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

Le 9 août 2024

PAR COURRIER ÉLECTRONIQUE

PERSONNEL

Maître Travis Walker
Avocat senior
Norton Rose Fulbright Canada S.E.N.C.R.L., s.r.l.
222, rue Bay
Bureau 3000, C.P. 53
Toronto ON M5K 1E7

Objet : Atteinte à la vie privée – HR23-00282

Maître,

Le 5 juin 2023, vous avez signalé au Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario (CIPVP) 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) au nom d'une personne prescrite en vertu de la LPRPS. Le CIPVP a ouvert le dossier HR23-00282 pour traiter cette affaire.

Cette atteinte à la vie privée a comporté la copie non autorisée de renseignements personnels sur la santé concernant environ 3,4 millions de personnes, lesquels se trouvaient dans le serveur de transfert sécurisé de fichiers de la personne prescrite. Les auteurs de menace ont obtenu l'accès non autorisé à ce serveur en exploitant une vulnérabilité de jour zéro[1] dans le logiciel de transfert de fichiers MOVEit qui était installé dans ce serveur.

I. Contexte

Qu'est-ce qu'une « personne prescrite » en vertu de la LPRPS?

En vertu de la LPRPS, une personne prescrite dresse ou tient des registres de renseignements personnels sur la santé visant à faciliter ou à améliorer la fourniture de soins de santé. Les personnes prescrites sont énumérées au paragraphe 13 (1) du Règlement de l'Ontario 329/04 – Dispositions générales. Elles dressent généralement des registres sur une affection ou maladie précise.

La personne prescrite qui a fait l'objet de la cyberattaque en cause dans cette atteinte à la vie privée est le registre désigné de l'Ontario concernant les renseignements sur la mère, le nouveau-né et

[1] Une vulnérabilité de jour zéro est une vulnérabilité logicielle dont l'existence n'est pas encore connue du fournisseur et n'a donc pas été atténuée. Un exploit de jour zéro est une attaque qui exploite une vulnérabilité de jour zéro. Voir le Glossaire du Centre canadien pour la cybersécurité.

l'enfant. Son rôle est de favoriser la prestation de soins de qualité à toutes les familles de la province.

Cette personne prescrite recueille, utilise et divulgue des renseignements sur les grossesses, les naissances, la période néonatale et l'enfance afin d'améliorer les soins conformément au paragraphe 39 (1) de la LPRPS. Elle recueille des données auprès de fournisseurs de soins de santé, de laboratoires et d'hôpitaux, entre autres, qui fournissent des traitements de fertilité, des soins aux personnes enceintes et des soins aux enfants, et traite ces données en vue de générer à l'intention de fournisseurs et d'établissements de soins de santé des renseignements qui leur permettront d'orienter les soins et d'améliorer la prise de décision[2]. Les activités de collecte, d'utilisation et de divulgation des données de la personne prescrite sont autorisées par la loi, réglementées par le CIPVP et financées par le ministère de la Santé de l'Ontario.

L'incident

Le 31 mai 2023, la personne prescrite a subi une brèche de cybersécurité causée par une vulnérabilité de jour zéro (la « vulnérabilité ») dans le logiciel de transfert de fichiers MOVEit de Progress Software qu'elle utilisait à ce moment-là pour effectuer des transferts sécurisés de fichiers[3]. La personne prescrite hébergeait le logiciel MOVEit dans son serveur interne de transfert sécurisé de fichiers, et elle l'utilisait pour chiffrer des fichiers en vue de les transmettre à des partenaires désignés.

Cette vulnérabilité a permis aux auteurs de menace d'utiliser le portail Web du logiciel pour contourner l'authentification multifactorielle de l'administrateur puis de déchiffrer les fichiers, y accéder et les copier. En raison de cette vulnérabilité, il a été possible d'accéder au serveur hébergeant le logiciel MOVEit (le « serveur touché »), et des données qui étaient en cours de transfert à des fins d'analyse, d'assurance de la qualité ou de distribution à des partenaires désignés ont été exfiltrées.

La personne prescrite a affirmé avoir pris les mesures correctives recommandées tout de suite après avoir été mise au courant de la vulnérabilité. Cependant, elle a affirmé qu'en raison de la nature de celle-ci, elle n'a pas été en mesure de prévenir l'attaque.

Une analyse approfondie a révélé que les fichiers copiés lors de l'atteinte à la vie privée contenaient les renseignements personnels sur la santé d'environ 3,4 millions de personnes, dont environ 1,4 million de personnes enceintes et 1,94 million de fœtus et d'enfants, qui provenaient d'un

---

[2] Les dépositaires de renseignements sur la santé peuvent divulguer des renseignements personnels sur la santé sans le consentement des particuliers concernés à des personnes prescrites afin que celles-ci puissent dresser ou tenir leurs registres. Les personnes prescrites peuvent utiliser des renseignements personnels sur la santé pour dresser ou tenir leurs registres et à des fins de recherche. Voir les questions fréquentes du CIPVP (en anglais seulement) pour des précisions sur les personnes prescrites.

[3] La personne prescrite a acheté une licence d'utilisation du logiciel de transfert de fichiers MOVEit. Par conséquent, au moment de la brèche de cybersécurité, la personne prescrite avait conclu un accord de licence de logiciel avec Progress Software sous la forme de ses modalités d'utilisation. Les données concernées étaient hébergées dans un serveur de la personne prescrite. Celle-ci n'a fourni aucun renseignement personnel ni aucun renseignement personnel sur la santé à Progress Software, et cette entreprise n'avait pas accès au serveur de transfert sécurisé de fichiers qui hébergeait les données concernées.

grand réseau composé essentiellement d'établissements et de fournisseurs de soins de santé et concernaient des traitements de fertilité, des soins aux personnes enceintes, des soins néonataux et des soins aux enfants fournis de janvier 2010 à mai 2023.

Selon la personne prescrite, rien ne semble indiquer que les données copiées ont été utilisées à des fins frauduleuses. Elle a surveillé Internet, y compris le Web caché, pour déceler des activités reliées à cet incident, et n'a trouvé aucune trace de la publication ou de la mise en vente des données en question.

La personne prescrite a indiqué qu'elle n'avait pas été le seul organisme à être touché par cette vulnérabilité, et que rien ne portait à croire que les auteurs de menace l'avaient prise pour cible délibérément. Elle a précisé que la vulnérabilité avait causé un incident de cybersécurité ayant touché des milliers d'organismes du monde entier.

II. Questions

Il est d'abord entendu que l'organisme touché est une personne prescrite en vertu de la LPRPS, que les données en cause dans l'atteinte à la vie privée comprenaient des dossiers de renseignements personnels sur la santé, et que cette atteinte a entraîné l'accès non autorisé à des renseignements personnels sur la santé dont la personne prescrite avait la garde ou le contrôle au moment de l'attaque.

Par conséquent, la seule question qui se pose dans le présent rapport est de savoir si la personne prescrite a réagi adéquatement à l'atteinte à la vie privée.

Question 1 – La personne prescrite a-t-elle réagi adéquatement à l'atteinte à la vie privée?

Lors d'une atteinte à la vie privée qui fait intervenir des renseignements personnels sur la santé, les personnes prescrites doivent prendre des mesures appropriées. Ainsi, elles doivent définir la portée de l'atteinte à la vie privée, la maîtriser, aviser les personnes concernées, mener une enquête et prendre des mesures correctives. Ces exigences sont énoncées dans le document *Manual for the Review and Approval of Prescribed Persons and Entities* du CIPVP (le « manuel »)[4].

Ces exigences sont essentiellement semblables à celles qui s'appliquent aux dépositaires de renseignements sur la santé en cas d'atteinte à la vie privée. Les mesures que les dépositaires doivent prendre sont énoncées dans le document du CIPVP intitulé *Lignes directrices sur les interventions en cas d'atteinte à la vie privée dans le secteur de la santé* (les « lignes directrices »)[5]. Comme les personnes prescrites, à quelques exceptions près, sont assujetties aux mêmes exigences quant aux mesures à prendre en cas d'atteinte à la vie privée faisant intervenir des renseignements personnels sur la santé, je me reporterai aux lignes directrices et au manuel pour évaluer les mesures que la personne prescrite a prises en l'occurrence.

Lors de mon examen de cette affaire au stade du règlement anticipé, j'ai demandé à la personne prescrite de me fournir des renseignements sur les mesures qu'elle avait prises en réaction à

[4] Manual for the Review and Approval of Prescribed Persons and Prescribed Entities – CIPVP.
[5] Lignes directrices sur les interventions en cas d'atteinte à la vie privée dans le secteur de la santé – CIPVP.

l'atteinte à la vie privée quant à sa portée, à sa maîtrise, à la notification, à l'enquête et aux mesures correctives. D'après les renseignements qu'elle m'a fournis, je conclus, pour les motifs qui suivent, que la personne prescrite a pris des mesures adéquates en réponse à l'atteinte à la vie privée.

Portée des données touchées

D'après son analyse des données touchées, la personne prescrite a établi que les fichiers copiés lors de l'atteinte à la vie privée contenaient les renseignements personnels sur la santé d'environ 3,4 millions de personnes, dont environ 1,4 million de personnes enceintes et environ 1,94 million de fœtus ou d'enfants.

Les renseignements personnels sur la santé copiés du serveur touché avaient été recueillis auprès de 242 établissements et fournisseurs de soins de santé, la plupart de l'Ontario, concernant des traitements de fertilité, des soins aux personnes enceintes, des soins néonataux et des soins aux enfants fournis de janvier 2010 à mai 2023. Les données exfiltrées comprenaient des fichiers qui étaient en cours de transfert à diverses fins, dont l'analyse, l'assurance de la qualité ou la distribution à des partenaires autorisés.

Les données exfiltrées comprenaient des renseignements personnels et des renseignements personnels sur la santé tels que les suivants : nom, adresse, code postal, date de naissance, numéro de carte Santé (sans code de version), résultats d'analyses en laboratoire, type de naissance et interventions ou procédures, facteurs de risque durant la grossesse, issue de la grossesse et de la naissance et autres caractéristiques de la personne ou des soins, par exemple, taille et indice de masse corporelle. Certaines des données exfiltrées comportaient des codes arbitraires, par exemple, des diagnostics en santé mentale et d'autres éléments recueillis à l'égard desquels il fallait choisir dans une liste préétablie d'options. Les types de données touchées variaient selon le particulier concerné.

Les données exfiltrées ne comprenaient pas les codes de version et les dates d'expiration des cartes Santé, ni les codes de sécurité à neuf caractères figurant au verso de ces cartes, ni d'images numérisées de ces cartes, de cartes de crédit, de renseignements bancaires ou financiers, de numéros d'assurance sociale ou encore d'adresses courriel ou de mots de passe de patients.

D'après les renseignements fournis, j'estime que la personne prescrite a pris des mesures raisonnables pour déterminer la portée de l'atteinte à la vie privée et fourni des renseignements adéquats sur le nombre de particuliers concernés par l'incident et les types de renseignements personnels sur la santé en cause.

Découverte et maîtrise de l'atteinte à la vie privée

Le 31 mai 2023, Progress Software (le « fournisseur ») a envoyé un avertissement de sécurité à la personne prescrite au sujet de la vulnérabilité. Après avoir reçu cet avertissement, la personne prescrite a confirmé l'exploitation et l'extraction de données en effectuant une analyse des journaux de transfert de fichiers de MOVEit, du serveur de transfert sécurisé de fichiers et du système de détection aux terminaux. La personne prescrite a pris immédiatement les mesures correctives suggérées dans l'avertissement de sécurité pour neutraliser la vulnérabilité.

Pour maîtriser l'atteinte à la vie privée, la personne prescrite a désactivé l'accès au serveur touché et l'a mis hors ligne. Par prudence, le système d'information de la personne prescrite, hébergé dans des serveurs différents d'un centre de données distinct, a également été mis hors ligne et éteint afin de réduire le risque de mouvement latéral et d'attaques supplémentaires de la part des auteurs de menace.

Le même jour, les membres de l'équipe de direction de la personne prescrite ont été informés de l'exploitation de la vulnérabilité. La personne prescrite a également informé son assureur et a obtenu les services d'un avocat spécialisé dans la gestion des atteintes à la vie privée (l'« avocat »). De plus, elle a retenu les services d'experts externes en cybersécurité aux fins de son enquête.

Le 1er juin 2023, les experts externes en cybersécurité de la personne prescrite ont pu extraire des indications confirmant l'exploitation du serveur touché. Une analyse supplémentaire a confirmé l'exploitation du portail Web du logiciel MOVEit, la présence d'un interpréteur de commandes Web persistant, l'accès à des données de nature délicate et l'exfiltration de données deux jours après l'exploitation initiale, mais avant que le fournisseur ne signale la vulnérabilité à la personne prescrite.

La personne prescrite a ensuite déterminé tous les utilisateurs qui avaient accès à la fois au serveur touché et à son système d'information. Les mots de passe de ces personnes ont été réinitialisés par précaution, afin d'atténuer le risque d'autres exploitations.

Les experts externes en cybersécurité de la personne prescrite n'ont trouvé aucun signe de mouvement latéral des auteurs de menace hors du serveur touché. Ils ont donc délivré, le 5 juin 2023, une attestation confirmant la sécurité du système d'information de la personne prescrite. Le même jour, la personne prescrite et son avocat ont examiné l'attestation, et ont conclu que le système d'information de la personne prescrite était sécuritaire et l'ont remis en ligne.

Bien que la personne prescrite ait pris toutes les mesures correctives recommandées, l'accès au portail accessible sur le Web du logiciel MOVEit, la source de la vulnérabilité, a été désactivé, et le serveur touché a été mis hors service.

La personne prescrite a précisé n'avoir jamais été en contact avec les auteurs de menace. De plus, elle a conservé l'accès à tous les fichiers de données touchés en tout temps.

D'après les renseignements fournis, j'estime que la personne prescrite a pris des mesures raisonnables pour maîtriser l'atteinte à la vie privée après l'avoir découverte.

Notification

Soulignons qu'en règle générale, une personne prescrite n'avise pas directement les particuliers en cas d'atteinte à la vie privée faisant intervenir des renseignements personnels sur la santé dont elle a la garde ou le contrôle. On s'attend plutôt à ce qu'elle avise le dépositaire de renseignements sur la santé ou l'organisme qui a fourni ces renseignements, afin qu'il puisse aviser lui-même les

particuliers concernés conformément au paragraphe 12 (2) de la LPRPS. Cette règle est énoncée comme suit dans le manuel :

> [Traduction]
>
> … en tant que collecteur secondaire de renseignements personnels sur la santé, la personne prescrite ou l'entité prescrite ne doit pas aviser directement de l'atteinte à la vie privée le particulier concerné par ces renseignements. Le cas échéant, l'avis aux particuliers doit être donné par le ou les dépositaires pertinents, à moins que le CIPVP n'autorise un autre mode de notification des particuliers concernés par l'atteinte à la vie privée.

Cependant, la portée et les circonstances de l'atteinte à la vie privée justifiaient en l'occurrence un autre mode de notification, c'est-à-dire de la part de la personne prescrite, que le CIPVP a approuvé au préalable conformément au manuel.

Après avoir consulté le CIPVP, la personne prescrite a pris les mesures suivantes pour aviser de l'atteinte à la vie privée les organismes publics ainsi que les dépositaires de renseignements sur la santé et particuliers concernés.

Notification initiale

Après l'incident, la personne prescrite a avisé :

- la Police provinciale de l'Ontario, le 1er juin 2023;
- le ministère de la Santé et Santé Ontario, le 1er juin 2023;
- le CIPVP, le 5 juin 2023;
- les dépositaires de renseignements sur la santé concernés, le 6 juin 2023.

De plus, la personne prescrite a publié un avis sur son site Web le 7 juin 2023. Le même jour, elle a mis sur pied un centre d'assistance téléphonique afin de fournir des renseignements de base au public.

Avis aux dépositaires de renseignements sur la santé concernés

Le manuel prévoit que si les renseignements personnels sur la santé fournis à une personne prescrite sont volés ou perdus, ou encore recueillis, utilisés ou divulgués sans autorisation, la personne prescrite doit aviser à la première occasion raisonnable le dépositaire de renseignements sur la santé qui lui a fourni les données.

La personne prescrite a avisé les dépositaires de renseignements sur la santé de l'incident le 6 juin 2023. De plus, à compter du 28 juin 2023, elle a envoyé aux dépositaires de renseignements sur la santé et à d'autres partenaires une mise à jour sur son enquête ainsi que des renseignements sur la quantité et la portée des données émanant d'eux qui avaient été exfiltrées. Les dépositaires de renseignements sur la santé ont été également invités à des séances de discussion (webinaires) animées par la personne prescrite en collaboration avec l'avocat externe et l'assureur de la personne prescrite. Ces séances ont eu lieu les 5, 7, 10, 17 et 19 juillet 2023.

Avis aux particuliers concernés

Après mûre réflexion, la personne prescrite a opté pour un processus de notification *indirecte* centralisé et coordonné, en collaboration avec les fournisseurs de soins de santé touchés, pour que les particuliers concernés reçoivent un message clair, cohérent et fiable au sujet de l'atteinte à la vie privée, et qu'ils disposent de plusieurs moyens équitables d'obtenir des renseignements supplémentaires.

Avant de décider de donner un avis indirect aux particuliers concernés par l'atteinte à la vie privée, la personne prescrite a tenu compte du caractère délicat des données en question, du fait qu'un avis direct supposerait une grossesse passée et pourrait traumatiser à nouveau une personne ayant eu une grossesse ou une naissance non déclarée ou dont l'issue a été défavorable.

La personne prescrite a également tenu compte de la structure unique des données touchées. Par exemple, dans bien des cas, de trois à six dépositaires de renseignements sur la santé avaient fourni les mêmes renseignements sur le même particulier pour chaque naissance ou grossesse, de sorte qu'un processus décentralisé de notification directe pris en charge par ces dépositaires de renseignements sur la santé aurait pu faire en sorte que les particuliers concernés reçoivent des avis multiples de la part d'organismes différents au sujet des mêmes dossiers compromis.

Parmi les autres facteurs pertinents, mentionnons le nombre élevé de parties concernées (environ 3,4 millions) et la probabilité que les coordonnées détenues à leur sujet soient périmées, étant donné que les données touchées remontaient dans certains cas à 2010.

Après avoir tenu compte de ces variables, la personne prescrite a établi qu'un processus centralisé de notification indirecte, dirigé par elle en collaboration avec les dépositaires de renseignements sur la santé et permettant aux parties concernées de s'auto-identifier, serait le moyen le plus sécuritaire et le plus efficace de notifier ces parties.

Processus de notification indirecte

La personne prescrite a avisé les particuliers concernés de l'atteinte à la vie privée le 25 septembre 2023, après avoir consulté le CIPVP et obtenu son autorisation.

Le processus de notification indirecte de la personne prescrite comportait les éléments suivants :

1. Avis public dans les médias et les sites Web des dépositaires de renseignements sur la santé indiquant la nature de l'incident et recommandant de visiter le site Web sur cet incident que la personne prescrite avait mis sur pied.
2. Site Web sur l'incident, accessible en plusieurs langues, avec des questions d'auto-identification permettant aux particuliers de déterminer s'ils étaient concernés par l'incident.
3. Service d'assistance téléphonique (en anglais et en français), accessible du lundi au vendredi de 8 h à 16 h, heure de l'Est.
4. Possibilité de poser des questions plus détaillées aux représentants de la personne prescrite au besoin.

Le processus de notification indirecte de la personne prescrite comportait les étapes suivantes :

Mesures préalables à la notification

- Préparation du contenu de l'avis pour la personne prescrite et les dépositaires de renseignements sur la santé, notamment le contenu du microsite, des questions fréquentes, un communiqué de presse, des déclarations pour les sites Web et des messages à afficher sur place;
- Création du microsite, avec des contenus en cinq langues;
- Rédaction du script pour le service d'assistance téléphonique;
- Rédaction des principaux messages;
- Information des parties prenantes.

Notification

- Diffusion du communiqué de presse sur les fils de presse le 25 septembre 2023;
- Lancement du microsite sur l'incident le 25 septembre 2023 (mise hors service le 12 février 2024);
- Publication des déclarations des dépositaires de renseignements sur la santé dans leurs sites Web et affichage dans leurs locaux le 25 septembre 2023 (jusqu'au 31 décembre 2023);
- Activation du service d'assistance téléphonique le 25 septembre 2023 (mise hors service le 31 janvier 2014);
- Rapports quotidiens de surveillance des médias traditionnels et sociaux, du service d'assistance téléphonique et de la fréquentation des sites Web;
- Coordination d'entrevues avec les médias.

Mesures faisant suite à la notification

- Poursuite de la surveillance quotidienne des médias traditionnels et sociaux;
- Mesure quotidienne d'audience Web effectuée par un fournisseur externe;
- Rapports quotidiens et hebdomadaires et recours aux échelons supérieurs par les fournisseurs du service d'assistance téléphonique.

Contenu de l'avis indirect

Le site Web de la personne prescrite contenait un résumé de l'incident, un questionnaire d'auto-identification détaillé, une liste de questions fréquentes, une liste des fournisseurs des données touchées, un lien vers le communiqué de presse de la personne prescrite sur l'incident et les coordonnées de son centre d'assistance téléphonique sur cet incident, qui a été accessible du lundi au vendredi de 9 h à 17 h, de juin 2023 au 31 janvier 2024.

D'après mon examen, le site Web de la personne prescrite sur l'incident contenait tous les éléments qui doivent figurer dans un avis aux patients selon les lignes directrices du CIPVP, y compris des renseignements sur la nature et la portée de l'atteinte à la privée, les types de renseignements personnels sur la santé en cause et les mesures que la personne prescrite avait prises pour maîtriser l'atteinte à la vie privée. Il précisait également que le CIPVP avait été informé de celle-ci et que les parties concernées avaient le droit de porter plainte au CIPVP, et contenait les coordonnées du

centre d'assistance téléphonique de la personne prescrite concernant l'incident, que l'on pouvait joindre pour toute question.

Analyse des mesures de notification prises par la personne prescrite

D'après les renseignements dont je dispose, j'estime que la personne prescrite a pris des mesures raisonnables pour aviser de l'atteinte à la vie privée les particuliers concernés.

Cela dit, je suis consciente du fait qu'il est généralement préférable que les dépositaires de renseignements sur la santé, ou les personnes prescrites agissant en leur nom à des fins de notification, donnent un avis direct aux particuliers éventuellement concernés par une atteinte à la vie privée. Une correspondance directe est plus susceptible d'attirer l'attention du particulier sur cette possibilité qu'un avis affiché. Cependant, en l'occurrence, étant donné le très grand nombre de particuliers touchés par cet incident et les circonstances uniques de l'atteinte à la vie privée, il était raisonnable pour la personne prescrite de conclure qu'il était impossible de donner un avis direct.

Un dépositaire de renseignements sur la santé qui envisage de donner un avis indirect devrait consulter au préalable le CIPVP au sujet de ses intentions et être disposé à expliquer pourquoi, selon lui, il est raisonnable de donner un tel avis dans les circonstances, et à décrire comment il entend s'y prendre. Parmi les facteurs qui peuvent peser en faveur d'un avis indirect, mentionnons un nombre élevé de parties concernées, la probabilité que leurs coordonnées soient périmées et la probabilité qu'un avis direct pose un risque de préjudice pour les particuliers.

Les dépositaires de renseignements sur la santé qui souhaitent donner un avis indirect doivent prendre des mesures raisonnables pour le porter à l'attention des parties concernées. Se contenter de publier un avis indirect dans leur site Web ne suffira presque jamais pour respecter les obligations en matière de notification en vertu de la *Loi*, car il est possible que les parties concernées n'aient pas l'habitude de visiter le site Web du dépositaire, de sorte qu'elles seraient peu susceptibles d'y trouver l'avis à moins qu'on ne leur suggère de le visiter.

Le dépositaire de renseignements sur la santé qui envisage de donner un avis indirect doit examiner attentivement les modes de communication les plus susceptibles de joindre les particuliers concernés. Il faut bien réfléchir à la stratégie qui sera la plus efficace pour rejoindre le public cible. Le recours à plusieurs méthodes de notification du public constitue probablement le moyen le plus efficace de rejoindre les personnes concernées. Une stratégie multimédia comprenant des communiqués de presse, des avis bien visibles sur la page d'accueil du site Web du dépositaire, des publications sur les comptes de médias sociaux du dépositaire concernant l'atteinte à la vie privée, des affiches installées dans les zones très fréquentées de son établissement, des annonces dans les journaux concernant l'atteinte à la vie privée et d'autres mesures propres à chaque cas visant à porter l'avis à la connaissance des parties concernées devrait être considérée comme une pratique exemplaire dans ces circonstances.

En ce qui concerne le contenu de l'avis indirect, le dépositaire de renseignements sur la santé doit s'assurer que cet avis contient des renseignements complets sur l'atteinte à la vie privée et assez de précisions pour que le lecteur puisse déterminer facilement s'il est concerné par l'incident et

pourquoi. Ainsi, l'avis indirect doit identifier clairement les catégories de patients qui ont été touchés par l'atteinte à la vie privée, la période en question, les renseignements concernés et en quoi ces renseignements ont été touchés par l'atteinte à la vie privée. L'avis indirect doit aussi contenir tous les éléments que les avis aux patients doivent comprendre conformément aux lignes directrices.

Dans la présente affaire, j'estime que la personne prescrite a pris des mesures raisonnables pour porter l'avis indirect à l'attention des parties concernées. Ainsi, elle a publié un communiqué de presse sur l'incident, lequel a fait l'objet d'une large couverture, elle a demandé aux 242 fournisseurs de soins de santé concernés de publier et de tenir à jour un avis sur l'incident dans leur site Web et leurs établissements pendant au moins 90 jours, et elle a mis sur pied un site Web spécialisé sur l'incident qui a été en ligne pendant quatre mois et demi suivant la remise de l'avis aux parties concernées.

J'estime également que la personne prescrite a pris des mesures raisonnables pour que l'avis indirect contienne des renseignements complets sur l'incident, avec suffisamment de précisions pour permettre au lecteur de déterminer s'il était concerné et en quoi il l'était. Pour tirer cette conclusion, j'ai examiné les renseignements accessibles dans le site Web de la personne prescrite sur l'incident, lequel contenait entre autres un questionnaire d'auto-identification détaillé permettant aux particuliers de déterminer si l'atteinte à la vie privée avait eu une incidence sur eux. Les personnes souhaitant obtenir des renseignements supplémentaires ou des éclaircissements sur l'atteinte à la vie privée pouvaient joindre un service d'assistance téléphonique qui a été accessible du lundi au vendredi pendant quatre mois suivant la notification.

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

Selon les lignes directrices du CIPVP, l'enquête sur une atteinte à la vie privée et les mesures correctives doivent comprendre un examen des circonstances entourant l'incident et de la question de savoir si les politiques et procédures en place sont suffisantes pour protéger les renseignements personnels sur la santé. Cette démarche est conforme aux exigences imposées aux personnes prescrites à la suite d'une atteinte à la vie privée selon le manuel.

<u>Enquête sur l'attaque</u>

La personne prescrite a fait appel à des experts externes en cybersécurité dans le cadre de son enquête, laquelle lui a permis de constater que les auteurs de menace avaient lancé leur attaque contre le serveur touché le 28 mai 2023. Ce jour-là, ils ont exploité une vulnérabilité d'une injection SQL (CVE-2023-34362) pour obtenir l'accès non autorisé au serveur touché par élévation des privilèges. Plus précisément, les auteurs de menace ont créé une porte dérobée en installant le nouvel interpréteur de commandes Web human2.aspx camouflé sous le nom de human.aspx, un élément légitime du logiciel de transfert de fichiers MOVEit. Aucune donnée n'a été exfiltrée pendant cette attaque initiale.

Le 31 mai 2023, les auteurs de menace ont exfiltré environ six gigaoctets de données contenues dans 120 fichiers. Cette exfiltration a eu lieu environ deux heures avant que le fournisseur n'envoie

l'avertissement de sécurité à ses clients, y compris à la personne prescrite, pour les mettre au courant de la vulnérabilité.

L'enquête de la personne prescrite a révélé que les auteurs de menace avaient copié les données à environ 12 h 30, heure de l'Est, le 31 mai 2023. Le fournisseur a envoyé son premier avertissement de sécurité à environ 14 h, heure de l'Est, ce jour-là. Cet avertissement a été mis en quarantaine par les mécanismes de sécurité du système de courrier électronique de la personne prescrite.

La personne prescrite a déclaré avoir maîtrisé l'atteinte à la vie privée le 31 mai 2023 vers 18 h. Selon elle, rien ne permettait de croire que les auteurs de menace étaient parvenus à accéder au serveur touché après 12 h 30 ce jour-là.

D'après les renseignements fournis, j'estime que la personne prescrite a pris des mesures raisonnables pour enquêter sur les circonstances entourant l'atteinte à la vie privée et qu'elle en a déterminé adéquatement sa cause première et les différents agissements des auteurs de menace au cours de l'attaque.

Mesures correctives

Cette atteinte à la vie privée a été causée par une vulnérabilité de jour zéro dans le portail Web du logiciel MOVEit, que les auteurs de menace ont exploitée pour obtenir l'accès aux renseignements personnels sur la santé stockés dans le serveur de transfert sécurisé de fichiers de la personne prescrite.

Après l'atteinte à la vie privée, la personne prescrite a désactivé le portail Web, mis hors service le serveur touché et cessé d'utiliser le logiciel de transfert de fichiers MOVEit.

Par la suite, la personne prescrite a choisi un nouveau fournisseur de logiciel de transfert sécurisé de fichiers[6]. Pour ce faire, elle a passé en revue les normes de l'industrie et consulté d'autres personnes prescrites et entités prescrites au sujet de leurs services de transfert sécurisé de fichiers. Après cette vérification initiale, la personne prescrite a consulté des experts externes en sécurité qui ont confirmé que le fournisseur choisi était approprié pour elle compte tenu des normes de l'industrie et de ses besoins. La personne prescrite a précisé que l'accès à un portail Web n'était pas nécessaire en l'occurrence.

Des tests d'intrusion ont été effectués, et les recommandations formulées par la suite ont été prises en compte pour le paramétrage du nouveau système. Ainsi, la personne prescrite implante une architecture de sécurité multicouche en lien avec son système de transfert sécurisé de fichiers; ses particularités ont été communiquées au CIPVP mais ne sont pas publiées pour des raisons de sécurité.

[6] Comme dans le cas de MOVEit, la personne prescrite a acheté uniquement une licence d'utilisation du nouveau logiciel de transfert sécurisé de fichiers. Le nouveau fournisseur n'a pas accès aux données de la personne prescrite, car celle-ci héberge le logiciel dans son environnement.

De plus, la personne prescrite a fait savoir que dorénavant, tous les services d'analytique seraient limités à l'environnement de la personne prescrite et que les logiciels et données seraient accessibles uniquement par réseau privé virtuel.

D'après les renseignements fournis, je suis persuadée qu'après l'atteinte à la vie privée, la personne prescrite a pris des mesures correctives raisonnables et a amélioré ses mesures de sécurité afin d'éviter que des attaques de ce genre ne se reproduisent.

Examen des règles de pratique et de procédure en place pour protéger la vie privée

En vertu du paragraphe 13 (2) du Règlement 329/04 pris en application de la *Loi*, le CIPVP doit examiner et approuver tous les trois ans les règles de pratique et de procédure des organisations désignées comme personnes prescrites pour l'application de l'alinéa 39 (1) c) de la *Loi*. Ces règles de pratique et de procédure visent à protéger la vie privée des particuliers dont ces organisations reçoivent les renseignements personnels sur la santé les concernant et à maintenir la confidentialité de ceux-ci.

Les attentes du CIPVP à l'égard des personnes prescrites pour l'application de l'alinéa 39 (1) c) de la LPRPS sont énoncées dans le manuel, qui représente le principal document décrivant les règles de pratique et de procédure que le CIPVP attend des personnes prescrites et des entités prescrites.

Entre autres choses, le manuel prévoit que les personnes prescrites et les entités prescrites doivent élaborer et mettre en œuvre, à tout le moins, une politique générale de sécurité de l'information, et que cette politique [traduction] « doit exiger que des mesures raisonnables dans les circonstances soient prises pour protéger les renseignements personnels sur la santé contre la perte, le vol ou une utilisation ou une divulgation non autorisée, et s'assurer que les dossiers de renseignements personnels sur la santé sont protégés contre une duplication, une modification ou une élimination non autorisée ». Cette obligation correspond à celle qu'impose aux dépositaires de renseignements sur la santé le paragraphe 12 (1) de la LPRPS.

Les pratiques de protection de la vie privée et de sécurité de la personne prescrite qui étaient en place au moment de l'atteinte à la vie privée figuraient dans la version 3.1.1 de son plan de gestion de la confidentialité et de la sécurité de l'information (PGCSI). Le CIPVP a approuvé ces pratiques dans le cadre de son processus d'examen triennal[7] le 31 octobre 2020, pour une période de trois ans qui a pris fin le 31 octobre 2023. C'est le 31 octobre 2023 que le CIPVP a examiné et approuvé à nouveau les pratiques de protection de la vie privée et de sécurité de la personne prescrite, pour une période de trois ans devant prendre fin le 31 octobre 2026. Ces pratiques sont énoncées dans la version 3.2.2 du PGCSI de la personne prescrite et comprennent les recommandations que le CIPVP a formulées lors de son dernier examen triennal.

Les pratiques de protection de la vie privée et de sécurité du PGCSI de la personne prescrite qui sont les plus pertinentes dans le contexte de cet incident sont les suivantes :

[7] Des renseignements et documents sur le processus d'examen et d'approbation du CIPVP pour les entités et personnes prescrites en vertu de la LPRPS figurent dans la page Reviews and Approvals: Documentation | Commissaire à l'information et à la protection de la vie privée de l'Ontario (ipc.on.ca/fr) (en anglais seulement).

- P-29, P-29A et P-29B (gestion des atteintes à la vie privée, protocole de gestion des atteintes à la vie privée, formulaire de signalement des atteintes à la vie privée);
- P-30 (journal des atteintes à la vie privée);
- S-05 (conservation sécurisée de dossiers de renseignements personnels sur la santé);
- S-07 (transfert sécurisé de dossiers de renseignements personnels sur la santé);
- S-10 (journalisation, audit et surveillance des événements liés à la protection de la vie privée et à la sécurité de l'information);
- S-11 (gestion des vulnérabilités et des correctifs);
- S-17 (gestion des brèches de sécurité de l'information);
- S-18 (journal des brèches de sécurité de l'information).

Après l'atteinte à la vie privée, et en réaction à cet incident, la personne prescrite a modifié les politiques suivantes :

- S-05 : Cette politique a été mise à jour afin de prévoir que les fichiers hébergés dans le serveur de transfert sécurisé de fichiers doivent en être retirés après une période prescrite.
- S-07 : Cette politique a été mise à jour afin de refléter le nouveau processus de dimensionnement pour le transfert sécurisé de fichiers, qui comporte une variété de contrôles de sécurité supplémentaires.

Compte tenu des renseignements dont je dispose, j'estime qu'après l'atteinte à la vie privée, la personne prescrite a examiné ses pratiques de protection de la vie privée et de sécurité pour déterminer si elles étaient adéquates, et elle a mis à jour les pratiques pertinentes et les politiques connexes afin d'être mieux en mesure de protéger les renseignements personnels sur la santé contre de telles atteintes à la vie privée.

J'estime également que les pratiques de protection de la vie privée de la personne prescrite répondent aux attentes de notre bureau lors de telles brèches de cybersécurité. Plus précisément, l'examen des politiques de protection de la vie privée et de sécurité de la personne prescrite et des renseignements qu'elle a fournis au cours du traitement de ce dossier me porte à croire que la personne prescrite a mis en place des mesures adéquates aux fins de la prévention et de la gestion des incidents, de la détection des exploitations à distance et de la dissuasion.

Les pratiques de prévention des incidents de la personne prescrite comprennent une formation annuelle obligatoire à la cybersécurité, des pratiques et procédures de gestion de l'identité et de l'accès (S-01, S-03, S-05), des pratiques et procédures de journalisation, de surveillance et d'audit des incidents du système afin de détecter de façon proactive les problèmes éventuels de sécurité et d'y réagir (S-10) ainsi que des pratiques de protection des données au repos et en transit, y compris le chiffrement AES à 256 bits de toutes les données contenues dans le serveur de transfert sécurisé de fichiers.

Les pratiques de gestion des incidents de la personne prescrite comprennent des politiques et procédures d'intervention en cas d'atteinte à la vie privée et de brèche de sécurité (P-29, P-29A, P-29B, P-30, S-17, S-18), lesquelles décrivent les mesures à prendre en conséquence et le personnel responsable de chaque mesure, ainsi que des mesures visant à tester sa capacité de

réaction aux incidents et sa posture en matière de sécurité et à les tenir à jour, notamment des exercices de table annuels, des évaluations de l'impact sur la vie privée et des évaluations de la menace et des risques.

Les pratiques de détection des exploitations à distance et de dissuasion de la personne prescrite comprennent des outils de détection et d'intervention à tous les terminaux du réseau, des mesures de renforcement de la sécurité pour les systèmes virtuels fondés sur un référentiel CIS et la vérification continue des vulnérabilités dans tous les systèmes. Parmi les autres mesures, mentionnons une politique de gestion des vulnérabilités et des correctifs (S-11) et des mesures de renseignement sur les cybermenaces, consistant notamment à obtenir du renseignement sur les cybermenaces, tactiques et cibles actuelles et nouvelles et à en faire le suivi.

III. Conclusion et recommandations

Compte tenu des circonstances et des mesures qu'a prises la personne prescrite, j'estime que celle-ci a réagi adéquatement à cette atteinte à la vie privée et qu'il n'y a pas lieu de poursuivre notre examen de cette affaire.

Plus précisément, j'estime que la personne prescrite a pris des mesures appropriées pour maîtriser l'atteinte à la vie privée, faire enquête à son sujet et aviser les particuliers concernés. J'estime également que la personne prescrite a pris des mesures correctives adéquates et démontré qu'elle a mis en place des pratiques suffisantes de protection de la vie privée et de cybersécurité pour éviter d'autres incidents semblables. Cependant, le CIPVP pourrait rouvrir ce dossier si des renseignements supplémentaires justifiant la tenue d'une enquête plus approfondie étaient portés à son attention.

Le CIPVP recommande vivement à la personne prescrite d'examiner et de suivre les conseils fournis dans les documents d'orientation suivants du CIPVP : *Feuille-info sur la technologie : Se protéger contre les rançongiciels*, *Feuille-info sur la technologie : Se protéger contre l'hameçonnage*, *Lignes directrices sur les interventions en cas d'atteinte à la vie privée dans le secteur de la santé* et *L'accès non autorisé aux renseignements personnels sur la santé : détection et dissuasion* pour s'assurer que ses politiques et ses règles de pratique et de procédure sont suffisantes afin de réduire le risque qu'une atteinte à la vie privée semblable se produise.

Le CIPVP vous remercie de votre collaboration dans cette affaire et de votre souci de respecter la *Loi*. La présente confirme que le CIPVP a fermé ce dossier.

Veuillez agréer, Maître, mes sincères salutations.

Denise Eades
Analyste