

Avis Important

Incident de Cybersécurité

Date de l'incident : 29 mars 2025

Radiomedic a été victime d'une cyberattaque de type rançongiciel le samedi 29 mars 2025. Cette attaque a transgressé nos systèmes de sécurité en place et a entraîné le chiffrement non autorisé de nos serveurs, ce qui a temporairement rendu les données de certains patients inaccessibles. Nous n'avons pas de preuve à ce jour que des renseignements personnels de nos patients ont été copiés ou exfiltrés, toutefois le niveau de risque a été jugé suffisant pour justifier une notification publique à titre préventif.

Informations potentiellement concernées :

- Nom
- Date de naissance
- Numéro RAMQ
- Numéro de téléphone / courriel
- Détails d'examens d'imagerie médicale

***Aucune donnée bancaire n'est concernée par cet incident.**

****Aucune donnée concernant notre personnel n'est impliquée dans cet incident.**

Mesures prises :

- Fermeture des cliniques, déconnexion immédiate et sécurisation des serveurs
- Collaboration avec des experts en cybersécurité
- Signalement aux corps policiers
- Signalement à la Commission d'accès à l'information du Québec (CAI)
- Ajout d'un service de cybersécurité avec monitoring continu 24h/24 (MDR)
- **Aucune donnée perdue grâce à nos copies de sauvegarde sécurisées**

Ce que vous pouvez faire :

- Soyez vigilant face à des appels, courriels ou messages inhabituels.
- Évitez de partager vos informations personnelles sans vérification.
- Contactez-nous si vous doutez d'une communication suspecte liée à votre dossier médical.

Pour toute question relative à la protection de vos renseignements personnels :

Responsable de la protection des renseignements personnels 📞 Téléphone : 514-470-0105

✉ Courriel : legal@radiomedic.ca Web: [Politique de confidentialité - Radiomedic](#)

Nous vous remercions de votre compréhension et restons à votre disposition pour toute question. Votre santé et votre sécurité, notre priorité.