Ontario
eHealth Ontario

Résumé des obligations en matière de sécurité pour les sites qui accèdent aux DSE à partir d'un compte ONE ID ou ClinicalConnect

Le présent document a pour objet de fournir un résumé des exigences de sécurité pour se connecter aux DSE en tant qu'observateur à partir d'un compte ONE Mail ou ClinicalConnect. Il est primordial d'appliquer des mesures de sécurité efficaces pour protéger les données des patients et ainsi assurer la confiance du public à l'égard des DSE. Veuillez consulter le site Connexion et commencer votre processus d'orientation, et communiquer avec nous à l'adresse connecting.security@ehealthontario.on.ca si vous avez des questions.

1. Votre **agent de sécurité** (c.-à-d. le responsable de la sécurité informatique) doit assister au webinaire sur la sécurité, qui présente un aperçu des exigences de sécurité des DSE et sert de formation aux agents de sécurité. (Consulter le module d'apprentissage en ligne) ou (télécharger le module).
2. Demander à la **personne légalement responsable** d'examiner les responsabilités des **autorités locales en matière d'enregistrement (ALE)** et des **commanditaires** et confier ces rôles à des personnes ou à des groupes. S'assurer que ces personnes suivent la formation sur la sécurité et la protection de la vie privée à l'intention des ALE et des commanditaires. Les nouvelles ALE doivent suivre la formation sur ONE ID ou ClinicalConnect à l'intention des ALE.
3. S'assurer d'avoir une politique de sécurité des renseignements qui respecte les politiques en matière de sécurité des DSE ou adapter le modèle de politique de sécurité des renseignements mis à votre disposition à l'*annexe D* du Guide de sécurité des DSE.
4. S'assurer que votre organisme est conforme aux exigences de sécurité comportementales, techniques et administratives :

Exigences comportementales
Demander à vos utilisateurs finaux en milieu clinique de suivre la formation sur la sécurité et la protection de la vie privée à l'intention des utilisateurs finaux en milieu clinique; elle leur permettra de comprendre les exigences imposées et aidera votre organisme à atteindre la conformité.

Exigences techniques
S'assurer de ce qui suit :

a. seuls les outils approuvés des dépositaires de renseignements sur la santé sont utilisés pour se connecter à la solution de DSE;
b. le chiffrement est appliqué au disque dur de tous les appareils qui ont accès à la solution de DSE à distance;
c. les utilisateurs finaux en milieu clinique possèdent des mots de passe qui s'appliquent aux outils approuvés des dépositaires de renseignements sur la santé pour accéder aux DSE à l'ouverture de session de l'appareil. les mots de passe doivent contenir au moins huit (8) caractères et comprendre au moins trois (3) des éléments suivants :
    - un numéro,
    - une lettre en majuscule,
    - une lettre en minuscule,
    - un caractère spécial.
d. les navigateurs et les systèmes d'exploitation sont tenus à jour;
e. durant la communication de RPS au bureau du programme, comme lors de l'accès et des demandes de rectification, s'assurer que les renseignements sont cryptés en utilisant les fonctions des produits comme Microsoft Office, ou utiliser le service ONE Mail;

f. mettre en place un produit antivirus et s'assurer qu'il reste à jour;
g. si vous offrez une connexion Wi-Fi pour invités, s'assurer que le réseau pour invités est segmenté à partir du réseau de votre bureau.

Obligations administratives

h. Conserver un dossier de tous les fournisseurs de services électroniques qui soutiennent votre participation aux DSE et leur communiquer les exigences de sécurité (p. ex., le service de dépannage informatique).
i. Maintenir et mettre en œuvre un processus d'intervention en cas d'incident lié à la sécurité ainsi qu'une procédure. Un modèle de gestion d'un incident lié à la sécurité se trouve à l'*annexe C* du Guide de sécurité des DSE.