EXIGENCES EN MATIÈRE DE SÉCURITÉ POUR LES PRATICIENS EXERÇANT SEULS QUI SIGNENT L'ENTENTE ENTRE CYBERSANTÉ ET LES MÉDECINS

Version 1.0 – 3 décembre 2018

1. Définitions

« **La solution de DES** » fait référence à l'un des éléments suivants : Le visualiseur clinique ConnectingOntario, le visualiseur ClinicalConnect, SILO-DME, le portail ONE, ONE Access ou tout autre visualiseur utilisé pour l'accès aux DSE détenus par cyberSanté Ontario.

2. Résumé

Le présent document contient les exigences minimales en matière de sécurité pour les professionnels de la santé individuels (le « praticien exerçant seul ») qui sont dépositaires des renseignements sur la santé (DRS), conformément à ce qui est défini dans la *Loi sur la protection des renseignements personnels sur la santé*, et qui ont signé l'entente (l'« entente ») de cyberSanté Ontario (« cyberSanté ») et qui utiliseront des comptes ONE ID pour visionner des renseignements par l'entremise d'une solution de DSE. À moins d'indication contraire dans ce document, les mots commençant par une majuscule ont la même signification que dans l'entente.

Il s'agit des exigences minimales de la Politique et des Normes sur la sécurité dans le cadre de l'utilisation du DSE pour accéder à la solution de DSE; par conséquent, les praticiens exerçant seuls doivent entièrement s'y conformer. Pour obtenir de plus amples renseignements à propos de chacune des exigences, veuillez consulter le *Guide de sécurité des DSE à l'intention des organismes ayant seulement des droits de visualisation qui ont un compte ONE ID ou ClinicalConnect.*

3. Exigences en matière de sécurité

3.1 Politique de sécurité de l'information

3.1.1 Le praticien exerçant seul doit élaborer, mettre en œuvre et maintenir pour son organisme des normes ou des procédures en matière de sécurité des renseignements qui respectent les principes de la Politique et des Normes de sur la sécurité dans le cadre de l'utilisation du DSE.

3.2 Politique d'utilisation acceptable des données et des technologies de l'information

3.2.1 Les mots de passe doivent avoir les caractéristiques suivantes :

- Posséder un minimum de huit caractères et inclure une combinaison de lettres majuscules et minuscules, de chiffres ou de caractères spéciaux (p. ex. !, $, #, _, ~, %, ^)
- Ne pas être évidents, facilement devinables ou se retrouver dans un dictionnaire de mots courants
- Ne pas comprendre d'acronymes, de dates de naissance, de nombres séquentiels, ou encore de noms, de date de naissance ou de date d'anniversaire d'un membre de la famille ou d'un animal domestique
- Ne jamais comprendre trois caractères identiques consécutifs (p. ex., « AAA »)

3.2.2 Ne doivent jamais être divulgués à personne ou mis par écrit.

3.2.3 Changez fréquemment vos mots de passe, au moins une fois tous les 90 jours.

3.2.4 En cas de soupçon ou de confirmation que le mot de passe d'un utilisateur a été divulgué ou que sa confidentialité a été compromise, cet utilisateur doit immédiatement modifier son mot de passe et aviser son point de contact interne désigné dans le processus de gestion des incidents de sécurité.

3.3 Gestion des procédures et des appareils utilisés pour la participation à la solution de DSE

3.3.1 N'utilisez que les systèmes/appareils et les processus acquis pour la pratique du praticien exerçant seul pour participer à la solution de DSE, qu'ils soient utilisés localement ou à distance (p. ex., des postes de travail en lien avec la pratique ou des outils d'accès à distance avec chiffrement du disque, mots de passe et antivirus).

3.3.2 Si des renseignements personnels sur la santé sont enregistrés sur un appareil mobile (p. ex., téléphone, ordinateur portatif, tablette) qui est utilisé pour accéder à la solution de DSE et que cet appareil est apporté hors du site de pratique, les renseignements doivent être chiffrés ou le disque de l'appareil doit faire l'objet d'un chiffrement complet.

3.4 Communiquer de manière sécuritaire avec cyberSanté

3.4.1 Le praticien exerçant seul doit avoir en place un processus de chiffrement des courriels de nature confidentielle ou utiliser une solution de transfert de fichiers sécurisée et approuvée, telle que ONE Mail, qui chiffre les courriels envoyés aux autres utilisateurs de ONE Mail.

3.5 Fournisseurs de services électroniques

3.5.1 Le praticien exerçant seul doit tenir à jour la documentation relative aux contrats et aux ententes de soutien ainsi qu'aux niveaux de service pour tous les fournisseurs de services électroniques qui prennent en charge la participation de son organisme aux DSE.

3.5.2 Avant de conclure un contrat avec un nouveau fournisseur de services électroniques, le praticien exerçant seul doit évaluer les risques potentiels associés à ce nouveau fournisseur et trouver des façons d'atténuer ces risques.

3.6 Gestion des incidents de sécurité de l'information

3.6.1 Le praticien exerçant seul doit établir un point de contact interne (p. ex., un service de dépannage, un chef de bureau, un responsable des services administratifs) à qui les incidents de sécurité réels ou soupçonnés seront signalés et qui sera chargé de les analyser.

3.6.2 Le praticien exerçant seul doit s'assurer que tous les utilisateurs, les mandataires et les fournisseurs de services électroniques sont au fait qu'il en va de leur responsabilité de signaler immédiatement tout incident de sécurité réel ou soupçonné.

3.6.3 Suivez le processus de la Politique de gestion des atteintes à la confidentialité pour tout incident entraînant une atteinte à la confidentialité.

3.7 Le réseau et les opérations

3.7.1 Le praticien exerçant seul doit mettre en œuvre et gérer des processus de contrôle de réseau de manière à ce que les ordinateurs à l'interne (votre réseau) soient séparés d'Internet (le périmètre) et qu'ils soient protégés contre les menaces pouvant s'y retrouver.

Par exemple, si l'organisme du praticien exerçant seul fournit un accès Internet Wi-Fi aux patients, veuillez-vous assurer que ce réseau soit séparé de celui du réseau interne du praticien exerçant seul, de manière à ce que les personnes non autorisées ne puissent avoir accès au réseau interne.

3.8 Logiciels malveillants

3.8.1 Le praticien exerçant seul doit veiller à ce qu'une méthode de détection des logiciels malveillants soit appliquée à tous les appareils et les systèmes utilisés pour la participation à la solution de DSE.

3.8.2 Le praticien exerçant seul doit s'assurer que la méthode de détection des logiciels malveillants et que les correctifs sont à tous les appareils et les systèmes.

3.9 Sécurité physique

3.9.1 Le praticien exerçant seul doit s'assurer que les espaces de travail sont protégés contre les accès physiques non autorisés. Les méthodes de protection contre les accès physiques peuvent comprendre :

- La segmentation des espaces publics et des bureaux
- L'utilisation d'armoires verrouillées pour le rangement du matériel et pour l'archivage des renseignements confidentiels
- L'installation de verrous ou de serrures sur les portes et les fenêtres à risque
- L'installation de systèmes de télévision en circuit fermé et leur surveillance
- L'installation de systèmes de détection d'intrus sur les portes externes et la vérification régulière des fenêtres qui sont accessibles

3.9.2 Le praticien exerçant seul doit s'assurer d'avoir en place des procédures permettant de prévenir la destruction de données qui sont conformes aux orientations fournies par le Commissaire à l'information et à la protection de la vie privée.

3.10 Validation de l'identité et gestion de l'adhésion

Le praticien exerçant seul (ou son délégué) doit assumer les responsabilités suivantes :

3.10.1 La validation de l'identité de tous les mandataires du praticien exerçant seul qui auront accès aux renseignements des DSE en son nom, au moyen de preuves documentaires et contextuelles, dont l'examen d'au moins une pièce d'identité avec photo délivrée par le gouvernement.

3.10.2 La vérification que toutes les personnes inscrites sont âgées de 16 ans ou plus.

3.10.3 La mise à jour des dossiers d'identité selon les faits connus, p. ex., mettre à jour les dossiers afin de corriger les erreurs ou d'éliminer les comptes en double.