Information and Privacy
Commissioner of Ontario
Commissaire à l'information et à la
protection de la vie privée de l'Ontario

February 28, 2025

SENT VIA EMAIL

PERSONAL AND CONFIDENTIAL

Cathy Beagan-Flood
Lawyer
Blake, Cassels & Graydon LLP
199 Bay Street
Suite 4000
Toronto, ON M5L 1A9

Dear Cathy Beagan-Flood:

RE: Reported Breach - HR24-00254

On May 9, 2024, you reported a breach pursuant to the *Personal Health Information Protection Act* (the *Act* or *PHIPA*) on behalf of Innomar Strategies (Innomar) to the Office of the Information and Privacy Commissioner of Ontario (IPC). The IPC opened file HR24-00254 to address this matter.

The circumstances of this breach involved the exfiltration[1] of data from Innomar's systems which contained personal health information of approximately 100,000 individuals.

What happened?

You reported that on February 21, 2024, Cencora (the parent company of Innomar) was impacted by a cybersecurity breach caused by threat actor(s) leveraging a previously unidentified vulnerability of one of Cencora's affiliates. Once the threat actor exploited the vulnerability, they used tools to obtain credentials and move laterally to gain access to Cencora's systems and then into Innomar's systems. This is when Innomar learned that data on its own servers had been accessed and exfiltrated.

Innomar advised that upon becoming aware of the vulnerability, it immediately deployed remediation measures and was able to contain the breach on February 21, 2024. Innomar reports that although data was exfiltrated, it was not encrypted[2] by the threat actor(s) or otherwise lost and their systems remained operational after the incident.

[1] Exfiltration is the unauthorized removal of data or files from a system by an intruder. See Glossary – Canadian Centre for Cyber Security.
[2] Encryption is converting information from one form to another to hide its content and prevent unauthorized access. See Glossary – Canadian Centre for Cyber Security.

On April 10, 2024, an in-depth analysis revealed that data was exfiltrated which contained the personal health information of approximately 100,000 individuals. This incident affected individuals who utilized certain patient support and drug benefit programs delivered by Innomar.

You reported that Innomar engaged several cybersecurity vendors to monitor the internet, including the dark web, for any activity related to this incident and found no sign of the impacted data being posted or offered for sale. As of the date of this letter, it is Innomar's position that there is no evidence the exfiltrated data has been misused for malicious purposes.

Issues:

As a preliminary matter, it is agreed that Innomar is a health information custodian (custodian) pursuant to the *Act*, that the data impacted by the breach included personal health information and the breach resulted in the unauthorized access to information that was in the custody or control of Innomar.

Accordingly, the sole issue in this letter is whether Innomar responded adequately to the breach.

Did Innomar respond adequately to the breach?

In Ontario, custodians have a duty under the *Act* to protect personal health information against privacy breaches. A privacy breach occurs when personal health information is collected, used or disclosed without authorization. This can include theft, loss, or unauthorized copying, modification or disposal.

As set out in *Responding to a Health Privacy Breach: Guidelines for the Health Sector (the PHIPA Breach Guidelines)*,[3] when confronted with a breach of personal health information, custodians must take appropriate steps in response. These steps include:

- identification of the scope of the breach,
- containment of the personal health information involved,
- notification to those affected, and
- investigation and remediation of the breach.

As part of my review of this matter at Early Resolution, I sought information from Innomar about its response to the breach with respect to scope, containment, notification, investigation, and remediation. Based on the information provided and for the reasons that follow, I find that Innomar responded adequately to the breach.

Scope of Impacted Data:

Innomar's analysis of the incident determined that the exfiltrated files contained the personal health information of approximately 100,000 people.

[3] Responding to a Health Privacy Breach: Guidelines for the Health Sector - IPC

The data exfiltrated included personal information and personal health information. The types of data impacted varied for each affected individual. Innomar identified the categories of affected information to include:

- first and last name,
- address,
- date of birth,
- height and weight,
- telephone number,
- email address,
- dates and location of service,
- health diagnosis/condition,
- medications/prescriptions,
- medical record number,
- patient number,
- health insurance/subscriber number,
- signature,
- lab results,
- medical history.

Based on the information provided, I am satisfied that Innomar took reasonable steps to ascertain the scope of the breach and has provided adequate information about the number of individuals affected and types of information impacted.

Discovery and Containment of the Breach:

Upon initial detection of the unauthorized activity on their servers, Innomar immediately initiated its incident response protocol which included rotating credentials[4] for all accounts across its environments, disabled all compromised accounts, identified the threat actor's initial point of entry to prevent further access from that point, and blocked all known indicators of compromise. Innomar reports that since containment measures were deployed, there has been no detection of unauthorized activity.

Innomar's containment efforts also included notification to law enforcement and engagement of cyber security experts to monitor the dark web to determine if the data had been publicly disclosed by the threat actor(s). As of the date of this report, Innomar notes there is no evidence of public disclosure of the exfiltrated data.

Based on the information provided, I am satisfied that Innomar took reasonable steps to attempt to contain the breach following its discovery.

[4] Credential rotation is a security procedure in which digital identity or credentials are replaced with a new set periodically to mitigate the risk of compromise.

Notification Efforts:

On May 31, 2024, Innomar provided notification of the breach to affected individuals via mail. Innomar's notification letter addressed the following:

- the details and extent of the breach.
- the specifics of the information at issue.
- the steps that have been taken/will be taken to address the breach.
- that the IPC was notified of the breach.
- that the individual has the right to file a complaint with the IPC.
- the appropriate individual within the organization that the affected parties should contact if they have questions.

In parallel, Innomar also reported this breach to data protection authorities internationally, the Office of the Privacy Commissioner of Canada, and all provincial and territorial Canadian Privacy Commissioners and Ombudsmen. Additionally, In coordination with its pharmaceutical partners, Innomar retained credit monitoring services, prepared information for call center services and notified affected parties of this incident.

Based on the information before me, I am satisfied that Innomar took reasonable steps to notify the affected individuals about the breach.

Investigation and Remediation of the Breach:

The IPC's *PHIPA Breach Guidelines* state that the investigation and remediation of a breach should include a review of the circumstances surrounding the breach and a review of the adequacy of existing policies and procedures in protecting personal health information.

Investigation of the Attack:

Upon investigation, Innomar reports the breach was caused by threat actor(s) leveraging a vulnerability of one of Cencora's affiliates. Once the threat actor exploited the vulnerability, they obtained credentials and moved laterally to gain access and exfiltrate information from Cencora and Innomar's systems. The unauthorized activity was detected by Cencora who then reported the incident to Innomar, and its other affiliates.

Upon discovery of the breach, Innomar conducted an extensive investigation which included analyzing logs, alerts, and forensic artifacts from affected systems and extracted information from the affected data sources.

Additionally, Innomar's cybersecurity experts conducted assessments to determine whether the threat actor(s) left persistence mechanisms[5]. The assessment concluded that the breach was

[5] Persistence mechanisms are commonly used in malware to ensure that it remains active and functional on a compromised system even after reboots or attempts to remove it. The use of persistence mechanisms in malware allows the malicious code to maintain control over the system for extended periods, which is critical for long-term exploitation, data theft, or further spreading of the infection.

contained on February 21, 2024, and no persistence mechanisms were found. Further, Innomar reports there is no evidence to suggest the threat actor(s) successfully accessed the affected servers after containment took place.

Based on the information provided, I am satisfied that Innomar took reasonable steps to investigate the circumstances surrounding the breach and has adequately determined its root cause and the series of actions taken by the threat actor(s) during the attack.

Remediation Efforts:

After discovering the breach on February 21, 2024, Innomar reports it has since strengthened its perimeter defences and firewalls, enhanced network segmentation to prevent lateral access and implemented additional data loss prevention mechanisms to prevent exfiltration of sensitive information. Additional steps were taken to ensure that no other systems would allow the same initial access in the future, and supplementary remediation efforts remain ongoing.

To reduce the risk of a similar event occurring in the future, Innomar has added to its extensive cyber controls by working with cybersecurity experts to reinforce the systems and information security protocols.

Based on the information provided, I am satisfied that, following the breach, Innomar took practical steps to remediate this incident and to enhance its security systems against further attacks of this kind.

Review of Existing Privacy Practices and Procedures:

The IPC's expectations of custodians responding to a breach are set out in the *PHIPA Breach Guidelines.* This document describes the response plan that custodians should implement when faced with a breach.

The *PHIPA Breach Guidelines* mandates custodians to develop, implement and review the adequacy of existing policies and procedures in protecting personal health information. Policies should address section 12 of the *Act* which requires that "steps be taken that are reasonable in the circumstances to ensure that the personal health information is protected against theft, loss and unauthorized use or disclosure and to ensure that the records of personal health information are protected against unauthorized copying, modification or disposal."

Innomar's privacy and security policies that are most relevant to this incident include:

- *Infrastructure Security Standard* - outlines measures to ensure the protection and integrity of Innomar's systems, data, and assets from security threats and ensures proper management and recovery procedures.

- *Access Control Policy* - establishes guidelines for managing user access, ensuring that access is granted based on employment functions, and includes requirements for user authentication, password security, and access to critical systems.

- *Access Management Standard* – outlines standards for user account management, authentication processes, and security for information and system access.

- *Network Security Policy* - establishes security protocols to limit vulnerabilities and ensure secure communication and network operations.

- *Password Policies* – outlines requirements for creating and managing passwords to ensure strong security practices and protect sensitive information.

In direct response to the incident, Innomar made updates to its Infrastructure Security Standard in March 2024. These updates included revisions to specific sections regarding:

- Intrusion-prevention and detection systems.
- File integrity systems.
- Controls with respect to inventory of information assets.
- Controls regarding configuration management.

Security Controls:

Prior to the breach, Innomar reported they had extensive security controls in place to mitigate risks of cyber breaches.

Innomar's Information Security Office monitors its information systems which host personal health information on a 24 hours per day, 7 days per week basis for security and operational purposes. Innomar also monitors these systems regularly for potential information security vulnerabilities. Any vulnerabilities identified through these scans are tracked and prioritized for remediation.

Further, Innomar reports use of intrusion detection systems to detect and notify appropriate personnel of suspicious information security events. Innomar also has file integrity systems to monitor files and applications to alert personnel to unauthorized modification of critical system files.

Innomar employs extensive access controls[6] in accordance with the principle of least privilege[7]. Innomar also employs specified roles and responsibilities for monitoring and overseeing access restrictions. Moreover, Innomar protects data through network security measures, limiting

[6] Access Control - Certifying that only authorized access is given to assets (both physical and electronic). For physical assets, access control may be required for a facility or restricted area (e.g. screening visitors and materials at entry points, escorting visitors). For IT assets, access controls may be required for networks, systems, and information (e.g. restricting users on specific systems, limiting account privileges). See Glossary – Canadian Centre for Cyber Security.

[7] Principle of Least Privilege - giving an individual only the set of privileges that are essential to performing authorized tasks. This principle limits the damage that can result from the accidental, incorrect, or unauthorized use of an information system. See Glossary – Canadian Centre for Cyber Security.

internal and external access and implements similar measures for shielding data at rest and in transit.

In addition, Innomar engages a top 100 Certified Public Accountant (CPA) firm to evaluate its information security and privacy management systems annually. The most recent information security evaluation, conducted in December 2023, determined that Innomar's information security practices were in compliance with applicable industry standards. The review concluded that Innomar's systems met the necessary requirements for maintaining a strong security posture. According to the CPA, no nonconformities or opportunities for improvement were identified during the evaluation. Following this assessment, Innomar was re-certified on February 8, 2024, confirming that its practices continued to align with industry standards and best practices.

Innomar provides monthly information security training to staff that focuses on real-world cyber events and includes an employee knowledge check at the end of every module. Since this incident, Cencora has published two articles on its internal SharePoint site to educate staff about cyberattacks and how to prevent them.

Cyber Security Incident Response Protocol:

In addition to their security controls, Cencora has a dedicated Cyber Security Incident Response Team responsible for managing the technical analysis and mitigation efforts related to cybersecurity incidents. This team plays a crucial role in identifying and addressing security threats, while also providing guidance on incident management activities that could potentially impact Cencora's business operations.

Moreover, Cencora has a multi-layered cybersecurity incident response plan that outlines a series of well-defined steps to identify, assess, and mitigate the risks associated with cybersecurity attacks. This comprehensive approach encompasses preventive measures, threat detection, containment protocols, and post-incident analysis.

I am satisfied that Innomar's privacy practices are consistent with the expectations of our office when reviewing cybersecurity breaches of this kind. Specifically, upon review of the information provided during the processing of this file, I am satisfied that Innomar has adequate measures in place with respect to incident prevention, incident management, and detecting and deterring similar cybersecurity breaches.

Conclusion and Recommendations:

In consideration of the circumstances of this breach, I recommend that Innomar conduct a comprehensive review and update the remainder of its privacy and security policies, ensuring that all relevant policies reflect the lessons learned from this incident. This review should consider the specific circumstances surrounding the breach, including any identified vulnerabilities or gaps in current protocols, and incorporate appropriate safeguards to mitigate future incidents of this kind.

Moreover, if subject to a breach of similar scale in the future, I strongly recommended that Innomar consult with the IPC prior to issuing mass notification to affected individuals. This will allow for strategic planning to determine the most effective method of notification and will ensure that notifications are clear, timely, and appropriately coordinated.

While recognizing Innomar's efforts in conducting a thorough investigation, I note section 6.3(2) of O'Reg 329/04 made under the *Act* requires health information custodians to notify the IPC of a privacy breach at the first reasonable opportunity when there are reasonable grounds to believe that personal health information in their custody or control has been stolen (i.e., exfiltrated).

Generally, this means that notification is to be provided at the first reasonable opportunity after the discovery of a breach with further information to be provided upon the completion of an investigation. As such, I recommend that this be noted in Innomar's Cybersecurity Incident Response Plan so it can be considered in the event of any future breaches.

After considering the circumstances of this reported breach and the actions taken by Innomar, I am satisfied that the health information custodian responded adequately to the breach and that no further review of this matter is required.

Yours truly,

Fadi Youssef
Analyst