Centre de santé communautaire
Somerset Ouest

MISE À JOUR IMPORTANTE CONCERNANT L'INCIDENT DE CYBERSÉCURITÉ : FAITS ET QUESTIONS

Qu'est ce qui s'est passé ?

Comme de nombreuses autres organisations, nous avons été victimes d'un incident cybernétique. En d'autres termes, un tiers non autorisé avait accédé à nos systèmes informatiques et crypté (c'est à dire verrouillé ou rendu inaccessible) certains de nos serveurs sur lesquels nous stockons nos fichiers.

Aussitôt que nous en avons pris connaissance, nous avons désactivé notre connexion Wi-Fi et notre réseau. Nous avons également immédiatement fait appel à des experts en cybersécurité afin de sécuriser notre environnement informatique et d'enquêter sur ce qui s'était passé.

Quand cet incident s'est-il produit ?

Nous avons découvert cet incident le 30 avril 2026.

Quelles mesures avez-vous prises pour régler cet incident ?

Depuis que nous avons pris connaissance de cet incident, nous avons collaboré avec des experts en cybersécurité afin de:

- Contenir l'incident et sécuriser nos systèmes;
- Comprendre ce qui s'est passé et déterminer si des renseignements personnels avaient été compromis; et
- Renforcer nos mesures de sécurité et faire en sorte qu'un tel incident ne se reproduise plus.

Nous avons signalé cet incident à deux organismes gouvernementaux chargés de la protection de la vie privée: le Commissaire à l'information et à la protection de la vie privée de l'Ontario (CIPVP) et le Commissariat à la protection de la vie privée du Canada (CPVP).

- Le CIPVP veille à la protection des renseignements médicaux en vertu de la Loi sur la protection des renseignements personnels sur la santé (pour les bénéficiaires de nos services de santé).
- Le CPVP veille à la protection des autres informations privées en vertu de la Loi sur la protection des renseignements personnels et les documents électroniques (pour les bénéficiaires de nos programmes communautaires).

Nous avons également signalé cet incident à la police.

Est-ce que vos services sont affectés ?

Nos programmes et services sont actuellement fonctionnels. Nous avons communiqué directement avec des clients pour des cas exceptionnels.

Pourquoi vos systèmes de sécurité informatique n'ont-ils pas été en mesure de prévenir cet incident cybernétique ?

Au fil des ans, nous avons travaillé en étroite collaboration avec notre prestataire de services informatiques afin de sécuriser nos systèmes. Cependant, les cybermenaces sont en constante évolution, et ce type d'incident n'est pas toujours évitable. Depuis la découverte de cet événement, nous avons collaboré avec des experts en cybersécurité afin de renforcer notre sécurité et d'éviter qu'un tel incident ne se reproduise. Nous surveillons activement nos systèmes afin de nous prémunir contre de futures menaces.

La sécurité de vos données constitue une priorité absolue pour nous.

Avez-vous mené une enquête sur cet incident ?

Oui, nous avons fait appel à des experts en cybersécurité pour nous aider à enquêter sur ce qui s'est passé. Toutefois, pour préserver la sécurité de nos systèmes informatiques, nous ne communiquerons pas davantage de détails sur cette enquête.

Est-ce que la menace est désormais écartée ?

Oui, l'incident a été contenu. Nous ne décelons plus aucun signe d'activité non autorisée.

Peut-on à l'avenir communiquer des informations personnelles au CSCSO en toute sécurité ?

Aucun système informatique ne peut être à l'abri à 100 % de toutes les attaques potentielles. La protection de vos informations reste néanmoins une priorité absolue pour nous. Nous avons collaboré avec des experts en cybersécurité afin de renforcer notre sécurité et d'éviter qu'un tel incident ne se reproduise. Nous estimons que les mesures que nous avons mises en place ont permis de sécuriser nos systèmes, et nous continuons à les surveiller de près afin de protéger vos informations.

Mes renseignements personnels ont-ils été compromis ?

Nous ne savons pas exactement quelles informations spécifiques peuvent avoir été exposées pour chaque individu. Toutefois, l'enquête nous a permis de déterminer les types de renseignements auxquels le tiers non autorisé avait accédé et/ou extrait.
Si vous bénéficiez des services de notre Carrefour d'aide aux sans-abris et de lutte contre les dépendances (Carrefour AIDE « *HART* »), de nos services de santé mentale et de counselling, du Programme de santé pulmonaire d'Ottawa, du Centre de santé pour les nouveaux arrivants d'Ottawa ou des soins de santé primaires, certains ou l'ensemble des renseignements suivants vous concernant peuvent avoir été consultés et/ou obtenus par le tiers non autorisé:

- Nom
- Date de naissance
- Adresse personnelle
- Sexe
- Numéro de téléphone
- Permis de conduire
- Numéro du Régime d'assurance-santé de l'Ontario (RASO)
- Numéro de demandeur du Programme ontarien de soutien aux personnes handicapées (POSPH)
- Demandes de logement du client
- Nom du prestataire de soins de santé
- Liste des médicaments
- Liste des allergies
- Antécédents médicaux, sociaux et familiaux
- Symptômes
- Diagnostic
- Plan de traitement
- Évaluation de handicap
- Résultats de l'examen physique
- Résultats des analyses et des examens d'imagerie
- Orientations vers des spécialistes
- Notes de consultation des spécialistes

Selon nos experts, il n'y a pas eu d'accès non autorisé à notre système de dossiers médicaux électroniques, dans lequel sont conservées la plupart des informations médicales personnelles de nos clients.

Vous pouvez consulter l'avis complet au: www.swchc.on.ca/cyber-incident.

Comment puis-je me protéger ?

Nous vous exhortons à faire preuve de prudence et à rester vigilant face aux menaces susceptibles de porter atteinte à votre identité et à vos renseignements personnels.

Voici quelques mesures que vous pouvez prendre pour vous protéger:

- Faites preuve de prudence lorsque vous communiquez des informations personnelles ou médicales, en particulier lorsque la demande est inattendue. Si une personne vous contacte à l'improviste pour vous demander des renseignements personnels, ne les divulguez pas.
- Ne cliquez sur aucun lien et ne téléchargez aucune pièce jointe provenant de courriels suspects.
- Si vous recevez un message qui semble provenir de notre centre et qui vous demande de l'argent ou d'autres renseignements personnels, sans que vous ne l'attendiez, il peut s'agir d'une arnaque. Contactez-nous directement pour confirmer avant de répondre au message.
- Si vous soupçonnez que quelqu'un utilise votre numéro d'assurance-santé de l'Ontario (RASO) sans votre autorisation, vous pouvez contacter le ministère de la Santé de l'Ontario au 1-888-781-5556, du lundi au vendredi (sauf les jours fériés), de 8 h 30 à 17 h, ou par courriel au reportohipfraud.moh@ontario.ca. Le ministère mènera une enquête et pourrait communiquer vos informations aux forces de l'ordre en cas de suspicion de fraude.

Autres questions

Pour toute question supplémentaire non traitée dans l'avis ou dans la Foire aux questions, veuillez contacter notre responsable de la protection de la vie privée au: privacyofficer@swchc.on.ca.