

MISE À JOUR IMPORTANTE CONCERNANT L'INCIDENT DE CYBERSÉCURITÉ

Au Centre de santé communautaire de Somerset Ouest (CSCSO), nous prenons très au sérieux la confidentialité et la sécurité des données personnelles et des informations médicales qui nous sont confiées. Le présent avis a pour but de vous informer que nous avons été victimes d'un incident de cybersécurité susceptible d'avoir touché vos données personnelles et/ou vos informations médicales.

Veuillez lire attentivement cet avis, qui sera bientôt disponible dans les langues suivantes: arabe, chinois simplifié et traditionnel, dari, khmer, pachto, espagnol, swahili et vietnamien, en plus du français. Vous pouvez suivre cette page pour avoir les dernières mises à jour.

Qu'est-ce qui s'est passé ?

Le 30 avril 2026, nous avons découvert qu'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 immédiatement pris des mesures pour contenir l'incident et sécuriser nos systèmes. Nous avons également fait appel à des experts en cybersécurité pour nous aider à enquêter sur ce qui s'était passé, à déterminer quelles données avaient été consultées et à vérifier si des informations sensibles avaient été compromises.

Malheureusement, l'enquête a confirmé que certaines données à caractère personnel et certaines informations médicales avaient été extraites de nos systèmes.

Quelles renseignements ont été concernés ?

Les données concernées varient d'une personne à l'autre, et 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.

À l'heure actuelle, rien n'indique que vos informations personnelles aient été utilisées à des fins d'usurpation d'identité ou de fraude.

Quelles sont les mesures qui ont été prises ?

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 fait appel à des experts en cybersécurité afin de renforcer notre sécurité et d'éviter qu'un tel incident ne se reproduise. Nous avons confiance dans les mesures que nous avons prises pour faire face à cet événement et estimons que nos infrastructures sont désormais sécurisées. Nous surveillons activement nos systèmes afin de nous prémunir contre de futures menaces. La sécurité de vos données constitue une priorité absolue pour nous.

Nous avons signalé cet incident à deux autorités chargées 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). Vous n'avez aucune démarche à effectuer, mais si vous le souhaitez, vous avez le droit de déposer une plainte auprès du CIPVP en suivant ce lien:

<https://www.ipc.on.ca/fr/ressources/formulaires/plainte-concernant-la-protection-de-la-vie-privee-en-matiere-de-sante>

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). Encore une fois, vous n'avez aucune démarche à effectuer, mais si vous le souhaitez, vous avez le droit de déposer une plainte auprès du CPVP en suivant ce lien: <https://www.priv.gc.ca/fr/signaler-des-preoccupations/> Nous avons également porté cette affaire à l'attention des forces de l'ordre.

Que pouvez-vous faire à ce sujet ?

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.

Pour des renseignements additionnels

- Vous pouvez consulter les dernières informations importantes concernant cet incident cybernétique ainsi que la foire aux questions (FAQ) au: www.swchc.on.ca/cyber-incident.
- 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

Nous regrettons sincèrement que cet incident se soit produit et vous assurons que nous le prenons très au sérieux.

Nous vous remercions pour votre patience et votre compréhension.