Santé Ontario

Direction opérationnelle : Participation au modèle opérationnel provincial de cybersécurité

DESTINATAIRES : Corporations hospitalières générales, telles que définies dans les groupes A, B et C de la Loi sur les hôpitaux publics, L.R.O. 1990

ÉMETTEURS : Angela Tibando, Directrice, Excellence numérique en santé
Susan deRyk, Directrice générale régionale du Centre et de l'Ouest
Anna Greenberg, Directrice générale régionale de Toronto et de l'Est
Brian Ktytor, Directeur général régional du Nord-Ouest et du Nord-Est

CC : Matthew Anderson, Président et président-directeur général

DATE DE PUBLICATION : 20 juin 2023

Introduction

Le secteur des soins de santé est exposé à l'évolution des cybermenaces, qui peuvent compromettre la capacité de protéger les actifs de santé numériques de la province et de fournir des soins essentiels aux patients. Afin de répondre aux différents niveaux de maturité cybernétique et de réduire le risque global de cyberattaques dans le secteur des soins de santé, Santé Ontario, en partenariat et avec le financement du ministère de la Santé, a élaboré, piloté et évalué un modèle opérationnel provincial de cybersécurité (MOPC). Le modèle crée un réseau provincial conçu pour améliorer la protection des renseignements sur la santé et renforcer la continuité de la prestation des services de soins aux patients conformément aux exigences existantes en matière de d'assurance cybernétique, de réglementation et d'agrément.

Grâce à l'exécution de six projets pilotes du Centre régional des opérations de sécurité (CROS) et à des investissements ciblés au cours des deux années précédentes, les dispositions du modèle ont amélioré l'efficacité des services financiers et opérationnels, accru la cyber-résilience et aidé les entités du secteur de la santé à répondre aux exigences en matière d'assurabilité. Les projets pilotes ont également élargi la portée du partage des ressources et stimulé la mise en œuvre collective d'une approche holistique de la cybersécurité fondée sur les risques et conforme aux normes de l'industrie reconnues à l'échelle internationale.

Dans la prochaine phase du modèle opérationnel provincial de cybersécurité, les pilotes du centre opérationnel de sécurité régional existants seront transformés en groupes locaux de mise en œuvre et les groupes locaux de mise en œuvre nouvellement désignés formeront le noyau de la prestation de services partagés de cybersécurité aidant les hôpitaux à s'acquitter de leurs responsabilités réglementaires et législatives.

Direction opérationnelle

Aux fins de la présente direction opérationnelle, toutes les références aux hôpitaux généraux désignent les corporations hospitalières classées dans les groupes A, B et C dans la Loi sur les hôpitaux publics, L.R.O. 1990. Classement des hôpitaux | ontario.ca

En vertu de cette direction opérationnelle, tous les hôpitaux généraux sont tenus de s'aligner sur le modèle opérationnel provincial de cybersécurité. Le modèle concrétise la vision provinciale de la cybersécurité qui appuie le mandat de Santé Ontario d'interconnecter, de coordonner et de moderniser en toute sécurité le système de soins de santé de notre province afin de garantir que les patients ontariens reçoivent les meilleurs soins possibles axés sur le patient, quand et où ils en ont besoin.

Dans le cadre du modèle opérationnel provincial de cybersécurité, les rôles et responsabilités en matière de gouvernance et d'exécution sont les suivants :

Santé Ontario :

- définir l'orientation et la vision de la cybersécurité dans le secteur provincial de la santé;
- soutenir l'exécution et l'opérationnalisation du modèle par la publication d'orientations, de politiques, de normes, de directives et d'ententes de financement en matière de cybersécurité;
- assurer l'intégration des capacités de cybersécurité dans toutes les stratégies et exécutions numériques provinciales et régionales, en faisant rapport aux comités consultatifs régionaux sur la santé numérique;
- désigner des groupes locaux de mise en œuvre pour les services de cybersécurité partagés dans chaque région de Santé Ontario;
- affecter les hôpitaux à des groupes locaux de mise en œuvre pour la consommation de services de cybersécurité partagés;
- opérationnaliser la cybergouvernance provinciale, les plateformes technologiques, les modèles et les cadres d'incubation; et
- soutenir la mise en place d'un rôle de leadership régional en matière de cybersécurité et de comités de cybersécurité dans chaque région.

Groupes locaux de mise en œuvre :

- aider Santé Ontario à exécuter son mandat et à opérationnaliser le modèle opérationnel de cybersécurité de Santé Ontario;
- fournir des services partagés de cybersécurité aux fournisseurs de services de santé en coordination avec les fournisseurs de services de sécurité gérés qualifiés de Santé Ontario;
- aligner la technologie et les pratiques de cybersécurité sur l'orientation établie par Santé Ontario et le modèle opérationnel de cybersécurité de Santé Ontario, y compris l'approvisionnement et la gouvernance;
- développer des stratégies de co-investissement avec les membres des services partagés pour soutenir la continuité et la progression des services;
- rationaliser et harmoniser les capacités de cybersécurité entre les membres des services partagés en ce qui concerne les personnes, les processus, la technologie et les données; et
- aider les membres des services partagés à s'aligner sur l'orientation, les directives et les exigences de Santé Ontario en matière de cybersécurité et à les mettre en œuvre, y compris l'alignement avec le modèle opérationnel de cybersécurité de Santé Ontario.

Hôpitaux généraux :

- utiliser les services de cybersécurité partagés d'un groupe local de mise en œuvre assigné et s'aligner sur les priorités provinciales en matière de cybersécurité;
- continuer à exploiter des systèmes de gestion de la sécurité de l'information et des programmes de confidentialité efficaces;
- continuer à assumer la responsabilité de la protection des actifs, des données, des assurances et des exigences législatives;
- suivre les directives de notification de réponse aux incidents publiées par Santé Ontario, telles que mises à jour de temps à autre, et soumettre les informations requises par Santé Ontario à l'échange de renseignements sur les cybermenaces de Santé Ontario;
- aligner la technologie et les pratiques cybersécurité sur l'orientation établie par Santé Ontario et le modèle opérationnel de cybersécurité de Santé Ontario, et le groupe local de mise en œuvre assigné;
- continuer à réaliser les investissements permanents et nécessaires dans les capacités de cybersécurité, conformément au modèle opérationnel provincial de cybersécurité;
- développer des stratégies de co-investissement et participer à des contributions de services partagés avec un groupe local de mise en œuvre assigné afin de soutenir la continuité et la progression des services;
- assurer un soutien au niveau de la direction pour le modèle opérationnel de cybersécurité de Santé Ontario et sa mise en œuvre au sein de l'organisation; et
- exécuter, surveiller et mettre en œuvre les initiatives de cybersécurité.

Calendrier de participation

Exercice 2023-2024 : Avant le 30 juin 2023

- Santé Ontario désignera des groupes locaux de mise en œuvre dans chaque région
- Santé Ontario attribuera chaque hôpital général à un groupe local de mise en œuvre

Exercice 2023-2024 : Juillet 2023 à mars 2024

- Chaque hôpital général participera à la co-planification et à la conception des services partagés en collaboration avec le groupe local de mise en œuvre qui lui a été assigné
- Les groupes locaux de mise en œuvre établiront un modèle de services partagés, comprenant la gouvernance, la stratégie de co-investissement des membres, les feuilles de route technologiques et les soutiens des centres des opérations de sécurité hybrides
- Chaque hôpital général signera une entente de services partagés avec un groupe local de mise en œuvre
- Chaque hôpital général commencera à intégrer et à participer activement aux services partagés de cybersécurité fournis par le groupe local de mise en œuvre

Exercice 2024-2025 et au-delà

- Tous les hôpitaux généraux doivent travailler dans le cadre du modèle opérationnel provincial de cybersécurité et conformément à la direction opérationnelle.

D'autres fournisseurs de services de santé, tels que définis par la *Loi de 2019 pour des soins interconnectés*, recevront une direction opérationnelle distincte à l'avenir.

Pour toute question concernant la direction opérationnelle, veuillez communiquer avec le Centre de cybersécurité de Santé Ontario.