SoinsSantéCAN
Leadership. Innovation. Collaboration.

DÉCLARATION D'ENGAGEMENT POUR LES SOINS DE SANTÉ CYBERSÉCURITAIRES

Au 21e siècle, la sécurité des patients dépend de la cybersécurité. Les cyberattaques peuvent nuire aux systèmes de soins des patients et aux équipements médicaux. Elles peuvent interrompre des réseaux de communications et d'approvisionnement et menacer l'intégrité et la confidentialité des dossiers de santé et d'autres fondements des soins de santé modernes.

D'autre part, les solutions numériques peuvent aussi être une source importante de résilience des infrastructures essentielles et favoriser l'accès aux soins, même lorsque les services de santé locaux sont interrompus.

Nous, en tant que représentants des organisations énumérées ci-dessous, reconnaissons l'importance et l'urgence de protéger les systèmes d'infrastructures essentielles et les données contre les cybermenaces dans les organisations de soins de santé du Canada. Notre approche concorde avec la Stratégie nationale sur les infrastructures essentielles à laquelle ont souscrit les gouvernements fédéral, provinciaux et territoriaux et avec le Plan d'action sur les infrastructures essentielles.

En allant de l'avant, nous sommes conscients que les solutions numériques peuvent favoriser une plus grande résilience des infrastructures essentielles et que les défis liés à la protection des soins de santé contre les cyberattaques s'inscrivent dans un contexte de sécurité en évolution constante. Nous reconnaissons également que des cyberincidents peuvent toucher des systèmes de soins de santé essentiels partout dans le monde et entraîner ainsi des conséquences catastrophiques, y compris sur la disponibilité des systèmes de technologie de l'information et des communications et sur l'intégrité et la confidentialité des données, des systèmes auxquels le secteur des soins de santé se fie de plus en plus.

La promotion de la cybersécurité dans le secteur de la santé du Canada exige une action collective et collaborative. Ensemble, nous nous engageons à prendre les six mesures concrètes qui suivent pour améliorer la préparation et la résilience en matière de cybersécurité :

1. **Plaider en faveur :** plaider en faveur de la cybersécurité dans le système de santé du Canada;
2. **Informer :** s'assurer que nos dirigeants, nos employés et nos partenaires sont informés de l'étendue du défi et des possibilités d'atténuer le risque;
3. **Contribuer :** contribuer aux plans d'action communs qui créent la résilience collective aux cyberattaques;
4. **Progresser :** assurer la progression de la cybersécurité de manière cohérente avec notre mandat et tenir compte des occasions de prévention, d'atténuation, de préparation, de réaction et de rétablissement;
5. **Partager :** partager l'information, les pratiques exemplaires et les outils avec d'autres intervenants du secteur de la santé et d'autres secteurs pour bâtir la capacité et la résilience collectives;
6. **Faire preuve de transparence :** comme la situation et la capacité de chaque organisation sont uniques, nous confirmerons d'ici le Mois de la sensibilité à la cybersécurité, en octobre 2018, les mesures que nous prendrons pour concrétiser ces engagements dans notre contexte particulier et/ou avec notre collectivité.

Par ces mesures, nous sommes résolus à favoriser un système de santé solide, sécuritaire et efficace qui bénéficie à ceux que nous desservons.

_____ Nom

_____ Organisation