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

Le 28 février 2025

PAR COURRIER ÉLECTRONIQUE

PERSONNEL

Maître Cathy Beagan-Flood
Avocate
Blake, Cassels & Graydon S.E.N.C.R.L./s.r.l.
199, rue Bay
Bureau 4000
Toronto ON M5L 1A9

Objet : Atteinte à la vie privée déclarée – HR24-00254

Maître,

Le 9 mai 2024, vous avez signalé une atteinte à la vie privée en contravention de la *Loi de 2004 sur la protection des renseignements personnels sur la santé* (la *Loi* ou la LPRPS) de la part d'Innomar Strategies (Innomar) au Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario (CIPVP). Le CIPVP a ouvert le dossier HR24-00254 pour traiter cette affaire.

Cette atteinte à la vie privée a fait intervenir l'exfiltration[1] de données contenues dans les systèmes d'Innomar, qui contenaient des renseignements personnels sur la santé concernant environ 100 000 personnes.

Que s'est-il passé?

Vous avez affirmé que le 21 février 2024, Cencora (la société mère d'Innomar) avait subi une brèche de cybersécurité causée par un auteur de menace ayant exploité une vulnérabilité jusque-là inconnue d'une société affiliée de Cencora. Après avoir exploité cette vulnérabilité, l'auteur de menace a utilisé des outils pour obtenir des justificatifs d'identité et se déplacer latéralement pour accéder aux systèmes de Cencora puis à ceux d'Innomar. C'est alors qu'Innomar a appris que l'auteur de menace avait accédé à des données contenues dans ses propres serveurs et les avait exfiltrées.

Innomar a déclaré qu'après avoir été informée de la vulnérabilité, elle avait pris aussitôt des mesures correctives, et qu'elle avait pu maîtriser l'atteinte à la vie privée le 21 février 2024. La

[1] L'exfiltration est le retrait non autorisé de données ou de fichiers d'un système par un intrus. Voir le glossaire – Centre canadien de cybersécurité.

société a précisé que des données avaient été exfiltrées, mais que l'auteur de menace ne les avait pas chiffrées[2], que ces données n'avaient pas été perdues et que ses systèmes demeuraient opérationnels après l'incident.

Le 10 avril 2024, une analyse approfondie a révélé que les données exfiltrées contenaient des renseignements personnels sur la santé concernant environ 100 000 personnes qui utilisaient des programmes de soutien aux patients et de médicaments fournis par Innomar.

Vous avez précisé qu'Innomar avait fait appel à plusieurs fournisseurs de cybersécurité pour surveiller Internet, y compris le Web caché, pour déceler toute activité liée à cet incident, et qu'il n'y avait aucun signe qui permettait de croire que les données en question avaient été publiées ou mises en vente. À la date de la présente, Innomar considère qu'il n'existe aucune preuve voulant que les données exfiltrées aient été utilisées à des fins malveillantes.

Questions

Il a été convenu, à titre préliminaire, qu'Innomar est un dépositaire de renseignements sur la santé (un « dépositaire ») au sens de la *Loi*, que les données touchées par l'atteinte à la vie privée comprenaient des renseignements personnels sur la santé et que l'atteinte à la vie privée a donné lieu à l'accès non autorisé à des renseignements dont Innomar avait la garde ou le contrôle.

La seule question à trancher dans cette lettre consiste donc à savoir si Innomar a réagi adéquatement à l'atteinte à la vie privée.

Innomar a-t-elle réagi adéquatement à l'atteinte à la vie privée?

En Ontario, la *Loi* impose aux dépositaires l'obligation de protéger les renseignements personnels sur la santé contre les atteintes à la vie privée. Il y a atteinte à la vie privée lorsque des renseignements personnels sur la santé sont recueillis, utilisés ou divulgués sans autorisation, notamment s'ils sont volés ou perdus, ou encore copiés, modifiés ou éliminés sans autorisation.

Comme il est indiqué dans les *Lignes directrices sur les interventions en cas d'atteinte à la vie privée dans le secteur de la santé* (les « Lignes directrices sur les atteintes à la vie privée »)[3], le dépositaire doit prendre les mesures qui s'imposent en cas d'atteinte à la vie privée. Ces mesures sont les suivantes :

- déterminer la portée de l'atteinte à la vie privée;
- maîtriser l'atteinte à la vie privée;
- aviser les personnes concernées;
- mener une enquête et prendre des mesures correctives.

---

[2] Le chiffrement est une procédure par laquelle une information est convertie d'une forme à une autre afin d'en dissimuler le contenu et d'en interdire l'accès aux entités non autorisées. Voir le glossaire – Centre canadien de cybersécurité.

[3] Lignes directrices sur les interventions en cas d'atteinte à la vie privée dans le secteur de la santé – CIPVP

Dans le cadre de mon examen de cette affaire au stade du règlement anticipé, j'ai demandé à Innomar des renseignements sur son intervention à la suite de l'atteinte à la vie privée en ce qui concerne sa portée, sa maîtrise, la notification, l'enquête et les mesures correctives. D'après les renseignements qui m'ont été fournis et pour les motifs qui suivent, j'estime qu'Innomar a réagi adéquatement à l'atteinte à la vie privée.

Portée des données touchées

Innomar a analysé l'incident et conclu que les fichiers exfiltrés contenaient des renseignements personnels sur la santé concernant environ 100 000 personnes.

Les données exfiltrées contenaient des renseignements personnels et des renseignements personnels sur la santé. Les types de données concernées variaient selon la personne. Innomar a établi que les catégories de renseignements touchés étaient les suivantes :

- prénom et nom;
- adresse;
- date de naissance;
- taille et poids;
- numéro de téléphone;
- adresse courriel;
- dates et lieux de réception de services;
- diagnostic ou affection;
- médicaments ou ordonnances;
- numéro de dossier médical;
- numéro de patient;
- numéro d'assurance-santé ou d'abonné;
- signature;
- résultats d'analyses en laboratoire;
- antécédents médicaux.

D'après les renseignements fournis, j'estime qu'Innomar a pris des mesures raisonnables pour déterminer la portée de l'atteinte à la vie privée et fourni des renseignements suffisants sur le nombre de personnes concernées et les types de renseignements touchés.

Découverte et maîtrise de l'atteinte à la vie privée

Après avoir décelé l'activité non autorisée dans ses serveurs, Innomar a aussitôt mis en œuvre son protocole d'intervention en cas d'incident, qui a comporté la rotation des justificatifs d'identité[4] de tous les comptes dans l'ensemble de ses environnements, la mise hors service de

[4] La rotation des justificatifs d'identité est une procédure de sécurité qui consiste à renouveler l'identité numérique ou les justificatifs d'identité régulièrement afin de réduire le risque de compromission.

tous les comptes compromis, l'identification du point d'accès initial de l'auteur de menace afin d'éviter tout autre accès à partir de ce point, et le blocage de tous les indicateurs connus de compromission. Innomar a affirmé que, depuis la mise en œuvre de ses mesures de maîtrise de l'atteinte à la vie privée, aucune activité non autorisée n'a été détectée.

Les mesures de maîtrise d'Innomar comprenaient également la notification des forces de l'ordre et le recours à des experts en cybersécurité pour surveiller le Web caché afin de déterminer si l'auteur de menace avait divulgué les données publiquement. À la date du présent rapport, Innomar n'avait signalé aucune indication voulant que les données exfiltrées aient été publiées.

D'après les renseignements fournis, j'estime qu'Innomar a pris des mesures raisonnables pour tenter de maîtriser l'atteinte à la vie privée après l'avoir découverte.

Mesures de notification

Le 31 mai 2024, Innomar a avisé par courriel les personnes concernées par l'atteinte à la vie privée. Sa lettre de notification contenait les renseignements suivants :

- les particularités et la portée de l'atteinte à la vie privée;
- des précisions sur les renseignements en cause;
- les mesures qui ont été ou seront prises pour maîtriser l'atteinte à la vie privée;
- le fait que le CIPVP a été informé de l'atteinte à la vie privée;
- le fait que toute personne concernée peut porter plainte au CIPVP;
- les coordonnées d'une personne de l'organisation que les personnes concernées peuvent joindre si elles ont des questions.

Innomar a également signalé cette atteinte à la vie privée à des autorités internationales de protection des données, au Commissariat à la protection de la vie privée du Canada et à tous les commissaires et ombudsmen à la protection de la vie privée des provinces et territoires canadiens. De plus, en collaboration avec ses partenaires du secteur pharmaceutique, Innomar a fait appel à des services de surveillance du crédit, préparé des renseignements pour les centres d'appel et avisé les parties concernées de cet incident.

D'après les renseignements dont je dispose, j'estime qu'Innomar a pris des mesures raisonnables pour informer les personnes concernées de l'atteinte à la vie privée.

Enquête sur l'atteinte à la vie privée et mesures correctives

D'après les Lignes directrices sur les atteintes à la vie privée du CIPVP, l'enquête sur une atteinte à la vie privée et les mesures correctives doivent comprendre un examen des circonstances ayant entouré l'atteinte à la vie privée et un examen des politiques et procédures en vigueur pour déterminer si elles sont suffisantes pour protéger les renseignements personnels sur la santé.

Enquête sur l'attaque

Après avoir fait enquête, Innomar a déclaré que l'atteinte à la vie privée avait été causée par un auteur de menace qui avait exploité une vulnérabilité d'une société affiliée de Cencora. Après avoir exploité cette vulnérabilité, l'auteur de menace a obtenu des justificatifs d'identité et s'est déplacé latéralement pour obtenir l'accès aux systèmes de Cencora puis à ceux d'Innomar et exfiltrer des renseignements qu'ils contenaient. Cette activité non autorisée a été décelée par Cencora, qui a signalé l'incident à Innomar et à ses autres sociétés affiliées.

Après avoir découvert l'atteinte à la vie privée, Innomar a mené une enquête approfondie comprenant l'analyse de journaux, d'alertes et d'artéfacts criminalistiques des systèmes touchés et des renseignements extraits des sources de données concernées.

De plus, des experts en cybersécurité d'Innomar ont mené des évaluations afin de déterminer si l'auteur de menace avait installé des mécanismes de persistance[5]. Il a été conclu que l'atteinte à la vie privée avait été maîtrisée le 21 février 2024, et aucun mécanisme de persistance n'a été décelé. De plus, Innomar a affirmé qu'aucune indication ne permettait de croire que l'auteur de menace avait accédé aux serveurs touchés une fois les mesures de maîtrise mises en œuvre.

D'après les renseignements fournis, j'estime qu'Innomar a pris des mesures raisonnables pour faire enquête sur les circonstances entourant l'atteinte à la vie privée, et qu'elle a établi adéquatement sa cause et les différents agissements de l'auteur de menace au cours de l'attaque.

Mesures correctives

Innomar a affirmé qu'après avoir découvert l'atteinte à la vie privée, le 21 février 2024, elle a renforcé ses mesures de défense périphérique et ses pare-feu, rehaussé la segmentation de son réseau pour prévenir l'accès latéral et mis en œuvre des mécanismes supplémentaires de prévention des pertes de données afin d'éviter l'exfiltration de renseignements de nature délicate. La société a également pris d'autres mesures pour s'assurer qu'aucun autre système ne permettrait le même type d'accès initial dans l'avenir, et des mesures correctives supplémentaires sont en cours de mise en œuvre.

En plus de ses mesures de contrôle poussées, Innomar a fait appel à des experts en cybersécurité pour renforcer ses systèmes et ses protocoles de sécurité de l'information afin de réduire le risque qu'un tel incident se reproduise.

---

[5] Les logiciels malveillants comportent souvent des mécanismes de persistance pour s'assurer qu'ils restent actifs et fonctionnels dans un système compromis, même après que ce dernier a été relancé ou que l'on a tenté de les supprimer. De tels mécanismes permettent au code malveillant de conserver le contrôle du système pendant de longues périodes, ce qui est essentiel pour assurer l'exploitation à long terme, le vol de données ou la propagation de l'infection.

D'après les renseignements fournis, j'estime qu'après l'atteinte à la vie privée, Innomar a pris des mesures correctives concrètes et amélioré ses systèmes de sécurité afin de se prémunir contre d'autres attaques de ce genre.

Examen des pratiques et procédures actuelles de protection de la vie privée

Les attentes du CIPVP à l'égard des dépositaires quant aux interventions à la suite d'une atteinte à la vie privée sont établies dans ses Lignes directrices sur les atteintes à la vie privée. Ce document décrit le plan d'intervention que le dépositaire doit mettre en œuvre en cas d'atteinte à la vie privée.

Selon les Lignes directrices sur les atteintes à la vie privée, le dépositaire doit élaborer et mettre en œuvre des politiques et procédures et déterminer si elles sont suffisantes pour protéger les renseignements personnels sur la santé. Ces politiques doivent s'appuyer sur l'article 12 de la *Loi*, qui est libellé ainsi : « Un dépositaire de renseignements sur la santé prend des mesures qui sont raisonnables dans les circonstances pour veiller à ce que les renseignements personnels sur la santé dont il a la garde ou le contrôle soient protégés contre le vol, la perte et une utilisation ou une divulgation non autorisée et à ce que les dossiers qui les contiennent soient protégés contre une duplication, une modification ou une élimination non autorisée. »

Les politiques de protection de la vie privée et de sécurité d'Innomar qui sont les plus pertinentes dans le contexte de cet incident sont les suivantes :

- *Norme de sécurité de l'infrastructure* – mesures visant à assurer l'intégrité des systèmes, données et actifs d'Innomar et leur protection contre les menaces informatiques et prévoyant des mesures de gestion et de rétablissement.

- *Politique de contrôle d'accès* – lignes directrices sur la gestion de l'accès des utilisateurs, visant à faire en sorte que l'accès est accordé compte tenu des fonctions du poste, et prévoyant des exigences relatives à l'authentification des utilisateurs, à la sécurité des mots de passe et à l'accès aux systèmes essentiels.

- *Norme de gestion des accès* – normes sur la gestion des comptes utilisateurs, les processus d'authentification et la sécurité pour l'accès à l'information et aux systèmes.

- *Politique de sécurité du réseau* – protocoles de sécurité visant à limiter les vulnérabilités et à sécuriser les communications et le fonctionnement du réseau.

- *Politiques relatives aux mots de passe* – exigences concernant la création et la gestion des mots de passe afin d'assurer l'adoption de pratiques de sécurité rigoureuses et de protéger les renseignements de nature délicate.

En réaction directe à cet incident, Innomar a mis à jour sa norme de sécurité de l'infrastructure en mars 2024, en modifiant certaines sections concernant :

- les systèmes de prévention et de détection des intrusions;
- les systèmes visant à assurer l'intégrité des fichiers;
- les contrôles de l'inventaire des actifs informationnels;
- les contrôles de la gestion des configurations.

Contrôles de sécurité

Innomar a affirmé qu'avant l'atteinte à la vie privée, des contrôles de sécurité rigoureux étaient en place pour atténuer les risques des brèches de cybersécurité.

Le bureau de la sécurité de l'information d'Innomar surveille tous les jours, 24 heures sur 24, ses systèmes d'information qui contiennent des renseignements personnels sur la santé à des fins de sécurité et pour des raisons opérationnelles. Innomar surveille également ces systèmes régulièrement pour déterminer s'ils présentent des vulnérabilités sur le plan de la sécurité de l'information. La société effectue le suivi des vulnérabilités relevées lors de ces vérifications et veille à les éliminer en priorité.

De plus, Innomar a affirmé utiliser des systèmes de détection des intrusions pour déceler des événements suspects sur le plan de la sécurité de l'information et en informer le personnel compétent. Innomar dispose également de systèmes assurant l'intégrité des fichiers; ils permettent de surveiller les fichiers et applications et d'avertir le personnel en cas de modification non autorisée de fichiers système essentiels.

Innomar utilise des contrôles d'accès[6] rigoureux conformément au principe du droit d'accès minimal[7]. Cette société a établi également divers rôles et responsabilités pour ce qui est de la surveillance des restrictions d'accès. En outre, Innomar protège ses données par des mesures de sécurité du réseau, en limitant l'accès interne et externe, et prend des mesures semblables pour protéger les données au repos et en mouvement.

De plus, Innomar fait appel à l'une des 100 sociétés de comptables agréés publics (*Certified Public Accountant,* CPA) les plus importantes pour évaluer chaque année ses systèmes de sécurité de l'information et de gestion de la protection de la vie privée. La dernière évaluation de

[6] Contrôle de l'accès : Contrôle permettant de garantir que seules les entités autorisées ont accès aux actifs (physiques et électroniques). Pour ce qui concerne les actifs physiques, le contrôle de l'accès peut s'appliquer aux installations ou aux zones d'accès limité (p. ex., filtrage des visiteurs et du matériel aux points d'entrée, escorte accompagnant les visiteurs). Pour ce qui concerne les actifs de TI, le contrôle de l'accès peut s'appliquer aux réseaux, aux systèmes ou à l'information (p. ex. restreindre le nombre des utilisateurs de certains systèmes ou limiter les autorisations d'accès attribuées à certains comptes). Voir le glossaire – Centre canadien de cybersécurité.

[7] Droit d'accès minimal : Principe selon lequel il convient de n'accorder aux utilisateurs que les autorisations d'accès dont ils ont besoin pour accomplir les tâches qui leur ont été dûment attribuées. Ce principe permet de limiter les dommages pouvant résulter d'une utilisation non autorisée – abusive ou accidentelle – d'un système d'information. Voir le glossaire – Centre canadien de cybersécurité.

la sécurité de l'information, qui a eu lieu en décembre 2023, a permis d'établir que les pratiques de sécurité de l'information d'Innomar étaient conformes aux normes pertinentes de l'industrie, et que ses systèmes répondaient aux exigences nécessaires pour maintenir une forte posture de sécurité. Selon les CPA, aucune irrégularité ni possibilité d'amélioration n'a été relevée au cours de l'évaluation. Pour faire suite à cette évaluation, la certification d'Innomar a été renouvelée le 8 février 2024, confirmant que ses pratiques demeuraient conformes aux normes et pratiques exemplaires de l'industrie.

Innomar fournit une formation mensuelle sur la sécurité de l'information à son personnel; cette formation se concentre sur des événements de cybersécurité réels et comprend une vérification des connaissances des employés à la fin de chaque module. Depuis cet incident, Cencora a publié deux articles sur son site SharePoint interne pour renseigner le personnel sur les cyberattaques et leur prévention.

Protocole d'intervention en cas d'incident de cybersécurité

En plus de ses contrôles de sécurité, Cencora a constitué une équipe d'intervention en cas d'incident de cybersécurité qui est chargée de gérer l'analyse technique et les mesures d'atténuation en cas de tels incidents. Cette équipe joue un rôle crucial pour identifier les menaces de sécurité et y faire face, et elle fournit des conseils sur les activités de gestion des incidents qui pourraient se répercuter sur les activités commerciales de Cencora.

De plus, Cencora a dressé un plan d'intervention à plusieurs volets en cas d'incident de cybersécurité; ce plan énonce une série d'étapes bien précises en vue d'identifier, d'évaluer et d'atténuer les risques associés aux attaques de cybersécurité. Cette approche exhaustive comprend des mesures préventives, la détection des menaces, des protocoles de maîtrise et des analyses postincident.

J'estime que les pratiques de protection de la vie privée d'Innomar répondent aux attentes de notre bureau quant à l'examen de telles brèches de cybersécurité. Plus précisément, ayant examiné les renseignements fournis au cours du traitement du présent dossier, j'estime qu'Innomar a mis en place des mesures adéquates en matière de prévention et de gestion des incidents et en vue de déceler et de décourager de telles brèches de cybersécurité.

Conclusion et recommandations

Compte tenu des circonstances de cette atteinte à la vie privée, je recommande à Innomar de mener un examen complet de ses politiques de protection de la vie privée et de sécurité et de mettre à jour celles qui n'ont pas déjà été actualisées, afin que toutes les politiques pertinentes reflètent les leçons tirées de cet incident. Cet examen devrait prendre en considération les circonstances précises entourant l'atteinte à la vie privée, notamment les vulnérabilités ou lacunes relevées dans les protocoles actuels, et prévoir des mesures de précaution appropriées pour atténuer tout incident futur de ce genre.

De plus, je recommande fortement à Innomar, si elle devait subir une atteinte à la vie privée d'une portée semblable dans l'avenir, de consulter le CIPVP avant la notification d'un grand nombre de personnes concernées. Il serait ainsi possible d'effectuer une planification stratégique afin de déterminer la méthode de notification la plus efficace et de faire en sorte que les avis soient clairs, fournis en temps opportun et bien coordonnés.

Je reconnais les efforts qu'Innomar a déployés en vue de mener une enquête approfondie, mais je souligne qu'en vertu de la disposition 2 du paragraphe 6.3 (1) du Règlement de l'Ontario 329/04 pris en application de la *Loi*, le dépositaire de renseignements sur la santé est tenu d'aviser le CIPVP à la première occasion raisonnable s'il a des motifs de croire que des renseignements personnels sur la santé dont il a la garde ou le contrôle ont été volés (c.-à-d. exfiltrés).

En règle générale, cela signifie qu'il faut aviser le CIPVP à la première occasion raisonnable après que l'atteinte à la vie privée a été découverte, et fournir des renseignements après la tenue d'une enquête. Je recommande donc que cela soit ajouté au plan d'intervention en cas d'incident de cybersécurité d'Innomar et pris en compte au cas où une autre atteinte à la vie privée se produirait.

Après avoir examiné les circonstances de cette atteinte à la vie privée et les mesures qu'Innomar a prises, j'estime que ce dépositaire de renseignements sur la santé a réagi adéquatement à l'atteinte à la vie privée et qu'il n'est plus nécessaire de poursuivre le traitement de cette affaire.

Veuillez agréer, Maître, mes sincères salutations.

Fadi Youssef
Analyste