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

Le 14 juin 2024

Monsieur John Babos
Chef, Accès à l'information, protection de la vie privée et information ministérielle
Ministère de la Santé
99 Adesso Drive
Rez-de-chaussée
Concord ON  L4K 3C7
Courriel : GeneralAPO@ontario.ca

**Objet : PR21-00041**

Monsieur,

Le ministère de la Santé (MSAN) a signalé une atteinte à la vie privée en contravention de la *Loi de 2004 sur la protection des renseignements personnels sur la santé* (la « LPRPS ») au Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario (CIPVP) en novembre 2021, et le dossier susmentionné a été ouvert.

Cette atteinte à la vie privée a fait intervenir le vol de renseignements personnels sur la santé (RPS) de 359 663 personnes à partir de l'application COVaxON (système en ligne concernant la vaccination contre la COVID-19) par un employé du fournisseur dont l'InfoCentre provincial pour la vaccination (ICPV) avait retenu les services.

**Contexte**

L'ICPV est chargé, entre autres choses, de prendre les rendez-vous pour la vaccination, de fournir les preuves de vaccination, et de faire le suivi des stocks de vaccins et de l'administration des doses au moyen de l'application COVaxON. L'ICPV conclut des contrats avec des fournisseurs de services, qui procurent le personnel nécessaire pour s'acquitter de ces tâches et fournir des renseignements sur les rendez-vous pour la vaccination contre la COVID-19.

Le MSAN a précisé qu'il est dépositaire de renseignements sur la santé responsable des renseignements recueillis et hébergés dans l'application COVaxON par l'ICPV, et le ministère des Services au public et aux entreprises (MSPE) est le mandataire du MSAN, au sens de l'article 17 de la LPRPS, dont relève l'ICPV.

Le 15 novembre 2021, des personnes qui avaient rendez-vous pour se faire vacciner ou qui avaient téléchargé leur certificat de vaccination par l'entremise de COVaxON ont reçu des textos leur demandant des renseignements financiers. Un service de police municipal a informé le Centre des opérations en matière de cybersécurité (COC) du MSPE qu'un de ses agents et son conjoint

avaient reçu des textos importuns liés à l'ICPV. Le COC a informé le MSAN de la possibilité qu'il y ait eu accès non autorisé à l'application COVaxON, et le 17 novembre 2021, le MSPE a alerté la Police provinciale de l'Ontario. D'autres membres du public ont également fait savoir au MSAN et au MSPE qu'ils avaient reçu des textos importuns d'ordre financier leur demandant de répondre à des questions et de fournir des renseignements financiers personnels après qu'ils eurent pris rendez-vous pour recevoir un vaccin ou téléchargé des certificats par l'entremise du Portail de vaccination contre la COVID-19.

Le 22 novembre 2021, la Police provinciale a porté des accusations contre deux personnes, dont une était au service d'un fournisseur externe retenu pour fournir du personnel à l'ICPV. La seconde personne a été arrêtée au Québec. La Police provinciale estime que ces deux individus ont envoyé des milliers de textos importuns à des personnes qui avaient interagi avec COVaxON.

L'enquête de la Police provinciale a révélé que l'employé du fournisseur externe qui, dans le cadre de ses fonctions, était autorisé à accéder à COVaxON et à l'utiliser, avait volé dans ce système des noms et numéros de téléphone utilisés dans les textos.

Le MSPE et le COC ont soumis COVaxON à une enquête de sécurité pour vérifier l'utilisation et l'activité interne du système. L'analyse des journaux des utilisateurs a révélé de l'activité suspecte dans les registres de recherche de COVaxON et a permis d'établir qu'un seul utilisateur autorisé avait eu accès à un nombre anormalement élevé de dossiers en effectuant différentes recherches entre le 4 et le 20 novembre 2021. Le MSAN a établi que l'individu avait recueilli ces données en copiant-collant les résultats de sa recherche de son écran de recherche dans un tableur de son ordinateur portable. Le MSPE a conclu que les RPS ci-dessous ont été touchés, dans des combinaisons qui variaient selon la personne :

- Nom
- Numéro de téléphone
- Numéro de carte Santé
- Date de naissance
- Adresse courriel
- Clinique où le vaccin contre la COVID-19 avait été ou devait être reçu

Dans plus de 95 % des cas, le nom d'une personne, seul ou avec son numéro de téléphone, a été volé. En outre, les renseignements suivants représentaient environ 5 % du reste des autres renseignements subtilisés :

- Adresse courriel
- Numéro de carte Santé
- Date de naissance
- Clinique où le vaccin contre la COVID-19 avait été ou devait être reçu

**Questions et analyse**

Le MSAN soutient qu'en vertu de la LPRPS, il est un « dépositaire de renseignements sur la santé » en lien avec les dossiers de RPS que l'ICPV recueille et conserve, et que la personne qui a

volé les RPS de l'ICPV et son employeur (le fournisseur externe) étaient des « mandataires » du MSAN au sens de l'article 17 de la LPRPS.

Compte tenu des renseignements dont je dispose, je conviens que le MSAN est un « dépositaire de renseignements sur la santé » au sens du paragraphe 3 (1) de la LPRPS; que les dossiers auxquels une ou des personnes ont accédé sans autorisation et dont le ministère avait la garde ou le contrôle contenaient des « renseignements personnels sur la santé » au sens du paragraphe 4 (1) de la LPRPS; que la personne qui a volé des RPS de l'ICPV et son employeur (le fournisseur externe) étaient des « mandataires » du MSAN au sens de l'article 2 de la LPRPS; et qu'en raison de l'accès non autorisé commis par ses mandataires, des RPS ont été utilisés et divulgués en contravention de la partie IV de la LPRPS.

Les questions suivantes ont été soulevées pendant l'examen de ce dossier d'atteinte à la vie privée au stade du règlement anticipé :

1) Le MSAN a-t-il pris des mesures suffisantes pour maîtriser l'atteinte à la vie privée?
2) Le MSAN a-t-il pris des mesures suffisantes pour informer les personnes touchées par l'atteinte à la vie privée?
3) Le MSAN a-t-il pris des mesures raisonnables pour protéger les RPS recueillis par l'entremise de l'ICPV?
4) Le MSAN a-t-il pris des mesures raisonnables pour s'assurer que les conditions ou les restrictions imposées à ses mandataires quant à la collecte, à l'utilisation et à la divulgation de RPS étaient conformes à l'article 17 de la LPRPS?
5) Le MSAN a-t-il pris des mesures correctives raisonnables qui contribueront probablement à prévenir des atteintes à la vie privée semblables à l'avenir?

**Question 1 – Le MSAN a-t-il pris des mesures suffisantes pour maîtriser l'atteinte à la vie privée?**

Le MSAN s'est dit persuadé que cette atteinte à la vie privée a été rapidement maîtrisée compte tenu du fait que la Police provinciale a saisi les ordinateurs portables des accusés dans les jours qui ont suivi l'envoi du premier texto importun.

Comme les contrevenants présumés ont été arrêtés et que leurs portables ont été saisis moins d'une semaine après que l'atteinte à la vie privée a été constatée, et qu'ils n'ont envoyé aucun autre texto importun d'ordre financier par la suite, la Police provinciale et les ministères (MSAN et MSPE) considèrent qu'il est raisonnable de croire que l'atteinte à la vie privée a été maîtrisée rapidement.

Le MSAN soutient que le vol de données de l'ICPV avait pour but s'emparer des noms et numéros de téléphone d'Ontariennes et d'Ontariens (plus de 95 % des personnes touchées). Ces renseignements personnels ont ensuite été utilisés pour transmettre des textos importuns à ces personnes pour leur demander d'envoyer de l'argent aux contrevenants présumés. Étant donné que la Police provinciale a affirmé que personne n'avait communiqué avec elle concernant la

divulgation de leurs renseignements financiers en réponse aux textos importuns, le MSAN a fait savoir que le risque de vol d'identité et de fraude était très faible.

Dans ces circonstances, il semble que le MSAN n'ait pas d'autres mesures à prendre pour maîtriser l'atteinte à la vie privée.

**Question 2 – Le MSAN a-t-il pris des mesures suffisantes pour informer les personnes touchées par l'atteinte à la vie privée?**

Aux termes du paragraphe 12 (2) de la LPRPS, le dépositaire de renseignements sur la santé doit informer les personnes concernées par une atteinte à la vie privée à la première occasion raisonnable.

Le MSAN a fait valoir qu'il n'avait pas été mis au courant des particularités de l'atteinte à la vie privée pendant l'enquête criminelle de la Police provinciale, ce qui a retardé l'envoi d'un avis aux personnes concernées à ce sujet.

Le MSAN a indiqué que l'enquête de la Police provinciale était importante pour déterminer la portée de l'atteinte à la vie privée en relevant les noms des personnes concernées dans les éléments de preuve saisis dans le matériel informatique des accusés, en vue de permettre l'envoi d'avis à ces personnes.

En février 2022, la Police provinciale a fourni une liste contenant les noms de toutes les personnes concernées afin que les ministères puissent les confirmer en vue d'envoyer les avis. Ne sachant que les noms des personnes à l'exclusion de tout autre renseignement, le MSAN et le MSPE n'étaient pas en mesure d'identifier de façon certaine les personnes concernées par l'atteinte à la vie privée. À l'été 2022, la Police provinciale a fait savoir qu'elle pouvait fournir des données supplémentaires pour permettre l'envoi d'avis d'atteinte à la vie privée.

Le MSAN a envoyé des avis à 359 019 personnes concernées entre le 9 et le 14 décembre 2022, par courriel, par la poste et par composition automatique/téléphone.

En outre, le système ne contenait pas les coordonnées de 644 personnes concernées, et celles-ci n'ont donc pas été informées de l'atteinte à la vie privée.

Il a été impossible d'aviser certaines personnes concernées (p. ex., en cas de courriel rejeté parce qu'il n'était pas distribuable); un deuxième avis a donc été envoyé à compter du 22 mai 2023 à 11 512 personnes par la poste ou par composition automatique/téléphone; cette opération s'est terminée avec succès le 25 mai 2023.

L'avis d'atteinte à la vie privée contenait les renseignements suivants :

- des précisions sur l'atteinte à la vie privée et sur son ampleur;
- des précisions sur les RPS qui étaient en cause;
- les mesures qui avaient été prises pour maîtriser l'atteinte à la vie privée;

- le fait que le CIPVP avait été informé de l'atteinte à la vie privée, et la recommandation de consulter le site Web du CIPVP si la personne souhaitait déposer une plainte relative à la protection de la vie privée;
- les coordonnées de la personne du MSAN à qui s'adresser pour toute question.

Dans les circonstances, je suis satisfaite des mesures que le MSAN a prises pour informer les personnes concernées. Il est important que les dépositaires avisent les personnes concernées « à la première occasion raisonnable » en vertu de la LPRPS; cependant, en l'occurrence, je suis consciente du fait que l'enquête de la Police provinciale représente une circonstance atténuante qui a empêché de les informer plus tôt.

**Question 3 – Le MSAN a-t-il pris des mesures raisonnables pour protéger les renseignements personnels sur la santé recueillis par l'entremise de l'ICPV?**

En vertu du paragraphe 12 (1) de la LPRPS, le dépositaire de renseignements sur la santé doit s'assurer que les RPS sont raisonnablement protégés contre le vol, la perte et une utilisation ou une divulgation non autorisée, et que les dossiers qui les contiennent sont protégés contre une duplication, une modification ou leur élimination non autorisée. Avant l'atteinte à la vie privée, le MSAN avait pris les mesures suivantes pour protéger les RPS que détenait l'ICPV :

- L'ICPV procédait à la vérification de casier judiciaire et d'affaires judiciaires de ses employés et des employés de ses fournisseurs de services avant l'embauche. L'ICPV donnait également une formation à ses employés et aux employés de ses fournisseurs concernant leurs obligations prévues dans la LPRPS, et exigeait que ses employés et mandataires signent une entente de confidentialité reconnaissant leurs obligations en matière de protection de la vie privée et les engageant à protéger les renseignements personnels, dont les RPS.
- Le fournisseur de services s'assurait que chaque employé respectait les critères susmentionnés au moyen d'un suivi et d'enregistrements avant que le MSAN et le MSPE ne fournissent du matériel et des systèmes de la fonction publique de l'Ontario (FPO) aux employés et mandataires de l'ICPV pour qu'ils s'acquittent de leurs tâches.
- Chaque matin, avant d'ouvrir ses lignes téléphoniques au public, l'ICPV rappelait de vive voix à ses employés et aux employés de ses fournisseurs de services de garder confidentiels les RPS des particuliers.
- L'ICPV vérifiait au hasard les appels auxquels les employés répondaient à des fins de contrôle de la qualité et pour s'assurer du respect des règles de protection de la vie privée.
- Pour ouvrir une session dans le système COVaxON, l'employé devait suivre un processus d'authentification multifacteur en plus d'attester la lecture d'un avertissement concernant la protection de la vie privée.

Ces mesures sont conformes aux pratiques exemplaires prévues dans le document d'orientation du CIPVP *L'accès non autorisé aux renseignements personnels sur la santé : détection et dissuasion*[1], sauf pour les aspects suivants:

[1] *L'accès non autorisé aux renseignements personnels sur la santé : détection et dissuasion* - CIPVP

- Bien que tous les employés et agents de l'ICPV doivent suivre une formation sur la protection de la vie privée et signer une entente de confidentialité dès leur embauche, ils n'étaient pas tenus de renouveler leur entente de confidentialité chaque année.
- L'ICPV vérifiait au hasard les appels des employés à des fins de contrôle de la qualité et pour s'assurer du respect des règles de protection de la vie privée, mais il semble que l'accès à la base de données de COVaxON par le personnel et les mandataires n'était ni surveillé et ni contrôlé. La journalisation, l'audit et la surveillance peuvent prévenir efficacement l'accès non autorisé si tous les mandataires sont informés du fait que toutes leurs activités liées aux dossiers électroniques de RPS seront consignées, auditées et surveillées de façon continue, ciblée et aléatoire.

Je recommande qu'à partir de maintenant, tous les employés et mandataires de l'ICPV suivent une formation obligatoire sur la protection de la vie privée et signent des ententes de confidentialité au moment de leur embauche et chaque année par la suite pour leur rappeler les obligations en matière de protection de la vie privée qui leur incombent en vertu de la LPRPS ainsi que les règles et pratiques relatives aux renseignements du MSAN.

**Question 4 – Le MSAN a-t-il pris des mesures raisonnables pour s'assurer que les conditions ou les restrictions imposées à ses mandataires quant à la collecte, à l'utilisation et à la divulgation de RPS étaient conformes à l'article 17 de la LPRPS?**

Il est important de souligner que l'ICPV fournit à son personnel et à ses mandataires l'équipement dont ils ont besoin pour remplir leurs fonctions. L'ICPV permet également à son personnel et à ses mandataires d'accéder à l'application COVaxON et à la base de données connexe au moyen de cet équipement. Les contrats conclus avec les fournisseurs de services qui ont accès à des renseignements personnels et à des RPS sont importants pour assurer le respect de l'article 17 de la LPRPS. Le MSAN a conclu avec le fournisseur qui procure du personnel à l'ICPV un accord d'approvisionnement stratégique (contrat) qui comprend les critères suivants :

- exigences concernant la confidentialité pour protéger les renseignements personnels contre la collecte, l'utilisation, la divulgation ou la destruction non autorisées par le personnel et les mandataires;
- interdiction de copier les renseignements confidentiels;
- restrictions liées à l'utilisation et à l'accès qui mettent en relief les obligations en matière de conformité.

La Décision 110[2] en vertu de la LPRPS souligne l'importance de conclure un contrat qui énonce les attentes et les obligations relatives à la protection de la vie privée que doivent respecter les entrepreneurs indépendants qui auront accès à des RPS dont les dépositaires de renseignements sur la santé ont la garde et le contrôle comme le prévoit la LPRPS. De même, le rapport PR16-40[3]

[2] Décision 110 en vertu de la LPRPS – Commissaire à l'information et à la protection de la vie privée de l'Ontario (cipvp.ca)
[3] PR16-40 - Commissaire à l'information et à la protection de la vie privée de l'Ontario (cipvp.ca)

sur une plainte relative à la protection de la vie privée traite de l'importance qu'une institution signe un contrat détaillé avec tout fournisseur externe qui remplit des fonctions de base en son nom afin d'assurer le respect des règles et des pratiques relatives aux renseignements de l'institution et des obligations de cette dernière aux termes de la *Loi sur l'accès à l'information et la protection de la vie privée* (LAIPVP).

Les audits sont un autre moyen important, voire nécessaire, d'assurer une surveillance adéquate et la conformité aux règles et obligations de l'institution. Par conséquent, tout accord ou contrat avec un fournisseur doit prévoir des modalités explicites et exécutoires sur la tenue d'audits. S'il y avait eu des audits réguliers des activités du personnel, il aurait peut-être été possible de déceler immédiatement les agissements interdits de l'employé ou du contrevenant, empêchant ainsi le vol de RPS à partir de l'application COVaxON.

Le MSAN a fait savoir que la base de données de COVaxON utilise un logiciel particulier comme plateforme et qu'il est techniquement impossible d'empêcher les utilisateurs de copier des données à partir de l'écran d'interface du logiciel et de commettre ainsi une atteinte à la vie privée. Pour atténuer cette vulnérabilité, le MSAN a pris d'autres mesures correctives.

Il est évident que le MSAN doit prendre des mesures correctives pour mieux protéger les renseignements personnels lorsqu'il fait appel à des fournisseurs externes pour fournir des services nécessitant le traitement de RPS en vertu de la LPRPS. Ces mesures correctives sont abordées plus loin dans la section « Recommandations et prochaines étapes ».

**Question 5 – Le MSAN a-t-il pris des mesures correctives raisonnables qui contribueront probablement à prévenir des atteintes à la vie privée semblables à l'avenir?**

Après l'infraction, au début de 2022, l'ICPV a fourni à ses employés et aux employés de ses fournisseurs une formation d'appoint et exigé que tous les employés confirment avoir suivi cette formation. Celle-ci portait sur la responsabilité qu'ont les employés de recueillir, d'utiliser ou de partager des données personnelles sur la santé uniquement dans les circonstances autorisées en vertu de la LPRPS (ou de la LAIPVP). En outre, le personnel de l'ICPV et ses agents ont dû refaire leur formation sur la protection de la vie privée et signer de nouveau l'entente de confidentialité après cet événement.

Afin d'accéder à l'application COVaxON, les employés doivent suivre un processus d'authentification multifacteur en plus d'attester la lecture d'un avertissement sur la protection de la vie privée. Depuis l'atteinte à la vie privée, le MSAN a mis à jour les paramètres liés aux droits d'accès dans COVaxON, limitant les données et les fonctions auxquelles un employé peut accéder afin qu'il soit impossible désormais d'extraire et de conserver autant de renseignements que le contrevenant a pu subtiliser.

La fonctionnalité de recherche de COVaxON a été modifiée comme suit :

- Changements dans la page de recherche : La page de recherche initiale a été désactivée et remplacée par un nouvel écran de recherche. La page initiale comportait un algorithme de recherche à logique floue utilisant des champs démographiques sur le client. Le nouvel écran de recherche présente d'abord un champ dans lequel il faut entrer le numéro

de la carte Santé du client. C'est uniquement si le numéro de carte Santé ne permet pas d'obtenir une correspondance exacte que des champs de logique floue sont présentés à l'utilisateur.

Le système COVaxON interdit l'utilisation de caractères de remplacement, mais la logique floue ne permet pas d'obtenir uniquement des correspondances directes. L'algorithme à logique floue est une caractéristique importante qui permet d'éviter de créer des dossiers de clients en double.

- Masquage du numéro de carte Santé : Le numéro de carte Santé qui s'affiche lors d'une recherche de client est désormais partiellement masqué; seuls les quatre derniers chiffres s'affichent.

Outre ces changements, la formation des utilisateurs de l'ICPV a été améliorée pour souligner la nouvelle marche à suivre pour la recherche.

D'autres mécanismes de sécurité ont été mis en place pour empêcher que des employés n'exfiltrent des données. Le MSAN a demandé que le Centre des opérations en matière de cybersécurité du MSPE surveille l'application COVaxON dans le cadre de son programme de contrôle amélioré 24 heures sur 24, 7 jours sur 7, pour relever :

- un nombre anormalement élevé de dossiers qui sont consultés à partir des comptes d'utilisateurs de COVaxON;
- l'accès au même compte à partir d'adresses IP multiples (le protocole Internet est la norme de communication utilisée pour identifier les systèmes dans un réseau d'ordinateurs ou dans Internet. Chaque système réseauté se voit attribuer une adresse IP, qui permet d'identifier et de localiser ce système à des fins de transmission de données);
- un nombre suspect d'erreurs d'ouverture de session.

En outre, l'accès à l'interface de programmation d'application de la base de données de COVaxON est maintenant limité à un profil d'utilisateur précis.

Les mesures correctives susmentionnées ci-dessus sont suffisantes pour prévenir de futures atteintes à la vie privée, sous réserve des recommandations suivantes.

**Recommandations et prochaines étapes**

Il est essentiel de conclure des contrats avec les fournisseurs externes pour s'assurer que ceux-ci et leurs employés sont conscients de leurs obligations en matière de protection de la vie privée en vertu des lois applicables en ce qui concerne les renseignements personnels ou les RPS que leur confie un dépositaire. Compte tenu des renseignements fournis par le MSAN, il est difficile de déterminer comment l'ICPV confirme que les capacités de traitement des renseignements personnels et des RPS des fournisseurs respectent les modalités susmentionnées ou les exigences de la LPRPS quant à la collecte, à l'utilisation et à la divulgation de tels renseignements. Je recommande au MSAN de mettre en œuvre à la première occasion raisonnable les mesures suivantes en ce qui concerne ses relations avec des fournisseurs externes relativement à l'ICPV :

1. Veiller à ce que le MSAN exige du fournisseur qu'il prouve que le personnel qui a accès à l'application COVaxON suit une formation sur la protection de la vie privée et signe une

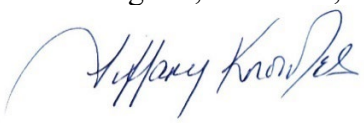
entente de confidentialité chaque année, et non seulement au moment de l'embauche, afin de sensibiliser le personnel à son obligation de se conformer aux règles et aux pratiques relatives aux renseignements du dépositaire ainsi qu'à ses obligations en matière de protection de la vie privée en vertu de la LPRPS. Il y a lieu également de consigner les dates où le personnel et les mandataires de l'ICPV ont rempli ces exigences obligatoires en matière de protection de la vie privée afin de confirmer la conformité à cette règle.

2. Veiller à ce que les fournisseurs et leurs employés comprennent que l'exfiltration de données à partir de l'application COVaxON est strictement interdite. Bien que cette interdiction soit explicitement énoncée dans le contrat du MSPE avec le fournisseur et dans l'accord de confidentialité signé par tous les mandataires de l'ICPV. Cette interdiction devrait être soulignée auprès du fournisseur et faire partie de la formation annuelle sur la protection de la vie privée du personnel et des mandataires.
3. Veiller à ce que le MSAN ou le MSPE procède régulièrement à un audit de l'accès des employés et mandataires à COVaxON pour confirmer que cet accès et l'utilisation des données sont conformes à la LPRPS. Un registre officiel détaillé de ces audits devrait également être établi.

Le MSAN a confirmé qu'il acceptait d'apporter les mesures correctives susmentionnées que le CIPVP recommande pour éviter qu'un tel incident ne se reproduise. Certaines d'entre elles ont déjà été prises.

Après avoir examiné les circonstances de cette infraction, je suis convaincue qu'il n'est pas nécessaire de poursuivre l'examen de ce dossier. Le présent rapport confirme que ce dossier est maintenant clos.

Veuillez agréer, Monsieur, mes sincères salutations.



Tiffany Knowles
Analyste