

L'absence d'une cybersécurité robuste, expose le réseau de santé numérique de la Nouvelle-Écosse à des risques sérieux – vérificatrice générale

À publier le 22 octobre – Le gouvernement provincial n'assure pas une cybersécurité efficace des réseaux de services de santé numériques de la Nouvelle-Écosse, ce qui peut exposer ce système en croissance rapide à des risques, affirme la vérificatrice générale Kim Adair.

Adair révèle dans un nouvel audit rendu public aujourd'hui que trois entités gouvernementales partageant la responsabilité du réseau de santé numérique de la Nouvelle-Écosse mais ils manquent de responsabilité en matière de cybersécurité.

Cet aspect est crucial en raison de la dépendance grandissante du gouvernement provincial à l'égard des réseaux numériques pour le stockage de l'information personnelle et sensible sur la santé de la majorité des Néo-Écossais.

Le ministère de la Cybersécurité et des Solutions numérique, le ministère de la Santé et du Mieux-être, et Santé Nouvelle-Écosse partagent la responsabilité de la cybersécurité. Notre rapport révèle que les structures de gouvernance clés mises en place pour surveiller la cybersécurité du réseau ont disparu en 2022 et n'ont pas été remplacées.

L'absence consécutive de gouvernance de la TI engendre une responsabilisation minimale à l'égard de la cybersécurité durant une période d'expansion rapide du réseau de santé numérique de la Nouvelle-Écosse.

Plusieurs organismes de soins de santé du Canada ont récemment été victimes de cyberattaques sérieuses ayant donné lieu au vol d'information de nature délicate, ayant perturbé les soins aux patients et ayant désactivé des réseaux.

La vérificatrice générale a, pour détecter les vulnérabilités et les menaces au sein du système de services de santé en ligne de la Nouvelle-Écosse, embauché des experts indépendants en cybersécurité qui ont effectué une multitude de tests de cybersécurité.

Des travaux supplémentaires ont révélé une tolérance répandue de l'acceptation des cyberrisques et une omission de gérer les risques courants.

Les résultats de l'audit sont tellement préoccupants que la vérificatrice générale a formulé 20 recommandations, préconisant notamment

- la création d'un cadre efficace de gouvernance de la TI assurant la gestion de la cybersécurité à l'échelle du réseau de santé numérique;
- la réalisation de toutes les évaluations de la cybersécurité en suspens et la mise en application de dispositions contractuelles minimales de cybersécurité dans le cas de tous les projets de connexion au réseau;

- la mise en place d'une formation obligatoire et régulière de sensibilisation à la cybersécurité pour tous les utilisateurs du réseau de santé;
- la préparation de plans d'action pour donner suite aux rapports techniques de nos experts en cybersécurité.

« Vu les préoccupations prononcées que suscite la cybersécurité au sein du réseau de santé numérique de la Nouvelle-Écosse, nous assurerons un suivi dans un an afin d'évaluer les progrès qu'aura faits le gouvernement dans la création et la mise en œuvre de plans d'action détaillés d'atténuation des risques. »