noted, the privacy breach involving Dr. Zhan's clinic is covered by *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)* involve one continuous snooping violation of *HIPA* over a period of many years and should be read together.

OIPC undertook an investigation and made several findings in this matter. We conclude that a privacy breach occurred simply because Ms. Morgan willfully, and with full knowledge, accessed the personal health information of six individuals without a need-to-know basis during the time she was employed by eHealth (2020-2021). There were appropriate safeguards in place. The violations of *HIPA* involved the willful actions of a rogue employee.

The Commissioner adopts the recommendations that have been made in *Investigation Report 082-2025* into this Investigation Report and recommends the following with respect to this matter:

(1) That eHealth require all users to sign the *Shared Client Index (SCI) Viewer Account Request Form* prior to granting access to SCI;

(2) That eHealth continue to pursue a proactive audit and monitoring program for all electronic health database systems in its use, specifically Panorama, CQE and SCI.

TABLE OF CONTENTS

I BACKGROUND 1

II DISCUSSION OF THE ISSUES 3

1. Jurisdiction 3

a. *HIPA* 3

i. First element – trustees 3

ii. Second element – personal health information 3

iii. Third element - Do the trustees have custody or control over the personal health information? 5

b. *HIPA* and *The Public Health Act, 1994* 7

2. Did a privacy breach occur? 7

a. SCI – Unauthorized Access to the Personal Health Information of One Individual 8

b. Panorama, CQE and SCI – Unauthorized Access to the Immunization Information of 6 Individuals 10

i. JSAP 11

ii. Panorama User Account Request Form and Panorama User Access Agreement 12

iii. SCI Viewer Account Request Form 15

iv. SCI Enterprise Viewer – Terms of Use 16

v. Annual training on eHealth Corporate Policy 16

vi. Auditing 17

3. Did Health and eHealth respond to the privacy breaches appropriately? 18

a. Containment of the Breach 18

b. Notification of Affected Individuals 19

c. Investigated the breach 20

d. Steps taken to prevent future breaches 21

III FINDINGS 22

IV RECOMMENDATIONS 22

I BACKGROUND

[1] On November 2, 2020, Danniela Morgan commenced employment with eHealth Saskatchewan (eHealth) as a Registry Administrator. As a Registry Administrator, Ms. Morgan required access to three electronic health database systems containing the personal health information of the citizens of Saskatchewan: (1) Panorama; (2) Panorama COVID Quick Entry (CQE); and (3) the Shared Client Index Enterprise Viewer (SCI).

[2] Ms. Morgan worked as a Registry Administrator with eHealth until October 1, 2021. On that day, eHealth terminated Ms. Morgan's accesses to Panorama, CQE and SCI.

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

[4] 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*:[2] 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)].[3]

[5] On October 29, 2024, Dr. Zhan granted Danniela Morgan unsupervised access to the eHealth electronic health record (eHR) Viewer so she could perform her duties at the Regina Cardiology Clinic. Her employment with Dr. Zhan concluded on February 7, 2025.

[6] On April 11, 2025, eHealth received notification from a concerned individual with respect to unauthorized accesses to personal health information on the part of Ms. Morgan. eHealth undertook an investigation and found that Ms. Morgan had inappropriately accessed the personal health information of 23 affected individuals while at the Regina Cardiology Clinic. This investigation is the subject of OIPC *Investigation Report 082-2025 (Part 2)*.

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

[3] *Female Faces Fraud Charges.* Regina Police Service. September 9, 2024.

[7] On May 7, 2025, eHealth undertook an investigation into Ms. Morgan's past accesses to the three electronic health database systems that Ms. Morgan had access to while under the employ of eHealth as a Registry Administrator in 2020 to 2021: Panorama, CQE and SCI.

[8] eHealth determined that Ms. Morgan had accessed the personal health information of six individuals without the need to know basis during her employ at eHealth from 2020 to 2021. This is the subject matter of this Investigation Report.

[9] On July 7, 2025, eHealth proactively reported the snooping to the Office of the Saskatchewan Information and Privacy Commissioner (OIPC).

[10] On August 25, 2025, OIPC notified both eHealth and Ms. Morgan that OIPC would be undertaking an investigation.

[11] On September 23, 2025, eHealth provided its submission to OIPC.

[12] On October 9, 2025, Ms. Morgan provided her submission to OIPC.

[13] On October 23, 2025, OIPC notified the Ministry of Health (Health) that OIPC would be undertaking an investigation. This is because, as discussed later in this Investigation Report, Health is a trustee of two of the three electronic health database systems: Panorama and CQE.

[14] On November 7, 2025, Health provided its submission to OIPC.

II DISCUSSION OF THE ISSUES

1. Jurisdiction

a. HIPA

[15] *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

[16] Health and eHealth qualify as trustees as defined by section 2(1)(t)(i) of *The Health Information Protection Act* (*HIPA*).[4]

ii. Second element – personal health information

[17] Danniela Morgan was granted access to three electronic health database systems that store health information within the province of Saskatchewan: Panorama, CQE and SCI as part of her duties as a Registry Administrator.[5] We must determine if the information contained

[4] *The Health Information Protection Act*, SS 1999, c H-0.021. Health and eHealth also qualify as a "government institution" as defined by section 2(1)(h) of *HIPA*.

[5] During the material time, Ms. Morgan was an employee of eHealth. Section 2(1) of *The Health Information Protection Regulations, 2023, RRS c H-0.021 Reg 2 (effective August 1, 2023), as amended by Saskatchewan Regulations 68/2023* defines "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; or

within each of the three electronic health database systems qualifies as *personal health information* pursuant to section 2(1)(m) of *HIPA*:

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

[18] The Panorama electronic health database system contains information such as the name, address, phone number, health services number (HSN), birth date, immunization details, adverse event details related to immunization, risk factors for vaccine eligibility and other relevant information gathered from individuals during the immunization service within the province of Saskatchewan.[6]

> (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;

[6] OIPC has found in the past that information regarding immunization qualifies as personal health information: OIPC Investigation Report 243-2023 at paragraph [14] and OIPC Review Report 082-2024 at paragraph [21].

[19] The CQE electronic health database system contains information such as the name, client identification, birth date, gender, address, HSN, and information about COVID-19 and influenza details of health care patients in the province of Saskatchewan.

[20] The SCI application allows the user to view information such as the name, birth date, gender, address, phone number, HSN, death indicator (yes or no), and medical record number of the facility or former health region and the last activity date of health care patients in the province of Saskatchewan.

[21] Based on the above, we can confirm that personal health information was present in this matter.

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

[22] "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.[7]

[23] Panorama is a database containing registration, immunization, and investigation and outbreak management data respecting Saskatchewan patients/clients. Panorama is established pursuant to *The Public Health Act, 1994*[8] and section 22.01 of *The Disease Control Regulations*.[9] Section 22.01(3) of the *Disease Control Regulations* provides what information is recorded in Panorama:

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

[8] *The Public Health Act, 1994*, S.S. 1994, c. P-37.1, as amended.

[9] *The Disease Control Regulations*, R.R.S, c. P-37.1 Reg 11, as amended.

> **22.01**(3) A person who provides immunization services, and who is authorized to use the immunization database mentioned in subsection (2) shall, as soon as is reasonably practicable, record the following information on that database:
>
> (a) registration information[10] with respect to the individual being immunized;
>
> (b) that informed consent to the immunization was received from or on behalf of the individual;
>
> (c) the vaccine provided and dosage;
>
> (d) the date of the immunization;
>
> (e) subject to subsection (4), eligibility criteria;
>
> (f) information required to be reported to a medical health officer pursuant to section 23;
>
> (g) any other information the minister considers necessary to document the immunization services provided.

[24] Health relies on the *Panorama System Joint Service & User Access Policy* (*JSAP*) to govern and control the collection, use and/or disclosure of personal health information stored within Panorama. Prior to being given access, users of Panorama must agree to the terms as set out. As such, we may conclude that Health has *control* over the personal health information in the Panorama electronic health database system.

[25] The *JSAP* outlines that eHealth is an information management service provider (IMSP) to Health for the information contained within Panorama as defined by sections 2(1)(j) and 18 of *HIPA*.

[26] Health also has control over the personal health information in the CQE electronic health database system as a trustee. CQE is a database system that provides access to the data in the Panorama electronic database system. Because of the integration of the information in

[10] Section 2(1)(q) of *HIPA* defines "registration information" to be information about an individual that is collected for the purpose of registering the individual for the provision of health services and includes the individual's health services number and any other number assigned to the individual as part of a system of unique identifying numbers that is prescribed in the regulations.

this way, the *JSAP* applies to the CQE electronic database system as well as to that in Panorama.

[27] Finally, eHealth operates SCI. Therefore, eHealth is the trustee with custody and control over the personal health information in SCI.

[28] All three elements are present for *HIPA* to be engaged. As such, OIPC has jurisdiction to undertake this investigation pursuant to the jurisdiction afforded by *HIPA*.

b. HIPA and The Public Health Act, 1994

[29] Since personal health information is collected and stored in the Panorama electronic database system pursuant to *The Public Health Act, 1994* and the *Disease Control Regulations*, sections 4(4) of *HIPA* must be considered:

> **4**(4) Subject to subsections (5) and (6), Parts II, IV and V of this Act do not apply to personal health information obtained for the purposes of:
>
> ...
> (g) *The Public Health Act, 1994*;

[30] In keeping with section 4(4) of the *HIPA*, OIPC may not consider Parts II (Rights of the Individual), IV (Limits on Collection, use and Disclosure) and V (Access to Personal Health Information) of *HIPA* in its analysis regarding Panorama and CQE.

[31] OIPC will consider all parts of *HIPA* regarding SCI.

2. Did a privacy breach occur?

[32] In this Investigation Report we will see that personal health information can be breached in two main ways. A privacy breach can occur when the personal health information is collected, used and/or disclosed without authority under *HIPA*.[11] However, we will also

[11] *Supra*, footnote 7 at paragraph [36].

see that a privacy breach can occur when the personal health information (such as immunization information) is appropriately safeguarded by the trustee and is then inappropriately accessed by a rogue employee.[12]

a. SCI – Unauthorized Access to the Personal Health Information of One Individual

[33] Section 2(1)(u) of *HIPA* defines "use" as:

> **2**(1) 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.

[34] When the employee of a trustee uses personal health information, it must do so in accordance with the "need-to-know" principle as set out in section 23 of *HIPA*. The need-to-know principle provides that trustees, and its 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.

[35] Further, section 26 of *HIPA* restricts the use of personal health information by trustees as follows:

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

> **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.
>
> (3) Nothing in subsection (2) authorizes a trustee as an employer to use or obtain access to the personal health information of an individual who is an employee or prospective employee for any purpose related to the employment of the individual without the individual's consent.

[36] Registry Administrators under the employ of eHealth provide support for Panorama by entering data and facilitating updates when errors are reported. The SCI application is used to verify the identity of individuals and ensure that the correct patient profile is entered or updated in Panorama or CQE. The eHealth audit revealed that Ms. Morgan viewed the personal health information of an affected individual in SCI on March 16, 2021, and again on May 6, 2021. eHealth reported that these accesses "cannot be explained as there are no other related events or supporting documentation".

[37] Ms. Morgan denied knowingly accessing personal health information without appropriate authorization or a valid work-related purpose. She maintained that while she may have engaged in inappropriate accesses, they were "unintentional and without malicious intent."

[38] In the absence of validation to support Ms. Morgan's access to SCI on these dates, she clearly did not have a need to know when snooping into the personal health information of this one individual on two occasions. A privacy breach occurred on SCI on March 16, 2021 and May 6, 2021 with unauthorized snooping into the personal health file of one individual. This individual was one of the six individuals that was snooped on in the discussion below.

b. Panorama, CQE and SCI – Unauthorized Access to the Immunization Information of 6 Individuals

[39] Immunization data is collected in Saskatchewan under the jurisdiction of *The Public Health Act, 1994* which is also subject to section 22.01(7) of *The Disease Control Regulations*. The eHealth investigation concluded that Ms. Morgan accessed six individuals' immunization information in violation of section 22.01(7) of the *Disease Control Regulations*, which provides:

> **22.01**(7) A person who collects information for the purposes of entering that information into the immunization database mentioned in subsection (2) or who uses information from that database shall maintain the confidentiality of that information and not further disclose or use that information for a purpose not authorized by the Act or these regulations, except:
>
> (a) with the consent of the individual to whom the information relates; or
>
> (b) if authorized by law.

[40] Part IV of *HIPA* sets out the provisions under which trustees must collect, use and/or disclose personal health information. However, as we explained in paragraphs [29] and [30] above, section 4(4) of *HIPA* carves out information collected pursuant to *The Public Health Act, 1994*. Since HIPA does not apply to the collection, use and disclosure of immunization data, we cannot comment on whether or not Ms. Morgan's access to the six individuals' immunization data was contrary to the provisions of *HIPA*, in fact we are only left to consider whether privacy breaches occurred as a result of personal health information (now we are speaking of immunization data) not being appropriately safeguarded pursuant to Part III of *HIPA*, section 16. If personal health information is not appropriately safeguarded, the actions of a rogue employee cannot be condemned in the same way had there been careful guardrails in place.

[41] 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.

[42] We can state at the forefront that both Health and eHealth had rigorous safeguards in place to protect personal health information in Panorama, CQE and SCI. However, before proceeding, we must acknowledge Ms. Morgan's submissions that her breaches may have resulted from "unclear instructions" or "limitations in system oversight." She explained:

> If the investigation identifies a breach, I respectfully ask that consideration be given to the training, guidance, and system controls provided at the time. Any missteps [on my part] may have resulted from unclear instructions or limitations in system oversight, rather than deliberate misconduct.

[43] Therefore, not only will this office consider to what degree the personal health information was safeguarded by Health and eHealth, but we will also consider whether Health and eHealth clearly communicated that unauthorized access to the personal health information of the residents of Saskatchewan is strictly forbidden.

i. JSAP

[44] As explained above in paragraphs [24] to [26], Health mandates the procedure for the collection, use and disclosure of personal health information in Panorama in *JSAP*. Users of Panorama *must* review and agree to the terms set out in the *JSAP* prior to being given access. The relevant sections of the *JSAP* are:

> ***1. High Level Policy***
>
> …
> Collection and use of the personal health information within Panorama is restricted to Authorized Health Purposes only as described in this Policy. Use (including viewing and secondary use) or disclosure for any other purpose is strictly prohibited.
>
> …
> ***6. Detailed Policy***
>
> …
> **6.4 Limiting Collection, Use and Disclosure.** The Ministry of Health, Source Trustees and Accessing Trustees and their authorized Users may only collect, use and disclose Registration, Immunization, Investigation and Outbreak Management Data stored within Panorama on a need to know basis in accordance with the user roles and encounter groups for an Authorized Health Purpose.

[45] *JSAP* is clear that users must abide by the need-to-know principle when accessing personal health information in Panorama. Users must sign the *Panorama User Access Agreement*, which will be the safeguard discussed next. By signing the agreement, the user confirms that they have reviewed the *JSAP*.

ii. Panorama User Account Request Form and Panorama User Access Agreement

[46] In order to be granted access to Panorama, users must first complete the *Panorama User Account Request Form*, which specifies the following:

> **Panorama User Roles and Responsibilities**
>
> - User access is audited.
> - Inappropriate use of the Panorama shall be reported to the eHealth Saskatchewan's Chief Privacy Officer.
> - Any violation of privacy legislation will be investigated and addressed.
> - Users are responsible for completion of the training available on the Panorama Program Page.

- Users are responsible for ensuring that the use of Panorama data is on a need-to-know basis for the purpose of their health care work and it is in accordance with their health organization's policies and procedures and HIPA.

- Users must be authorized by an Authorized Approver within an Approved Organization.

- A User is identified and authenticated by an Authorized Approver to view and use Panorama data. The Approved Organization and the Approver are accountable for actions of the User

[Emphasis added]

[47] Attached to the *Panorama User Account Request Form* is the *Panorama User Access Agreement* (*Agreement*). The *Agreement* provides:

Panorama User Access Agreement

The Panorama Joint Service and Access Policy ("JSAP") gives your health care organization the right to authorize you to access the Panorama solution, and outlines the obligations of both you and your organization to only access Panorama in compliance with the JSAP.

As an employee, contracted employee, student, or other service provider, I understand that as an authorized user of Panorama I will have access to confidential client information that includes, but is not limited to, information relating to client registration, immunizations, and/or communicable disease and outbreak investigations stored in Panorama (Panorama Information).

As a condition of being granted user rights and permissions for Panorama, I acknowledge that I am permitted to access and use the Panorama Information only for authorized health purposes or such other purposes that may be permitted by law, and that my access to and use of the Panorama Information is limited to that information I need to perform the legitimate duties within my health care organization that are specific to the role(s) for which I was authorized as a user.

In Particular:

1. I understand that the Panorama Information I use in the performance of my duties is confidential;

2. *I understand that my use of and access to the Panorama Information must be in accordance with the Panorama Immunization/Investigations &*

Outbreak Management Joint Service and Access Policy and that I have reviewed that Policy;

3. I understand that a client's express consent is required to disclose Panorama Information to a third party, except where applicable law permits disclosure of the information without consent or on an implied consent basis;

4. *I understand that I am not permitted to access or use Panorama Information regarding myself, my spouse, family members, friends, acquaintances, co-workers, and any other person for purposes unrelated to my duties. This includes looking up birth dates, addresses, immunization or investigations and outbreak information for personal use, out of curiosity or for any other purposes other than those for which the Panorama Information is intended*;

   4.1 I further understand that unauthorized use also includes printing or exporting any information including the names, birth dates, addresses, and clinical data of clients for purposes other than those for which Panorama has been approved;

5. I understand that any disposal of documents containing Panorama Information must be done by way of secure disposal which in accordance with my health care organization's policies;

6. I acknowledge that I am responsible and accountable for all activities conducted on the computer network under my Panorama user account and I am not to share my Panorama user account or password with others; and

7. I acknowledge that Panorama is audited and my activity may be monitored in order to protect and maintain the integrity of the system and to ensure compliance with privacy policies and procedures.

I understand that the consequences for not acting in accordance with this agreement include discipline and possible termination of my employment/service. I also understand that legal action may result from breach of these terms and may include prosecution of an offence where actions violate the provisions of the law. I understand that my name may be released to a complainant as part of full disclosure in a proven case of breach of privacy. In some circumstances, when a client requests information about who has accessed their personal health information, your name could be released following an assessment of the request.

_____

(Signature/date)

[Emphasis added]

[48] The *Agreement* explicitly communicates that users are forbidden from accessing the personal health information of others for purposes unrelated to their duties. The *Agreement* clearly stipulates that consulting the personal health information of others for personal use, or out of prurient interest, is prohibited.

[49] Ms. Morgan signed the *Agreement* on October 27, 2020. By signing the *Agreement*, she indicated she understood she was only to access personal health information in Panorama on a need-to-know basis.

iii. SCI Viewer Account Request Form

[50] The *Shared Client Index (SCI) Viewer Account Request Form* is a form that users must complete prior to being granted access to SCI. eHealth provides very detailed direction on what constitutes inappropriate use. It says:

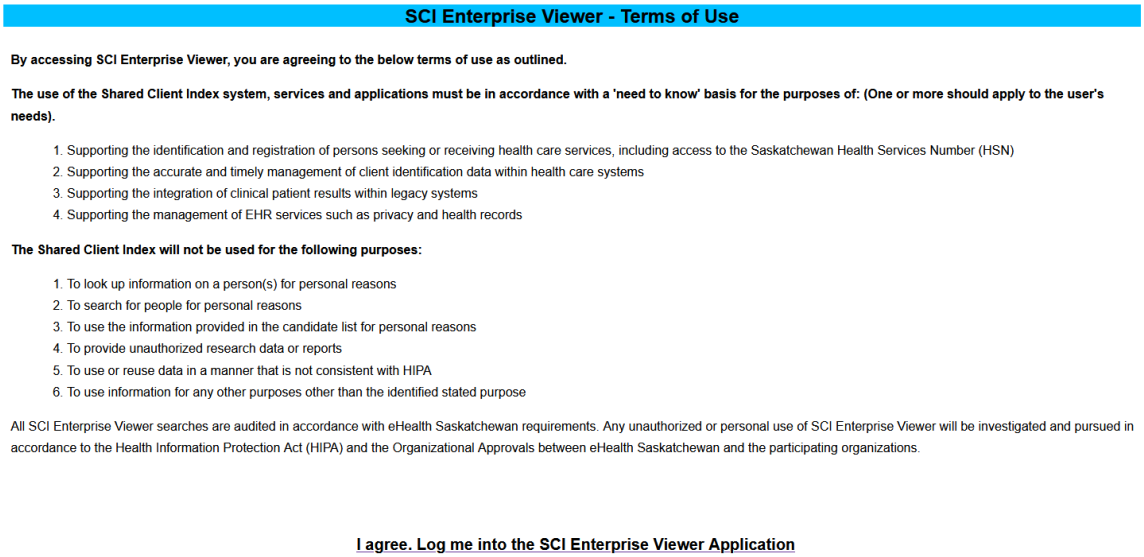
Use is Consistent with the Purpose
The use of the Shared Client Index system, services and applications must be in accordance with a 'need to know' basis for the purposes of: (One or more should apply to the user's needs). • Supporting the identification and registration of persons seeking or receiving health care services, including access to the Saskatchewan provincial health number. • Supporting the accurate and timely management of client identification data within health care systems. • Supporting the integration of clinical patient results within legacy systems. • Supporting the management of EHR services such as privacy and health records.
Use is Appropriate to User's Need to Know
The View options are: • SCI Viewer (Person Search) –The Default single column view providing access to the "SCI Record" only; the most recently updated attributes including names, identifiers, and address, including Provincial Health Number and death flag with associated date. • SCI Detailed View – If the User requires more detailed information about the data in the "SCI Record" or in their own organization in comparison to other sources, a more detailed, multi-column view is available showing multiple source records for a linked set.
Restrictions on Use
The Shared Client Index will not be used for the following purposes: • To look up information on a person(s) for personal reasons. • To search for people for personal reasons. • To use the information provided in the candidate list for personal reasons. • To provide unauthorized research data or reports. • To use or reuse data in a manner that is not consistent with HIPA. • To use information for any other purpose other than the identified stated purpose.

[51] Our review revealed that Ms. Morgan did not sign the SCI Viewer Account Request Form. The form only contained the signature of Ms. Morgan's manager and it was dated October 29, 2020 by the manager – days before Ms. Morgan commenced her employment with eHealth on November 2, 2020. eHealth explained that it generally does not require the

user's signature. Health explained that the form must be signed by the approver or sent directly by the approver to the Access Management Team. While this omission in the safeguard system is not wise, in the face of the education that was provided Ms. Morgan, we do not see it as detracting in any way from her intentional violations in this case.

iv. SCI Enterprise Viewer – Terms of Use

[52] Every time a user logs into SCI, the terms of use appear:[13]



SCI Enterprise Viewer - Terms of Use

By accessing SCI Enterprise Viewer, you are agreeing to the below terms of use as outlined.

The use of the Shared Client Index system, services and applications must be in accordance with a 'need to know' basis for the purposes of: (One or more should apply to the user's needs).

1. Supporting the identification and registration of persons seeking or receiving health care services, including access to the Saskatchewan Health Services Number (HSN)
2. Supporting the accurate and timely management of client identification data within health care systems
3. Supporting the integration of clinical patient results within legacy systems
4. Supporting the management of EHR services such as privacy and health records

The Shared Client Index will not be used for the following purposes:

1. To look up information on a person(s) for personal reasons
2. To search for people for personal reasons
3. To use the information provided in the candidate list for personal reasons
4. To provide unauthorized research data or reports
5. To use or reuse data in a manner that is not consistent with HIPA
6. To use information for any other purposes other than the identified stated purpose

All SCI Enterprise Viewer searches are audited in accordance with eHealth Saskatchewan requirements. Any unauthorized or personal use of SCI Enterprise Viewer will be investigated and pursued in accordance to the Health Information Protection Act (HIPA) and the Organizational Approvals between eHealth Saskatchewan and the participating organizations.

I agree. Log me into the SCI Enterprise Viewer Application

[53] These terms of use duplicate the content of the *SCI Viewer Account Request Form* just discussed above. These terms of use underline what constitutes appropriate use of SCI and what is prohibited. Therefore, even though it does not appear that Ms. Morgan reviewed and signed the *SCI Viewer Account Request Form*, she would have seen the terms of use and agreed to them every time she logged onto the SCI electronic health database system.

v. Annual training on eHealth Corporate Policy

[54] eHealth requires all employees to participate in annual training on its corporate policies, especially the corporate privacy policy. The privacy policy provides a definition of the

[13] Shared Client Index (SCI) Enterprise Viewer, eHealth Saskatchewan.

"need to know" principle and explicitly provides that eHealth employees cannot use or disclose personal information and/or personal health information for purposes other than those for which it was collected, except with the consent of the customer or as required by legislation. It also provides that only employees with a "need to know" requirement may access, collect, use or disclose personal information (or personal health information), vital statistics and/or any other confidential information. The policy clearly communicates that employees are to abide by the need-to-know principle in the course of their duties.

[55] eHealth indicated that Ms. Morgan completed the annual training on November 4, 2020, two days after she commenced full-time employment with eHealth.

[56] Health and eHealth rigorously communicated to its employees that they were to only access personal health information in SCI, Panorama and CQE on a need-to-know basis and not for any other purpose. By delivering these expectations from the outset, Health and eHealth required their employees to access personal health information appropriately. We find that Health and eHealth had robust systems in place and reasonably expected that Ms. Morgan understood that she was to only access personal health information on a need-to-know basis.

vi. Auditing

[57] Audits determine whether employee-users access personal health information off the electronic health database systems appropriately. At the time Ms. Morgan served as a Registry Administrator, eHealth conducted audits on a "request only" basis. There were no reported concerns regarding Ms. Morgan until April 2025, so eHealth had not conducted audits on Ms. Morgan up to that point. eHealth conceded that a proactive audit and monitoring program would have caught Ms. Morgan's snooping much earlier.

[58] eHealth indicated that it is now working on implementing a proactive audit and monitoring program for the eHealth Public Health Team. We applaud this effort and we recommend that it apply across the board to all electronic health database systems currently in use by Health and eHealth in Saskatchewan.

[59] Health and eHealth had appropriate and reasonable safeguards to protect personal health information in SCI, Panorama and CQE. The privacy breach did not result due to the lack of appropriate and reasonable safeguards. It occurred because Ms. Morgan wilfully violated the provisions of HIPA in accessing personal health information without a need-to-know basis. We acknowledge that it is very hard to protect personal health information when an employee goes rogue as was the case here.

3. Did Health and eHealth respond to the privacy breaches appropriately?

[60] The analysis of a trustee's response to privacy breaches 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

[61] Upon learning that a privacy breach has 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:[14]

- Stopping the unauthorized practice.
- Recovering the records.
- Shutting down the system that has been breached.
- Revoking access to personal health information.
- Correcting weaknesses in physical security.

[14] *Supra*, footnote 7 at paragraph [52].

[62] OIPC applies a standard of reasonableness to assess the containment of a breach. The trustee must demonstrate that it has reduced the magnitude of the breach and the resulting risk to affected within a reasonable consideration.[15]

[63] Ms. Morgan's unauthorized accesses went undetected for the duration of her employment with eHealth. The privacy breach in connection with Ms. Morgan's employment at eHealth was contained only upon her termination of employment in October of 2021. However, the unauthorized accesses to the personal health information of six individuals while Ms. Morgan was employed at eHealth were not detected until more than five years later, in 2025. Sadly, had eHealth used audits to detect Ms. Morgans snooping while she was employed at eHealth, her name could have been added to the eHealth Desk watchlist – which would have halted her unconstrained snooping expedition once and for all.

b. Notification of Affected Individuals

[64] It is best practice for trustees to 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:[16]

- A general description of what happened.
- A detailed description of the personal health information involved (e.g., name, medical record, etc.).
- A description of the types of harm that may possibly result from the privacy breach (i.e. identity theft).
- Steps taken and planned to mitigate the harm and to prevent future breaches.

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

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

- 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.

[65] In letters dated July 6, 2025, eHealth notified the six affected individuals in this case. Ms. Morgan continued to snoop on the personal health information of these six individuals when she commenced to work for Dr. Zhan at the Regina Cardiology Clinic in 2024-2025. Those letters served as effective notice, and they are discussed at length in *Investigation Report 082-2025.* eHealth enclosed audit reports with each letter that detailed the dates and times the Snooper accessed each of the affected individuals' personal health information in Panorama, CQE, and/or SCI.

[66] Based on the above, eHealth has notified the affected individuals appropriately with respect to this matter.

c. Investigated the breach

[67] 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. At the conclusion of its investigation, the trustee should have a solid grasp on what occurred which helps inform how to prevent future breaches.[17]

[68] Health and eHealth had in robust safeguards in place to protect personal health information in Panorama, CQE and SCI, including:

[17] *Ibid,* at paragraphs [83] to [84].

a. the *JSAP*;
b. the *Panorama User Account Request Form* and the *Panorama User Access Agreement*,;
c. the *SCI Viewer Account Request Form*,
d. *SCI Enterprise Viewer – Terms of Use*;
e. the provision of annual training on eHealth Corporate Policy, and
f. auditing.

OIPC found that these safeguards were reasonable and that the privacy breach occurred because Ms. Morgan was a rogue employee.

[69] However, in that earlier discussion of safeguards, we identified two areas that require eHealth consideration and improvement:

> 1) eHealth should always require a new user to sign and acknowledge the *Shared Client Inedex (SCI) Viewer Account Request Form* prior to eHealth granting access to SCI; and
>
> 2) audits should be conducted proactively and not on a "request only" basis.

d. Steps taken to prevent future breaches

[70] Prevention is perhaps one of the most important steps. A privacy breach cannot be undone but a trustee can learn from a breach and improve its practices. To avoid future breaches, a 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.[18]

[71] eHealth has now added Ms. Morgan's name to its Service Desks' watchlist. Any future requests that Ms. Morgan be given access to clinical systems, will be directly forwarded to the eHealth Privacy, Access and Patient Safety Unit for careful review.

[72] As noted, eHealth should always require a new user to sign and acknowledge the *Shared Client Index (SCI) Viewer Account Request Form* prior to eHealth granting access to SCI.

[18] *Ibid,* at paragraph [87].

[73] The audit initiative as contemplated by eHealth is, admittedly, a significant endeavour but this privacy breach makes clear that random, proactive audits are the only protection against an employee that decides to go rogue. This is especially true as the health care system in our province evolves rapidly to include electronic systems and artificial intelligence to deliver health care. OIPC commends eHealth for assuming the audit initiative.

III FINDINGS

[74] Health is the trustee of the personal health information in Panorama and CQE. eHealth is the trustee of the personal health information in SCI. As such, *HIPA* is engaged.

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

[76] A privacy breach occurred when Danniela Morgan accessed the personal health information of one affected individual in SCI in contravention of the need-to-know principle.

[77] eHealth and Health had appropriate and reasonable safeguards in place to protect the personal health information in Panorama, CQE and SCI. This privacy breach occurred because Ms. Morgan Willfully violated the provisions of *HIPA* in accessing personal health information without a need to know basis.

[78] eHealth contained the privacy breach by terminating Danniela Morgan's access to Panorama, CQE and SCI but did not detect the breach in a timely manner.

[79] eHealth notified the affected individuals appropriately with respect to this matter.

IV RECOMMENDATIONS

[80] I recommend that eHealth require users to sign and acknowledge the *Shared Client Index (SCI) Viewer Account Request Form* prior to granting access to SCI.

[81] I recommend that eHealth continue to pursue a proactive audit and monitoring program for all electronic health database systems in its use, specifically Panorama, CQE and SCI.

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

Grace Hession David
Saskatchewan Information and Privacy Commissioner