Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 136-2024, 169-2024, 183-2024, 187-2024, 191-2024

Innomar Strategies Inc.

November 25, 2024

Summary: Innomar Strategies Inc. (Innomar) proactively reported a privacy breach to the A/Commissioner that affected thousands of individuals, including 7,293 individuals in Saskatchewan. Threat actors gained unauthorized access to the systems of an affiliate of Innomar's parent company, Cencora, and then were able to move laterally into Innomar's systems. From there, personal health information was exfiltrated from Innomar's systems. The A/Commissioner made a number of findings, including that Innomar took reasonable steps to contain the privacy breach as well as to notify the affected individuals. Further, the A/Commissioner found that Innomar identified the root cause that enabled the threat actors to move laterally from Cencora's affiliate's systems to Innomar's system. He recommended that Innomar offer affected individuals a minimum of ten years of credit monitoring.

I BACKGROUND

[1] Innomar Strategies Inc. (Innomar) is an entity that operates privately-owned facilities across Canada, including four InnomarClinics™ in Saskatchewan.

[2] On February 21, 2024, Innomar and Cencora (Innomar's parent company) learned that data from Innomar's information systems had been exfiltrated. Their first evidence of "unauthorized interactive access" to its systems was on January 5, 2024 and the earliest evidence of exfiltration was from February 6, 2024. When it learned of the exfiltration on February 21, 2024, Innomar took immediate steps to contain the privacy breach (which

will be discussed later in this Investigation Report). After February 21, 2024, Innomar did not observe any further "unauthorized activity".

[3] On April 10, 2024, Innomar determined that personal health information such as names, addresses, dates of birth, height, weight, telephone number, email addresses, dates, location of services, health diagnosis/condition, medications/prescriptions, medical record number, patient numbers, health insurance/subscriber number, signature, lab results and medical history were a part of the information that had been exfiltrated from its systems.

[4] On May 9, 2024, Innomar proactively reported the privacy breach to my office, including how it believes that 7,293 individuals in Saskatchewan were affected by this breach.

[5] On May 17, 2024, my office notified Innomar that my office would be undertaking an investigation into the matter.

[6] On June 21, 2024, Innomar provided my office with its completed *Privacy Breach Investigation Questionnaire*. Further, throughout this investigation, Innomar provided responses to questions posed by my office.

II DISCUSSION OF THE ISSUES

1. Do I have jurisdiction?

[7] *The Health Information Protection Act* (HIPA) is engaged when three elements are present 1) a trustee, 2) personal health information, and 3) the trustee has custody or control over the personal health information.

a. Trustee

[8] As described in the background of this Investigation Report, Innomar operates privately-owned facilities across Canada, some of which are in Saskatchewan. According to Innomar's website, there are four "InnomarClinics™" and one "InnomarPharmacy™" in

Saskatchewan. InnomarClinics™ provides services including lab testing and blood work. InnomarPharmacy™ are pharmacies that provide personalized care.

[9] In an email dated October 11, 2024 to my office, Innomar's legal counsel indicated that the exfiltration of data did not affect InnomarPharmacy™ or any individual pharmacist. Therefore, my office will only consider the four InnomarClinics™ in Saskatchewan.

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

> **2**(1) In this Act:
>
> ...
> (t) **"trustee"** means any of the following that have custody or control of personal health information:
>
> ...
> (xv) any other prescribed person, body or class of persons or bodies;

[11] Subsection 4(b) of *The Health Information Protection Regulations, 2023* (HIPA Regulations) provides:

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

[12] The entity profile report from Information Services Corporation's (ISC) Corporate Registry provides that the proprietor of "Innomar Clinics" (not InnomarClinic™) is "Innomar Strategies Inc." Innomar is a business corporation with 10 directors and officers.

[13] Section 2-29 of *The Legislation Act* provides:

> **2-29** In an enactment:
>
> ...
> **"person"** includes **a corporation** and the heirs, executors, administrators or other legal representatives of a person;

[Emphasis added in bold and underline]

[14] Further, Innomar's website identifies that that nurses at InnomarClinics™. Nurses are a "health professional" as defined by subsection 2(1) of the HIPA Regulations.

[15] Finally, for guidance as to what qualifies as a "health service", I refer to section 1-2 of *The Provincial Health Authority Act*, which provides:

> **1-2** In this Act:
>
> ...
> **"health services"** with respect to:
>
> (a) the provincial health authority and health care organizations, includes services that are ancillary to health services and **any prescribed services**;
>
> [Emphasis added in bold and underline]

[16] Subsection 2(4) of *The Provincial Health Authority Administration Regulations* defines "health services" as:

> **2**(4) For the purposes of clause (a) of the definition of **"health services"** in section 1-2 of the Act, the following services are health services:
>
> ...
> (p) laboratory services;

[17] Based on the above, I find that Innomar qualifies as a trustee as defined by subsection 2(1)(t)(xv) of HIPA and subsection 4(b) of the HIPA Regulations.

b. Personal health information

[18] Subsections 2(1)(m)(i), (ii), (iii), (iv) and (v) of HIPA define "personal health information" as follows:

> **2**(1) In this Act:

...

(m) **"personal health information"** means, with respect to an individual, whether living or deceased:

(i) information with respect to the physical or mental health of the individual;

(ii) information with respect to any health service provided to the individual;

(iii) information with respect to the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual;

(iv) information that is collected:

(A) in the course of providing health services to the individual; or

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

(v) registration information;

[19] As noted in the background of this Investigation Report, the types of information involved are names, addresses, dates of birth, height, weight, telephone number, email addresses, dates, location of services, health diagnosis/condition, medications/prescriptions, medical record number, patient numbers, health insurance/subscriber number, signature, lab results and medical history. I find that the information involved in this matter qualifies as "personal health information" pursuant to subsections (2)(1)(m)(i), (ii), (iii), (iv) and (v) of HIPA.

c. Custody or control over the personal health information

[20] "Custody" is the physical possession of a record by a trustee with a measure of control. "Control" means having authority over a record (see Investigation Report 086-2024, 113-2024, 114-2024, 116-2024 at paragraph [15]).

[21] In an email dated June 21, 2024, to my office, Innomar explained as follows:

> The personal health information affected in the Incident (as defined in our May 9, 2024 incident report) is held by Innomar in connection with patient support programs (PSPs) that Innomar administers in partnership with various pharmaceutical companies. PSPs may include clinic and nursing and support (including infusion and injection administration/training), patient education and counselling, reimbursement navigation, and specialty pharmacy and logistics services. Innomar administers PSPs across Canada, including Saskatchewan.
>
> In this regard, Innomar operates privately-owned facilities in or from which health services are provided by health professionals (e.g. infusions administered at InnomarClinics™). Some of these facilities are located in Saskatchewan.
>
> **Innomar collects and maintains the personal health information of patients in order to provide these services. PSPs are administered by Innomar on behalf of its pharmaceutical partners, who ultimately own the data collected by Innomar. However, Innomar maintains custody of the personal health information collected in connection with PSPs and in many cases does not share individually-identifiable information with the associated pharmaceutical partner in the ordinary course.**
>
> [Emphasis added]

[22] Based on the above, Innomar has custody over the personal health information. Further, the information was exfiltrated from Innomar's systems, which suggests that Innomar had custody over the personal health information.

[23] All three elements are present in order for HIPA to be engaged. Therefore, I find that I have jurisdiction to conduct this investigation.

2. Did a privacy breach occur?

[24] A privacy breach occurs when personal health information is collected, used, and/or disclosed without authority under HIPA. A privacy breach also occurs when the trustee has not adequately safeguarded personal health information in their custody or control.

[25] The term "disclosure" is not defined in HIPA. However, in past investigation reports such as Investigation Report 345-2019, my office has defined "disclosure" as the exposure of personal health information to a separate entity, not a division or branch of a trustee that has custody or control of that information.

[26] In this case, personal health information that was stored on Innomar's information systems was exfiltrated. The exfiltration is an unauthorized disclosure of personal health information. As such, I find that a privacy breach has occurred.

3. Has Innomar properly responded to the privacy breach?

[27] When my office finds that a privacy breach has occurred, my office's investigation focuses on whether the trustee has properly responded to the privacy breach.

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

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

[29] I will consider each of the above steps to determine if Innomar appropriately addressed each of the above steps.

[30] Before I proceed, I should note that Innomar provided my office with details of its information security practices in response to my office's questions. However, this investigation report will only reproduce the details provided to my office that are necessary to support my findings and recommendations. This is to ensure no information is unnecessarily disclosed that may compromise Innomar's security posture.

a. Contain the breach (as soon as possible)

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

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

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

[32] In its initial reporting of the privacy breach to my office, Innomar described its containment steps as follows:

> Innomar immediately initiated its incident response process, obtained the assistance of law enforcement and leading cybersecurity experts. As noted above, upon becoming aware of the Incident on February 21, 2024, Innomar promptly took containment steps. These included rotating credentials for all accounts across its environments, disabling any accounts found to be compromised, identifying the threat actor's initial point of entry and preventing further access from that point, and blocking all known indicators of compromise (including all IP addresses and lateral movement tools found to be used in the Incident). There has been no observed unauthorized activity since these containment steps were completed on February 21, 2024 and there is no evidence of ongoing unauthorized activity. Also as noted above, Innomar has taken steps to resolve any threat of the exfiltrated data being disclosed publicly and has engaged several vendors to monitor the dark web.

[33] My office asked Innomar how long the vendors would be monitoring the dark web. Innomar responded by indicating that dark web monitoring "is ongoing". It said that the monitoring has not resulted in any of the exfiltrated data from being posted online or offered for sale. It said that should there be any evidence that any of the data was posted online, that Innomar would "take appropriate steps to mitigate any real risk of significant harm to affected individuals, which could include further individual notifications depending on the circumstances."

[34] Based on the above, I find that Innomar has taken reasonable steps to contain the privacy breach.

b. Notify affected individuals (as soon as possible)

[35] It is best practice to inform affected individuals when their personal health information has been a part of a privacy breach (*Privacy Breach Guidelines for Health Trustees*, p. 3).

[36] Page 4 of *Privacy Breach Guidelines for Health Trustees*, my office recommends that trustees should notify affected individual "as soon as possible after key facts about the breach have been established". Further, it provides guidance on what a notice to affected individuals should include, such as:

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

[37] Innomar sent letters to the affected individuals that included the above elements. Therefore, I find that Innomar has notified individuals affected by this privacy breach.

[38] Innomar also offered affected individuals credit monitoring services for a period of two years at no charge. In the past, my office had recommended that organizations offer credit monitoring to affected individuals for a minimum of five years. However, given my office's experience with investigating privacy breaches, I am now recommending that organizations offer affected individuals credit monitoring for a minimum of ten years, if

not longer. Data is easily stored by threat actors and they may release individuals' information at any time, especially when individuals least expect them to do so. Therefore, I recommend that Innomar offer affected individuals a minimum of ten years of credit monitoring.

[39] Earlier, I noted that Innomar learned that data was exfiltrated from its information systems on February 21, 2024. One hundred days later on May 31, 2024, Innomar began to mail individual notification letters. Affected individuals who contacted my office had received letters dated later than May 31, 2024. Some of the individuals expressed dissatisfaction with the length of time it took Innomar to notify them of the breach. Therefore, my office sought an explanation from Innomar regarding the length of time. Innomar explained that although the exfiltration of data was discovered on February 21, 2024, it did not determine that personal health information was exfiltrated until April 10, 2024. At that point, it worked with its program partners to notify the affected individuals. It noted practical challenges in mailing notices to affected individuals, including "potential duplication, incomplete mailing address information, and the like", that delayed sending notices. It explained:

> As you can imagine, given the number of stakeholders involved and the volume of individual notifications, this process has been extremely complex. Innomar has been notifying all affected individuals as soon as it has been reasonably able to do so, in all the circumstances. As we continue to have no evidence that any of the exfiltrated information has been or will be misused, we are confident that any delay in individual notification has not caused any greater risk of harm to any affected individual.

[40] I understand the perspective of an affected individual wishing to have been notified much sooner. However, I accept that notifying thousands of affected individuals not only in Saskatchewan but across Canada is challenging and will result in some delay. Further, I note that my office's *Privacy Breach Guidelines* at page 4 says that "notification of individuals affected by the breach should occur as soon as possible **after key facts about the breach have been established**" [Emphasis added]. As such, meaningful notices to affected individuals should not come instantaneously after a privacy breach has occurred. Notice should only occur after key facts about the privacy breach have been established. I

accept Innomar's explanation for the length of time it took to provide notice to affected individuals as reasonable.

c. Investigate the privacy breach

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

[42] Based on information provided to my office, it appears the privacy breach occurred in two parts. First, it appears that threat actors were able to gain access to a server of one of Cencora's affiliates. Then, based on the network segmentation arrangements at the time, the threat actors were able to obtain credentials to move laterally from the affiliate's systems to Innomar's systems. From there, the threat actors were able to exfiltrate personal health information.

d. Prevent future breaches

[43] The most important part of responding to a privacy breach is to implement measures to prevent similar privacy breaches from occurring (*Privacy Breach Guidelines for Health Trustees*, p. 6). This includes implementing measures that addresses the root cause (or causes) that led to the privacy breach in the first place.

[44] The root cause of the threat actors being able to move laterally from Cencora's affiliate's systems to Innomar's systems, Innomar explained it would implement further segmentation of its network systems to prevent actors from moving laterally:

> Among the security measures that will address the cause of the unauthorized access, Cencora is strengthening its perimeter defence systems, including through further segmentation of network systems to minimize the capacity for unauthorized lateral movement. By segmenting network systems, it will be more difficult for an actor who

> obtains unauthorized access to one entity's servers to move laterally into affiliates' servers.

[45] I find that Innomar's further segmentation of network systems to be reasonable in minimizing the likelihood of threat actors from moving laterally from system to system should a threat actor gain unauthorized access to a system.

III FINDINGS

[46] I find that I have jurisdiction to conduct this investigation.

[47] I find that a privacy breach has occurred.

[48] I find that Innomar has taken reasonable steps to contain the privacy breach.

[49] I find that Innomar has notified individuals affected by this privacy breach.

[50] I find that Innomar has identified a root cause of the privacy breach to be the network segmentation arrangement that existed at the time of the incident.

[51] I find that Innomar's further segmentation of network systems to be reasonable in minimizing the likelihood of threat actors from moving laterally from system to system should a threat actor gain unauthorized access to a system.

IV RECOMMENDATION

[52] I recommend that Innomar offer affected individuals a minimum of ten years of credit monitoring.

Dated at Regina, in the Province of Saskatchewan, this 25th day of November, 2024.

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