Guide de sécurité des DSE

À l’intention des organismes ayant seulement des droits de visualisation qui ont un compte ONE ID ou ClinicalConnect

Version 2.4

**Table des matières**

[Définition des principaux termes 4](#_Toc492907237)

[Introduction 6](#_Toc492907238)

[Aperçu de la solution 6](#_Toc492907239)

[Élaboration de votre programme de sécurité de l’information 8](#_Toc492907240)

[Principaux rôles et responsabilités 9](#_Toc492907241)

[Connexion – Étapes de la mise en œuvre et de l’adoption des mesures de sécurité 10](#_Toc492907242)

[Guide de référence rapide des politiques et normes de sécurité des DSE 11](#_Toc492907243)

[1. Politique de sécurité de l’information 11](#_Toc492907244)

[2. Norme d’utilisation acceptable des données et des technologies de l’information 12](#_Toc492907245)

[3. Norme sur la cryptographie 15](#_Toc492907246)

[4. Norme sur les fournisseurs de services électroniques 16](#_Toc492907247)

[5. Norme sur la gestion de l’information et des éléments d’actif 17](#_Toc492907248)

[6. Norme sur la gestion des incidents de sécurité de l’information 18](#_Toc492907249)

[Qu’est-ce qu’un incident? 18](#_Toc492907250)

[Le traitement d’un incident 18](#_Toc492907251)

[Rôles et Responsabilités 18](#_Toc492907252)

[Les quatre phases de la gestion des incidents de sécurité de l’information 19](#_Toc492907253)

[7. Norme sur les fournisseurs d’identités et Manuel de procédures relatives à l’admissibilité 21](#_Toc492907254)

[a. Autorité d’enregistrement 21](#_Toc492907255)

[b. Personne légalement responsable 21](#_Toc492907256)

[c. Autorité locale d’enregistrement 21](#_Toc492907257)

[d. Approbateur 22](#_Toc492907258)

[8. Norme sur les réseaux et les opérations 24](#_Toc492907259)

[Zones réseau 24](#_Toc492907260)

[Passerelles de sécurité 24](#_Toc492907261)

[Protection contre les programmes malveillants 24](#_Toc492907262)

[9. Norme sur la gestion des menaces et des risques 26](#_Toc492907263)

[Protection des documents sur l’évaluation de la menace et des risques reçus 26](#_Toc492907264)

[Annexe A : Index des ressources 27](#_Toc492907265)

[Annexe B : MODÈLE d’entente de confidentialité 29](#_Toc492907266)

[Annexe C : MODÈLE de rapport d’incident lié à la sécurité 30](#_Toc492907267)

[Annexe D : MODÈLE de politique de sécurité pour les organismes ayant seulement des droits de visualisation 30](#_Toc492907268)

[Annexe E : MODÈLE de liste de fournisseurs de services électroniques 30](#_Toc492907269)

[Annexe F : Diagrammes d’incident 31](#_Toc492907270)

[Annexe G : Définition des rôles et responsabilités 33](#_Toc492907271)

# Définition des principaux termes

| Terme | Définition |
| --- | --- |
| Chiffrement | Opération par laquelle un texte ordinaire est remplacé par un texte inintelligible aux personnes non autorisées; les données sont verrouillées avant l’envoi, puis elles sont déchiffrées ou ouvertes par une personne autorisée seulement. |
| Clé de chiffrement ou élément de clé | Clé ou élément utilisé pour chiffrer ou déchiffrer du texte. Souvent, on utilise un mot de passe pour chiffrer (verrouilller) ou déchiffrer (ouvrir) les données. Dans bien des cas, la clé doit rester confidentielle afin de protéger les données. Les dépositaires de renseignements sur la santé doivent veiller à ce que chaque clé de chiffrement ou élément de clé ait le moins de dépositaires possible. |
| Dépositaire de la clé | Mandataire ou fournisseur de services électroniques autorisé à utiliser la totalité ou une partie d’une clé de chiffrement tout au long de son cycle de vie, de sa création à sa destruction. |
| Incidents liés à la sécurité de l’information | Toute violation ou menace imminente de violation des politiques, normes, procédures ou pratiques de sécurité, ou tout incident qui pourrait compromettre l’utilisation ou menacer la sécurité d’un système d’information ou des processus opérationnels. |
| Niveau d’assurance 2 | Le niveau d’assurance indique le degré de confiance qu’on peut accorder à une déclaration d’identité.  Un niveau d’assurance 2 est nécessaire pour accéder aux renseignements hautement confidentiels de cyberSanté Ontario et du secteur de la santé destinés seulement aux personnes autorisées désignées.  Les exigences particulières sont décrites dans le document suivant :  ***https://www.ehealthontario.on.ca/images/uploads/services/resources/eHealth\_Ontario\_Federation\_Identity\_Provider\_Standard.pdf (en anglais)*** |
| Organisme ayant seulement des droits de visualisation | Organisme qui peut visualiser les données de [la solution de DSE] aux fins autorisées. L’organisme accède à la solution en lecture seule. Les organismes ayant seulement des droits de visualisation peuvent stocker quelques renseignements personnels sur la santé localement et de façon ponctuelle, mais ne peuvent importer de données ou en transférer de [la solution de DSE] à la solution qu’ils utilisent (p. ex., dossier médical électronique [DME]).  Dans le cadre des solutions de cyberSanté Ontario, ces organismes signent l’*Accord sur l’utilisation des services de DSE par un cabinet médical* ou l’*Annexe sur les services d’accès aux DSE.* |
| [la solution de DSE] | [la solution de DSE] comprend la solution et les systèmes de soutien destinés au stockage des renseignements personnels sur la santé auxquels les dépositaires de renseignements sur la santé ont accès. Les systèmes de soutien peuvent comprendre les systèmes administrés et utilisés par des fournisseurs de services électroniques dans une relation de sous-traitance. Ils excluent les systèmes d’information et les technologies de l’information que les dépositaires de renseignements sur la santé participants utilisent à titre de fournisseurs de soins de santé.  [la solution de DSE] comprend les éléments du portail utilisés par les fournisseurs de soins de santé dans le cadre de la prestation de soins aux patients, ainsi que les éléments du portail utilisés pour gérer les fonctions administratives, comme la production de rapports sur la protection de la vie privée, la gestion du consentement, la gestion des erreurs dans la liste d’attente, etc. |
| Violation de la vie privée | Les violations de la vie privée comprennent les situations dans lesquelles :   * une disposition de la *Loi de 2004 sur la protection des renseignements personnels sur la santé* ou de ses règlements d’application a été enfreinte ou est sur le point de l’être; * les dispositions sur la protection de la vie privée des [ententes en vigueur] ou de toute autre entente concernant [la solution de DSE] ont été enfreintes ou sont sur le point de l’être; * les politiques, procédures et pratiques en matière de protection de la vie privée concernant [la solution de DSE] ont été enfreintes ou sont sur le point de l’être; * les renseignements personnels sur la santé contenus dans [la solution de DSE] ont été perdus ou volés, ou ont été consultés par une personne non autorisée ou sont sur le point de l’être; * les renseignements personnels sur la santé de [la solution de DSE] ont été copiés, modifiés ou détruits sans autorisation, ou sont sur le point de l’être. |

# Introduction

Le présent guide vous aidera, en tant que dépositaire de renseignements sur la santé, à comprendre et à respecter les exigences en matière de sécurité concernant l’utilisation de [la solution de DSE] par vos bureaux en milieu communautaire, et à veiller à ce que les renseignements personnels sur la santé soient protégés et utilisés comme il se doit. Le guide présente le processus général de connexion à la solution, son aspect, les intervenants et leur rôle, ainsi que les façons de veiller à la sécurité de l’information dans le cadre de votre utilisation.

Une grande partie du guide résume la Politique et les normes de sécurité des DSE essentielles à la protection de la confidentialité, de l’intégrité et de la disponibilité des renseignements personnels sur la santé stockés ou traités dans [la solution de DSE]. Il offre des exemples et des conseils sur la façon dont votre organisme peut mettre en œuvre et respecter ces politiques. Pour en savoir plus sur les exigences, consultez la Politique et les normes de sécurité du DSE à l’intention des organismes ayant seulement des droits de visualisation.

La sécurité du DSE est importante pour minimiser le risque d’une violation de données, et confirmant il démontre l’engagement de votre organisation a la population de l’Ontario. Cela signifie la mise en œuvre des meilleures pratiques politiques et les contrôles pour protéger les données personnelles de santé. Attestant que votre organisation est conforme à la Politique et aux normes de sécurité du DSE signifie qu’il a mis en œuvre ces obligations et a communiqué au personnel de les suivre, maintenant et dans l’avenir. Toutes les organisations participantes ont une responsabilité personnelle et mutuelle de protéger les données des patients lorsqu’ils participent à la solution de dossiers de santé électroniques.

# Aperçu de la solution

Grâce à [la solution de DSE], les représentants autorisés de votre organisme auront accès aux renseignements des établissements de soins de santé externes. La solution offre un portail en ligne par lequel les utilisateurs finaux peuvent chercher un patient et accéder aux données. La *figure 1* offre un aperçu du portail en ligne de ConnexionOntario.

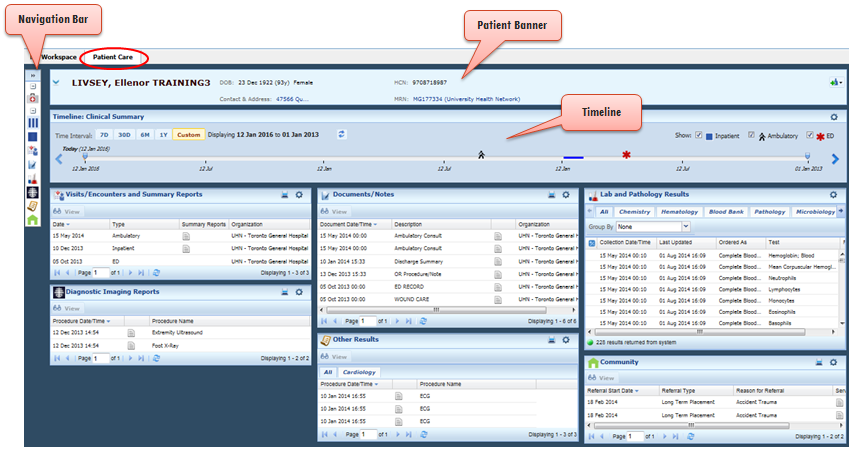


Figure 1 – Portail de [la solution de DSE]

Le visualisateur ClinicalConnect est également illustré dans la *Figure 2* à titre d’exemple.

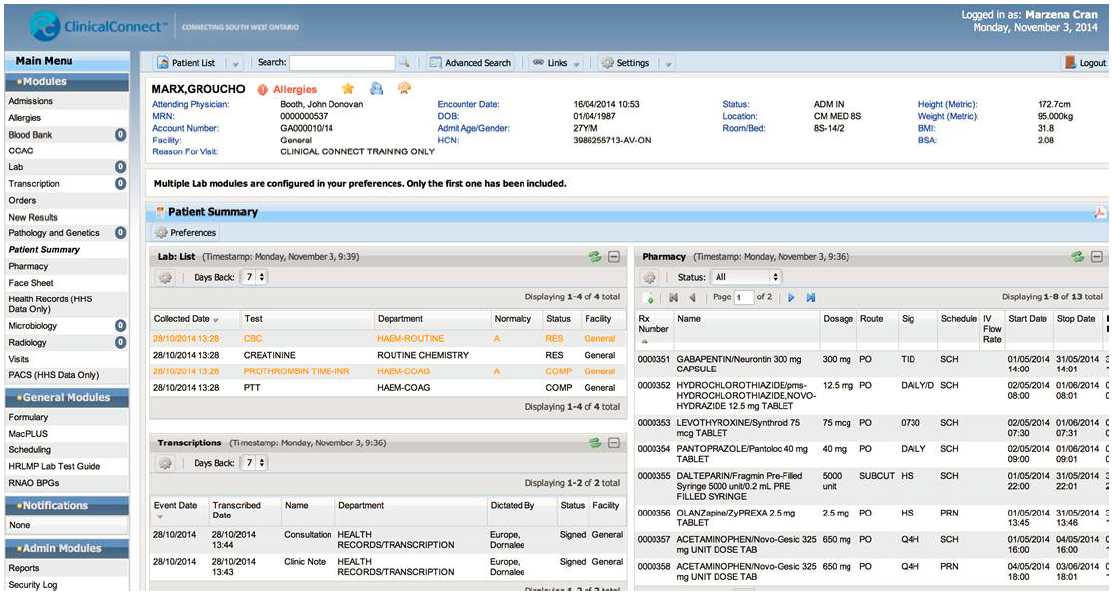


Figure 2. Visualisateur ClinicalConnect

# Élaboration de votre programme de sécurité de l’information

La *Loi de 2004 sur la protection des renseignements personnels sur la santé* (*LPRPS*) de l’Ontario vise précisément la protection de la vie privée dans le milieu de la santé. La *LPRPS* régit la façon de recueillir, d’utiliser et de divulguer les renseignements personnels sur la santé du système de soins de santé. Si tous les membres du personnel ont leur rôle à jouer dans la protection des renseignements, la *LPRPS* rend les dépositaires de renseignements sur la santé et leurs mandataires responsables de la sécurité de l’information.

Vous pourriez devoir élaborer ou améliorer le programme de sécurité de l’information de votre organisme pour veiller à ce qu’il respecte les politiques et normes de sécurité visant les DSE et puisse utiliser [la solution de DSE]. Vous devrez donc évaluer votre gestion des problèmes liés à la sécurité et adopter des pratiques exemplaires en la matière. Consignez les pratiques retenues et distribuez-les aux membres de votre équipe.

La sécurité de l’information est généralement axée sur la protection des renseignements confidentiels (p. ex., renseignements personnels sur la santé et mots de passe) et sur différents processus, comme la communication de renseignements confidentiels par courriel, l’enregistrement des utilisateurs et le signalement des incidents liés à la sécurité. Il est utile de se rappeler ces principes de base concernant la sécurité de l’information :

• **Confidentialité** – Veiller à ce que les renseignements confidentiels soient rendus disponibles ou divulgués seulement aux personnes autorisées, et à ce qu’ils demeurent confidentiels tout au long de leur cycle de vie.

• **Intégrité** – S’assurer que les renseignements confidentiels sont exacts et complets, et qu’ils restent valides tout au long de leur cycle de vie.

• **Disponibilité** – Veiller à ce que les personnes autorisées aient accès aux renseignements au moment et à l’endroit voulus.

Pour élaborer un programme de sécurité de l’information, votre organisme doit créer une politique de sécurité, définir les rôles et les responsabilités liés à la protection de l’information, veiller à ce que le personnel ait suivi une formation, surveiller la conformité à la politique, et être prêt à gérer des incidents imprévus.

Examinez les rôles qui font partie intégrante de la création d’un programme de sécurité présentés dans la *figure 2* et trouvez la personne ou le groupe de votre organisme le mieux qualifié pour s’en acquitter. Le *tableau 2* de l’*Annexe I : Définition des rôles et responsabilités* comprend des descriptions détaillées des rôles.

# Principaux rôles et responsabilités

La *Figure 2* présente les principaux rôles des dépositaires de renseignements sur la santé inhérents à l’élaboration d’un programme de sécurité de l’information et à la gestion de l’utilisation de [la solution de DSE] par votre organisme.Les pratiques exemplaires en matière de sécurité de l’information comprennent la désignation de personnes chargées de ces rôles et responsabilités qui veillent à ce que les actifs informationnels dont elles sont responsables soient protégés, et à ce que les processus de sécurité à l’appui soient respectés. Les bureaux en milieu communautaire regroupent plusieurs intervenants du programme de sécurité de l’information et de la protection des renseignements confidentiels et, dans certains cas, confient plusieurs de ces rôles à une même personne.

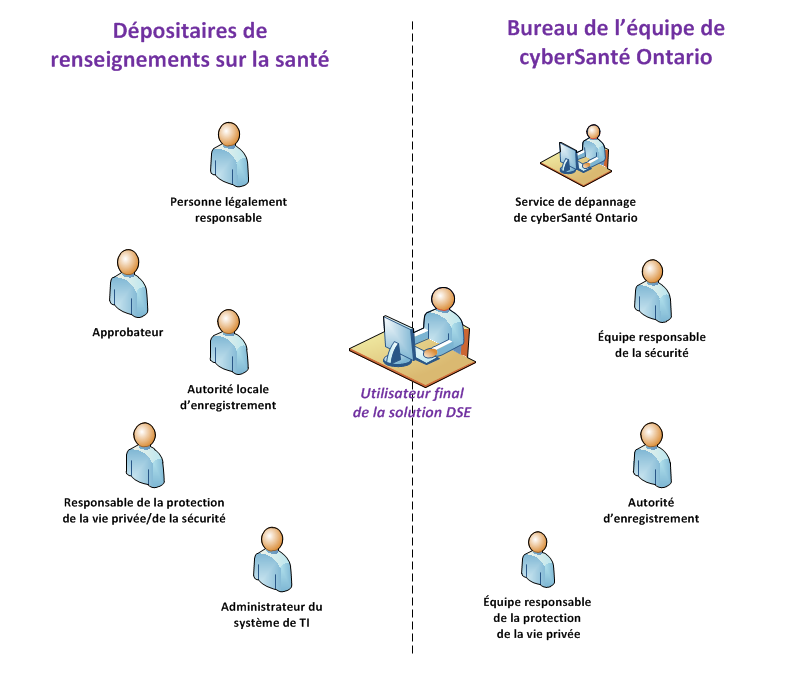


Figure 2 – Rôles et responsabilités des dépositaires de renseignements sur la santé

# Connexion – Étapes de la mise en œuvre et de l’adoption des mesures de sécurité

L’équipe responsable de la sécurité de ConnexionOntario a établi les étapes de connexion, qui sont présentées dans la *figure 3*:

Figure 3 – Étapes de connexion

Voici l’ensemble du processus que les établissements ayant seulement des droits de visualisation doivent suivre :

* Visionner ou revoir le webinaire sur la sécurité, formulé en langage clair et simple, visant à préparer votre organisme à l’utilisation de [la solution de DSE].
* Suivre ou rafraîchir la formation qui est disponible sur les processus d’enregistrement. Il est recommandé que les principaux intervenants de l’évaluation de la sécurité (responsable de la protection de la vie privée/de la sécurité et autorité locale d’enregistrement) suivent la formation avant d’entreprendre l’évaluation.
* Effectuer l’évaluation de la sécurité, qui sert à mesurer le degré de conformité de votre organisme et à cerner ses lacunes. L’équipe responsable de la sécurité de ConnexionOntario peut aider votre organisme à se préparer à utiliser la solution et à combler ses lacunes. De plus, des documents de référence et du soutien vous sont également offerts à cet effet.

Déclarer tout élément non conforme dans votre formulaire d’évaluation de la sécurité des DSE signé.

# Guide de référence rapide des politiques et normes de sécurité des DSE

La préparation des dépositaires de renseignements sur la santé ayant seulement des droits de visualisation à l’utilisation de [la solution de DSE] repose sur une Politique de sécurité des DES et huit normes de sécurité des DES qui en sont dérivées, lesquelles sont comprises dans la *Politique de sécurité tout-en-un du dossier de santé électronique à l’intention des organismes ayant seulement des droits de visualisation*.

La présente section comprend des résumés de la Politique et de chacune des normes de sécurité des DSE.

**Liste des politiques et normes de sécurité des DSE à l’intention des établissements ayant seulement des droits de visualisation**

1. Politique de sécurité de l’information
2. Norme d’utilisation acceptable des données et des technologies de l’information
3. Norme sur la cryptographie
4. Norme sur les fournisseurs de services électroniques
5. Norme sur la gestion de l’information et des éléments d’actif
6. Norme sur la gestion des incidents de sécurité de l’information
7. Norme sur les fournisseurs d’identités fédérées et Manuel des procédures relatives à l’admissibilité
8. Norme sur les réseaux et les opérations
9. Norme sur la gestion des menaces et des risques

## Politique de sécurité de l’information

Un programme de sécurité de l’information prend sa source dans une politique de sécurité de l’information, un document mis à la disposition de tout le personnel qui décrit les rôles, les responsabilités et les exigences en matière de sécurité de votre organisme.

Votre organisme pourrait déjà avoir une politique de sécurité de l’information; si c’est le cas, examinez les exigences de la Politique et des normes de sécurité des DSE pour cerner toute lacune à combler. Par exemple, votre politique de sécurité de l’information actuelle pourrait devoir être modifiée pour inclure la liste des systèmes partagés qu’elle couvre. Si votre organisme n’a pas une telle politique, envisagez d’utiliser le [*modèle de politique de sécurité de l’information*](#_Annexe_D_:)

Vous pourriez aussi avoir à revoir votre formation interne sur la protection de la vie privée et la sécurité. Si votre organisme n’offre pas de formation sur le sujet, envisagez d’utiliser les [*modules de formation sur la protection de la vie privée et la sécurité de ConnexionOntario*](http://www.ehealthontario.on.ca/fr/initiatives/resources/)*,* en entier ou en partie.

Assurez-vous d’assigner officiellement les rôles à des personnes de votre organisme, conformément à la Politique. Vous trouverez la liste des rôles des dépositaires de renseignements sur la santé à la *Figure 2,* et des renseignements supplémentaires au *tableau 2* de l’*Annexe I : Définition des rôles et responsabilités.* Si des modifications à votre organisme affectent la conformité à la Politique et aux normes de sécurité des DSE, elles doivent être communiquées à l’équipe responsable de la protection de la vie privée et de la sécurité du bureau de cyberSanté Ontario[la solution de DSE].

## Norme d’utilisation acceptable des données et des technologies de l’information

La Norme d’utilisation acceptable des données et des technologies de l’information décrit les exigences visant les utilisateurs, qu’il s’agisse de cliniciens, d’autorités locales d’enregistrement, de responsables de la sécurité, etc. Les [*modules de formation sur la protection de la vie privée et la sécurité de ConnexionOntario*](http://www.ehealthontario.on.ca/fr/initiatives/resources/) comprennent les exigences concernant l’utilisation des données. Lorsque les utilisateurs ouvrent leur première session dans [la solution de DSE], et chaque année par la suite, on leur demandera d’accepter la [*Convention d’utilisation du portail de DSE*](https://www.ehealthontario.on.ca/images/uploads/regional_partners/cGTA/EHR_Portal_User_Agreement_Fr.pdf)*,* qui les liera aux engagements de votre organisme. La convention leur demandera de confirmer qu’ils ont suivi la formation et qu’ils s’engagent à respecter les conditions énoncées.

La norme comprend un sous-ensemble d’exigences techniques que votre fournisseur de services de TI peut appliquer (p. ex., configuration des outils d’accès à [la solution de DSE] approuvés par le dépositaire de renseignements sur la santé; chiffrement des disques et des appareils mobiles; utilisation de logiciels antivirus; configuration de mots de passe sur les postes de travail des utilisateurs finaux). Pour en savoir plus, consultez les mesures à appliquer concernant l’utilisation des comptes et le contrôle des mots de passe des utilisateurs présentés au *tableau 1,* ainsi que les contrôles généraux présentés au *tableau 2.*

Tableau 1 – Utilisation du compte et contrôle des mots de passe

| **Utilisation du compte et contrôle des mots de passe** | |
| --- | --- |
| **À faire** | **Exemples / Notes** |
| Les dépositaires de renseignements sur la santé, leurs mandataires et les fournisseurs de services électroniques doivent toujours utiliser les identifiants qui leurs ont été assignés pour ouvrir une session dans [la solution de DSE]. | Inclure les critères suivants :   * Éviter de révéler ou de partager des identifiants. * Tous les utilisateurs sont responsables des actions exécutées sur [la solution de DSE] avec leur nom d’utilisateur. |
| Créer un mot de passe fort et difficile à deviner, et le garder pour soi! | « Ja1meLaP!zza1 » |
| Créer une phrase de passe.  Les mots de passe doivent être composés d’au moins huit caractères, lesquels entrent dans au moins trois des catégories suivantes :   * Chiffre * Lettre majuscule * Lettre minuscule * Caractère spécial | « Ja1meLaP!zza » |
| Mémoriser votre mot de passe, et le noter seulement si vous pouvez le cacher dans un endroit sécuritaire. | Noter seulement le mot de passe, qui doit être gardé sous clé dans un tiroir de votre bureau; ne pas inscrire le nom d’utilisateur sur la feuille. |
| Toujours modifier le mot de passe initial de [la solution de DSE]. | Les utilisateurs qui obtiennent un mot de passe temporaire lors de la création d’un compte ou de la réinitialisation du mot de passe doivent le modifier dès l’ouverture de la session initiale dans le système. |
| **À éviter** | **Exemples / Notes** |
| Créer un mot de passe comprenant une partie de votre nom d’utilisateur, trois caractères identiques consécutifs ou une série prévisible. | * Anniversaires, passe-temps, « AAA », nom d’animal de compagnie * Éviter de remplacer « Ja1meLaP!zza1 » par « Ja1meLaP!zza2 ». |
| Utiliser un mot de passe que vous utilisez pour un autre compte. | Ne pas utiliser le mot de passe de votre compte Hotmail ou Gmail, de votre compte bancaire, etc. |
| Laisser une autre personne utiliser votre identifiant (nom d’utilisateur et mot de passe) pour ouvrir une session dans [la solution de DSE] : ne le partagez pas, car vous êtes responsable des actions exécutées sur [la solution de DSE] avec votre nom d’utilisateur. | |
| Enregistrer votre nom d’utilisateur ou votre mot de passe dans une solution de signature unique, sauf si vous disposez d’un système de gestion approuvé par la norme d’authentification unique**.** | Éviter d’enregistrer votre nom d’utilisateur ou votre mot de passe à l’aide d’une macro-instruction ou d’une touche de fonction; ne pas autoriser votre navigateur à enregistrer votre mot de passe. |

Tableau 2 – Contrôles généraux de la solution de DSE

| **Contrôles généraux de la solution de DSE** | |
| --- | --- |
| **À faire** | **Exemples / Notes** |
| Ouvrir une session dans [la solution de DSE] seulement lorsque vos fonctions l’exigent. | Vous devez seulement utiliser le système dans le cadre de la prestation de soins de santé. Ne pas utiliser le système pour obtenir des renseignements sur des amis, des membres de votre famille, des voisins, des personnes connues, etc., ni sur vous-même. |
| Utiliser seulement les appareils et les processus approuvés par le dépositaire de renseignements sur la santé pour ouvrir une session dans [la solution de DSE]. | Ordinateurs, ordinateurs portables et appareils mobiles que le dépositaire de renseignements sur la santé a examinés et configurés de sorte qu’ils respectent les pratiques de sécurité (p. ex., chiffrement des disques des appareils utilisés à distance, mot de passe fort exigé au démarrage, configuration de l’antivirus, système à jour). |
| Enregistrer seulement le minimum de renseignements personnels sur la santé nécessaire sur les appareils mobiles.  Si des renseignements sur la santé ou des renseignements personnels de [la solution de DSE] sont sauvegardés sur un appareil mobile sans fil, s’assurer que le disque sur lesquels sont sauvegardés les données est chiffré ou que le système de l’utilisateur effectue un chiffrement intégral du disque. | La solution permet aux utilisateurs de télécharger des renseignements personnels sur la santé à partir de leur appareil local. Les utilisateurs pourraient aussi les télécharger sans le savoir. Par exemple, dans certains cas, pour ouvrir un fichier PDF ou une image, certains navigateurs téléchargent une copie sur le disque local. Il faut informer les utilisateurs qu’ils doivent vider régulièrement les dossiers de téléchargement ou temporaires de leur navigateur pour supprimer ces fichiers.  Les dossiers des appareils mobiles où sont enregistrés les renseignements personnels sur la santé doivent être chiffrés ou protégés par un mot de passe. Le chiffrement intégral du disque est la méthode privilégiée. |
| Chiffrer les courriels contenant des renseignements personnels sur la santé, et les envoyer à l’aide d’une solution de transfert de fichiers sécuritaire ou d’un système de courriel sécuritaire approuvés. | Vous pouvez utiliser ONE Mail pour envoyer de manière sécuritaire des renseignements confidentiels au bureau de l’équipe de [la solution de DSE] ou à d’autres utilisateurs de ONE Mail; pour tous les autres systèmes de courriel, les renseignements confidentiels doivent être chiffrés. Microsoft Office permet de chiffrer les documents avec un mot de passe fort; d’autres logiciels, comme WinZip, permettent de protéger les documents envoyés en pièce jointe avec un mot de passe. Assurez-vous de transmettre le mot de passe pour déchiffrer les données par une autre voie de communication (p. ex., au téléphone). |
| Utiliser une solution d’accès à distance approuvée par le dépositaire de renseignements sur la santé pour se connecter à distance à [la solution de DSE] (p. ex., connexion hors du réseau local du dépositaire). | Le dépositaire de renseignements sur la santé doit désigner les appareils à utiliser, comme les appareils dotés d’une fonction de chiffrement des données, de mots de passe forts, d’un logiciel antivirus et d’un système à jour. Il est possible d’utiliser d’autres outils, comme Terminal Services ou Citrix, qui peuvent être configurés pour enregistrer les données dans le système local. Les spécifications techniques fournissent des directives supplémentaires concernant la configuration minimale et recommandée (voir les exigences en matière de configuration du système [[Configuration Requirements for ConnectingOntario](https://www.ehealthontario.ca/portal/server.pt/gateway/PTARGS_32_55520_217_0_-1_47/http%3B/wcicollab.phportal.prod.ont.gss%3B11930/collab/docman/download/259158/0/0/0/CO_Configurations%20Requirements%20.pdf)]). |
| Lors d’un accès à distance, fermer la session plutôt que de simplement fermer l’application. | Fermer la session; ne pas seulement fermer la fenêtre. |
| **À éviter** | **Exemples / Notes** |
| Désactiver, outrepasser ou annuler les mesures de contrôle de la sécurité de l’information. | Par exemple, il ne faut pas désactiver les logiciels antivirus. |
| Interférer avec le fonctionnement normal du système, ou compromettre l’intégrité des données traitées par le système. | |
| Tenter d’exploiter une faille de sécurité réelle ou possible. | |
| Utiliser votre courriel personnel pour envoyer ou recevoir des renseignements personnels sur la santé. | Compte bancaire personnel, compte courriel, compte pour le magasinage (p. ex., comptes Gmail, Hotmail ou BestBuy). |
| Laisser un ordinateur dans un lieu public ou à la vue dans une voiture : il faut plutôt l’apporter avec soi ou le garder sous clé dans le coffre de la voiture. | |
| Communiquer des renseignements personnels sur la santé, sauf aux personnes autorisées dans le cadre de votre travail. | |
| Discuter de renseignements personnels sur la santé dans un lieu public, ou les consulter dans un endroit où d’autres personnes pourraient les voir. | |
| Laisser le compte ouvert et sans surveillance. | Fermez votre session ou verrouillez votre ordinateur lorsque vous devez le laisser sans surveillance. |
| Photographier les données de [la solution de DSE]. | |

## Norme sur la cryptographie

Pour protéger la confidentialité et l’intégrité des renseignements personnels sur la santé de [la solution de DSE], en tant que dépositaire de renseignements sur la santé, vous devez comprendre et utiliser les solutions cryptographiques sur vos systèmes d’information. Cela signifie qu’il vous faut veiller à ce que les données électroniques reçues et envoyées à l’aide de votre système soient chiffrées (verrouillées); ainsi, si les renseignements sont interceptés ou compromis, les données resteront protégées.

Voici quelques outils qui sont souvent dotés d’une fonction de chiffrement :

* **Disque dur des outils approuvés par le dépositaire de renseignements sur la santé –** Chiffrez le disque dur des outils mobiles ou ordinateurs portables approuvés par le dépositaire de renseignements sur la santé que les utilisateurs finaux utiliseront pour accéder à [la solution de DSE]. La solution permet aux utilisateurs finaux de télécharger des renseignements personnels sur la santé sur leur ordinateur; dans certains cas – par exemple, lorsqu’un utilisateur consulte un rapport ou une image –, les renseignements pourraient être téléchargés à son insu. Il est donc important de veiller à ce que le disque soit doté d’un algorithme cryptographique et d’un mot de passe fort, au cas où l’appareil serait volé ou perdu.
* **Courriel –** Utilisez le chiffrement lorsque vous envoyez des données confidentielles au bureau de l'équipe de [la solution de DSE] pour protéger les renseignements sur la vie privée et assurer la sécurité de la correspondance. Vous pouvez le faire en installant la solution ONE Mail, qui chiffre automatiquement les données en transit vers d’autres utilisateurs de ONE Mail, ou en utilisant les fonctions de chiffrement intégrées de Microsoft Office (onglet *Fichier* 🡪 *Informations* 🡪 *Protéger le document*). Assurez-vous que les utilisateurs finaux créent un mot de passe fort pour chiffrer le contenu des documents. N’envoyez pas les mots de passe par courriel; utilisez plutôt d’autres moyens de communication, comme le téléphone.
* **Navigateurs –** Les outils approuvés par le dépositaire de renseignements sur la santé (p. ex., ordinateurs) ouvriront automatiquement une session chiffrée dans [la solution de DSE] lors de la navigation sur son site Web. Il est important que les outils approuvés par le dépositaire de renseignements sur la santé soient dotés d’un système d’exploitation et d’un navigateur Web à jour afin que vous puissiez utiliser les solutions cryptographiques les plus récentes pour offrir la meilleure protection possible aux données en transit entre votre ordinateur et [la solution de DSE].
* **Périphériques réseau –** Les dépositaires de renseignements sur la santé peuvent aussi offrir un réseau sans fil aux utilisateurs. Il est important de le configurer pour pouvoir utiliser un algorithme de chiffrement récent et ainsi s’assurer qu’on ne puisse pas intercepter les données.

Dans [la solution de DSE], utilisez seulement les algorithmes cryptographiques approuvés. La [*Politique de sécurité tout-en-un du DSE à l’intention des organismes ayant seulement des droits de visualisation*](http://www.ehealthontario.on.ca/images/uploads/support/EHR_All_Security_Policy_for_Viewing_Organizations_FR.pdf) présente la liste des algorithmes cryptographiques approuvés.

Les organismes doivent s’assurer d’utiliser un niveau de chiffrement suffisant et de bien gérer les « clés » (mots de passe) utilisées pour déchiffrer l’information.

## Norme sur les fournisseurs de services électroniques

Les organismes peuvent demander à un fournisseur de services électroniques de leur offrir des services liés à l’utilisation de [la solution de DSE], p. ex. :

* Ordinateur local, ordinateur portable, appareils
* Connexion réseau

Les fournisseurs de services électroniques doivent préserver la confidentialité, l’intégrité et la disponibilité des systèmes et des services liés à l’utilisation de [la solution de DSE] par le dépositaire de renseignements sur la santé. Le *tableau 3* présente les responsabilités du dépositaire de renseignements sur la santé par rapport aux fournisseurs de services électroniques.

Tableau 3 – Responsabilités des dépositaires de renseignements sur la santé par rapport aux fournisseurs de services électroniques

| **Responsabilités du dépositaire de renseignements sur la santé** | **Exemples** |
| --- | --- |
| Tenir une liste des contrats de soutien, des ententes et des niveaux de service de tous les fournisseurs de services électroniques. | Décrire et consigner les systèmes et les services d’information offerts par un nouveau fournisseur de services électroniques, ou lors du renouvellement des ententes de services des fournisseurs d’applications, de réseau, d’espace de stockage, etc. |
| Préparer des documents officiels (p. ex., contrats, ententes et niveaux de service). | * Ententes ou contrats qui décrivent les aspects techniques et organisationnels des rôles et des responsabilités des fournisseurs de services électroniques dans le cadre de la relation, conformément à la *LPRPS* et aux politiques et procédures du dépositaire de renseignements sur la santé en matière de protection de la vie privée et de sécurité de l’information. * Rôles et responsabilités que les fournisseurs de services électroniques doivent remplir dans le cadre de l’implémentation, de l’entretien et du soutien des systèmes et des services d’information. * Objectifs des services (p. ex., dates et heures de la prestation des services). * Services attendus (p. ex., réparation). * Consignation des représentants des fournisseurs de services électroniques (p. ex., sous-traitants). |
| Avant de signer un contrat avec un nouveau fournisseur de services électroniques, évaluer les risques potentiels liés à la protection de la vie privée et à la sécurité, et préparer des plans d’atténuation pour minimiser les risques cernés. | |
| Établir une méthode normalisée pour résilier les ententes avec les fournisseurs de service électroniques. | * Désigner des mandataires pour s’occuper de la résiliation de l’entente. * Révoquer les droits d’accès physiques et logiques aux renseignements de l’organisme. * Remettre, transférer ou détruire tous les biens (p. ex., unité de sauvegarde des données, documentation, matériel informatique et appareil d’identification). |
| Avant d’accorder l’accès à [la solution de DSE] à un nouveau fournisseur de services électroniques, exiger qu’il applique les mesures de sécurité et de protection de la vie privée nécessaires. | |

## 

## Norme sur la gestion de l’information et des éléments d’actif

Veillez à ce que les renseignements personnels sur la santé soient transmis au bureau de l’équipe de [la solution de DSE] ou à [la solution de DSE] de manière sécuritaire (p. ex., en utilisant un système de courriel doté d’une fonction de chiffrement ou des outils approuvés par le dépositaire de renseignements sur la santé).

Par exemple, en cas d’incident en lien avec la sécurité ou la protection de la vie privée, vous pourriez avoir à envoyer des renseignements confidentiels au bureau de l’équipe de [la solution de DSE] de manière sécuritaire, en chiffrant les données (voir la [*Politique de sécurité tout-en-un du DSE à l’intention des organismes ayant seulement des droits de visualisation*](http://www.ehealthontario.on.ca/images/uploads/support/EHR_All_Security_Policy_for_Viewing_Organizations_FR.pdf)ONE Mail est un service adéquat pour envoyer des renseignements personnels sur la santé par courriel, car il permet de chiffrer automatiquement les données en transit vers les autres utilisateurs de ONE Mail.

Si votre organisme n’utilise pas ONE Mail, vous pouvez l’obtenir en communiquant avec le service de dépannage de cyberSanté Ontario, ou vous pouvez chiffrer les données en créant un mot de passe fort dans un document de Microsoft Office (onglet *Fichier 🡪 Informations 🡪 Protéger le document*) ou en utilisant l’outil d’un tiers. Veillez à ce que le mot de passe soit communiqué hors bande (p. ex., par téléphone). Voir les exigences de la section *Politique d’utilisation acceptable des données et des technologies de l’information* de la [*Politique de sécurité tout-en-un du DSE à l’intention des organismes ayant seulement des droits de visualisation*](http://www.ehealthontario.on.ca/images/uploads/support/EHR_All_Security_Policy_for_Viewing_Organizations_FR.pdf).

## Norme sur la gestion des incidents de sécurité de l’information

### Qu’est-ce qu’un incident?

Un incident est une violation ou une menace imminente de violation des politiques de sécurité de l'information, des normes, des procédures ou des pratiques, ou de n'importe quel événement de sécurité de l'information qui pourrait compromettre les opérations ou menacer la sécurité d'un système d'information ou le processus d'affaires.

Des exemples peuvent comprendre:

* La divulgation non autorisée, la destruction, la modification ou la retenue de l'information
* L’inobservation de respecter les exigences de sécurité de l'organisation
* L'accès non autorisé, l'utilisation, ou l'enquête malveillante des ressources d'information
* Un compromis de sécurité tenté, présumé ou actuel
* Le gaspillage, la fraude, l'abus, le vol, la perte ou la détérioration des ressources informatiques

### Le traitement d’un incident

Les organisations doivent mettre en œuvre un processus de gestion des incidents de sécurité de l'information qui:

* Identifie et résout les incidents rapidement et efficacement
* Minimise l'impact des incidents
* Réduit le risque d'incidents semblables

Ces phases sont décrites dans la politique sur la gestion des incidents de sécurité de l’information comme :

1. l'identification / le triage
2. la réaction
3. la récupération
4. le suivi

**Remarque:** Les politiques de confidentialité de DSE demandent également des sites à mettre en œuvre une politique de gestion de la violation de la vie privée. Dans les cas où il y a une violation de l'information personnelle sur la santé, le processus de gestion de la violation de la vie privée a la priorité et doit être suivi.

### Rôles et Responsabilités

**Point de contact** - un individu ou une équipe à laquelle les incidents réels ou présumés sont signalés. Cela peut être votre bureau local de service, un chef de bureau, ou une autre personne désignée par votre organisation. Le point de contact peut également être le chef de réponse aux incidents.

**Chef/équipe des réponses aux incidents –** initie le triage, la réponse, la récupération, et les activités de suivi des incidents. Le chef ou l'équipe de réponse aux incidents peut être le même que le point de contact. L'équipe d'intervention peut inclure le fournisseur de services informatiques ou un fournisseur de services électroniques qui est chargé de fonctions de gestion des incidents.

**Le bureau du programme de protection des renseignements personnels et de l'équipe des opérations de sécurité de [la solution de DSE] –** la protection des renseignements personnels et de l'équipe de sécurité qui se compose généralement des agents de [la solution de DES] qui appuient les fonctions d'incidents de sécurité afin de coordonner les activités et les notifications entre les dépositaires des renseignements personnels et d'autres parties prenantes.

### Les quatre phases de la gestion des incidents de sécurité de l’information

#### Détection/triage

|  |
| --- |
| * Signaler immédiatement tout incident en lien avec la sécurité présumé ou confirmé au point de contact de votre établissement (p. ex., service de dépannage ou responsable de la protection de la vie privée/de la sécurité). Le point de contact peut être votre gestionnaire ou votre superviseur, qui devra signaler l’incident au point de contact initial en cas d’incident en lien avec la sécurité de l’information.   **Point de contact :**   * En cas d’incident, créer un billet d’incident ou le consigner dans un registre qui devra comprendre au minimum : * l’heure et la date de l’incident signalé; * le nom et les coordonnées du mandataire ou du fournisseur de services électroniques qui a signalé l’incident; * les renseignements sur l’incident (p. ex., type, façon dont il a été constaté); * les répercussions et les mesures appliquées pour contenir l’incident. * Envoyer les billets d’incident au responsable en cas d’incident pour qu’il vérifie si un incident a bel et bien eu lieu. |
| **Équipe d’intervention ou responsable en cas d’incident :**   * Classer les incidents selon leur gravité et leur accorder un degré de priorité. * Commencer à préparer un rapport d’incident lié au programme de [la solution de DSE] ou à [la solution de DSE]. * Aviser l’équipe responsable de la protection de la vie privée et de la sécurité du bureau de [la solution de DSE] et tout dépositaire de renseignements sur la santé touché d’ici le jour ouvrable suivant la confirmation des incidents de gravité 1 ou 2. Inclure les renseignements minimaux de signalement. * Si un incident touche plus d’un dépositaire de renseignements sur la santé ou [la solution de DSE], l’équipe responsable de la protection de la vie privée et de la sécurité du bureau de [la solution de DSE] peut diriger les activités de gestion de l’incident et le signaler aux autres dépositaires de renseignements sur la santé. * L’équipe responsable de la protection de la vie privée et de la sécurité du bureau de [la solution de DSE] avisera le Comité ConnexionSécurité et/ou l’organisme de surveillance compétent dans les **72 heures** suivant le signalement de l’incident. |

#### Intervention

|  |
| --- |
| **Équipe d’intervention ou responsable en cas d’incident :**   * Essayer de limiter la portée et l’ampleur de l’incident. Voici quelques mesures d’atténuation : * Copie de sauvegarde du système d’information * Interruption des activités * Modification des mots de passe ou des listes de contrôle d’accès du système d’information compromis * Restriction de la connexion * Selon la gravité de l’incident, il pourrait être nécessaire de mettre en œuvre le plan de continuité des activités de l’organisme. |

#### Rétablissement

|  |
| --- |
| **Équipe d’intervention ou responsable en cas d’incident :**   * Rétablir les systèmes d’information touchés afin qu’ils redeviennent entièrement fonctionnels. Voici quelques mesures de rétablissement : * Élimination de la cause de l’incident (p. ex., suppression du maliciel) * Restauration du système d’information et validation de son état * Détermination du moment de la reprise des activités * Surveillance des systèmes d’information pour voir s’ils fonctionnent bien et confirmer qu’il n’y a plus de données ou de systèmes compromis |

#### Suivi

|  |
| --- |
| **Équipe d’intervention ou responsable en cas d’incident :**   * Mener une enquête sur les incidents pour en déterminer la cause (p. ex., effectuer une analyse des causes profondes). * Une fois l’incident résolu (lorsque toutes les activités de rétablissement ont été mises en œuvre et que les technologies de l’information et les systèmes d’information touchés sont revenus à leur état normal), l’équipe d’intervention ou responsable en cas d’incident doit rédiger le rapport d’incident. On pourrait demander ou exiger des rapports d’état réguliers, selon la durée de l’enquête. * Archiver les rapports d’incident pendant au moins 24 mois. * Fournir un rapport d’incident au bureau de l'équipe de [la solution de DSE] et à tout autre dépositaire de renseignements sur la santé touché dans les 72 heures suivant la réception de la demande de rapport d’incident. * Envoyer les versions définitives des rapports à l’équipe responsable de la protection de la vie privée et de la sécurité du bureau de [la solution de DSE] afin qu’ils soient présentés au Comité ConnexionSécurité et, au besoin, à l’organisme de surveillance compétent. * Appliquer les mécanismes d’examen des incidents en lien avec la sécurité se produisant dans votre organisme au moins une fois par mois afin de dégager les tendances et chercher à savoir s’il est possible de prendre des mesures de prévention pour réduire les risques d’incidents similaires à l’avenir. |

#### Collecte de preuves

|  |
| --- |
| **Équipe d’intervention ou responsable en cas d’incident :**   * Élaborer des procédures de collecte de preuves pour pouvoir imposer des mesures disciplinaires aux mandataires ou aux fournisseurs de services électroniques ou les poursuivre en justice. |

1. Un modèle de gestion des incidents de sécurité est mis à votre disposition pour vous aider à consigner les renseignements nécessaires en cas d’incident en lien avec la sécurité. Il peut servir de rapport final afin de répondre aux exigences de la politique. Consultez l’*Annexe F : Diagrammes d’incident*, qui comprend deux processus de gestion des incidents, avec ou sans autres dépositaires de renseignements sur la santé.

## Norme sur les fournisseurs d’identités et Manuel de procédures relatives à l’admissibilité

Cette norme et le manuel associé servent à veiller à ce que les procédures d’inscription des utilisateurs et des mandataires qui peuvent utiliser [la solution de DSE] soient adéquates et sécuritaires. Quatre intervenants sont visés :

1. Autorité d’enregistrement
2. Personne légalement responsable
3. Autorité locale d’enregistrement
4. Approbateur

### Autorité d’enregistrement

Entité supérieure généralement responsable d’un réseau d’organismes qui se charge de l’inscription et qui offre une fonction de gestion de l’identité. L’entité doit collaborer avec la personne légalement responsable des dépositaires de renseignements sur la santé pour inscrire les autorités locales d’enregistrement. [la solution de DSE] ou son délégué agit à titre d’autorité d’enregistrement auprès des dépositaires de renseignements sur la santé dont les mandataires et les fournisseurs de services électroniques recevront un accès à [la solution de DSE] par des processus de contrôle de l’accès, des procédures, des politiques et des systèmes de gestion de l’identité (p. ex., le programme ONE ID agit à titre d’autorité d’enregistrement pour les utilisateurs d’ONE ID).

### Personne légalement responsable

La personne légalement responsable est souvent un administrateur général de l’organisme, p. ex. le directeur de l’information. Cette personne est légalement responsable du processus d’inscription pour son dépositaire de renseignements sur la santé. Elle a pour rôle d’autoriser les approbateurs et les autorités locales d’enregistrement à s’occuper du processus d’inscription au nom du dépositaire de renseignements sur la santé. La personne légalement responsable signe les ententes légales au nom d’un organisme. Si votre organisme utilisera ONE ID pour se connecter à [la solution de DSE], votre personne légalement responsable peut déléguer ses responsabilités à une autre personne en soumettant un formulaire de délégation de personne légalement responsable (dans la trousse d’implémentation de [ONE ID)](https://www.ehealthontario.ca/portal/server.pt/gateway/PTARGS_0_95092_17880_717_89964_43/docman/download/205100/0/0/0/ONE%20ID%20Implementation%20Package.pdf) à cyberSanté Ontario.

La personne légalement responsable est le seul intervenant du dépositaire de renseignements sur la santé qui a le pouvoir de modifier le statut d’une autorité locale d’enregistrement, sauf si votre organisme utilise ONE ID : dans ce cas, l’équipe d’ONE ID de cyberSanté Ontario, à titre d’autorité d’enregistrement, peut révoquer le statut d’autorité locale d’enregistrement.

La personne légalement responsable désigne au moins une personne comme autorité locale d’enregistrement qui gérera l’inscription de ses mandataires et fournisseurs de services électroniques devant accéder à [la solution de DSE]. La personne légalement responsable désigne au moins une personne, un groupe ou un intervenant comme approbateur qui approuvera l’accès des mandataires à [la solution de DSE].

### Autorité locale d’enregistrement

L’autorité locale d’enregistrement gère l’enregistrement des utilisateurs, c’est-à-dire qu’elle s’assure qu’ils sont bien enregistrés et qu’ils font preuve de la diligence nécessaire avant de recevoir un accès (p. ex., formation, approbation par un approbateur valide, preuve d’identité).

Les autorités locales d’enregistrement doivent suive la formation à leur intention et être enregistrées conformément aux exigences du niveau d’assurance 2 de la politique. Les autorités locales d’enregistrement de ONE ID ont été enregistrées conformément aux exigences du niveau d’assurance 2.

Dans le cas des utilisateurs de ONE ID, la personne légalement responsable (ou son délégué) doit soumettre la candidature de l’autorité locale d’enregistrement à cyberSanté Ontario. Consultez le formulaire de nomination de l’autorité locale d’enregistrement (dans la trousse explicative de [ONE ID)](https://www.ehealthontario.ca/portal/server.pt/gateway/PTARGS_0_95092_17880_717_89964_43/docman/download/205100/0/0/0/ONE%20ID%20Implementation%20Package.pdf).

Lorsque l’autorité locale d’enregistrement accorde un accès, elle doit valider l’identité de l’utilisateur. Elle peut utiliser les anciens dossiers des ressources humaines pour éliminer le besoin d’une validation en personne; cependant, ces dossiers doivent comprendre la validation originale de l’identité.

### Approbateur

#### Accès clinique

Aux termes de la Norme sur les fournisseurs d’identités et du Manuel de procédures relatives à l’admissibilité, l’approbateur a le pouvoir d’autoriser l’accès à la solution. L’approbateur ne doit accorder accès aux composantes cliniques qu’aux utilisateurs qui ont pour but de recueillir des renseignements personnels sur la santé (RPS) pour prodiguer ou contribuer à prodiguer des soins de santé. Voici une liste non exhaustive des utilisateurs finaux susceptibles de satisfaire au critère selon lequel la personne doit dispenser des soins de santé ou aider à le faire :

* les professionnels de la santé reconnus qui voient des patients
* Résidents qui prodiguent des soins aux patients
* Personnel administratif qui sort les dossiers pour les médecins
* les commis d’unité qui examinent les résultats pour déceler le trouble du patient pour les médecins

#### Accès administratif

L’approbateur doit seulement accorder l’accès aux composants administratifs de [la solution de DSE] aux utilisateurs et aux fournisseurs de services électroniques qui offrent du soutien pour une fonction prévue pour les titulaires de postes d’administrateurs pour [la solution de DSE] (p. ex., responsables de la protection de la vie privée et administrateurs de systèmes).

#### Réinscription

Les utilisateurs dont l’accès a été révoqué doivent se réinscrire au service pour y avoir accès. L’identité des utilisateurs doit être validée, et ils doivent obtenir l’approbation de l’approbateur pour avoir de nouveau accès à la solution; le compte doit être mis à jour. Pour obtenir la description des processus de révocation, de suspension ou de rétablissement d’une inscription à un service, les organismes qui utilisent ONE ID doivent consulter la *Section 7 – Soutien et maintenance pour les personnes inscrites* du *Manuel des procédures des autorités d’enregistrement locales*.

#### Interdiction de l’accès à des fins de recherche

Les approbateurs ne doivent pas accorder l’accès à [la solution de DSE] si l’accès a été demandé pour une raison autre que celle de prodiguer ou de contribuer à prodiguer des soins de santé. Autrement dit, les motifs suivants ne sont pas acceptables :

* planification, évaluation ou surveillance de programmes;
* gestion de risques ou d’erreurs;
* amélioration de la qualité des soins, des programmes et des services;
* formation (à moins que la personne soit étudiante ou résidente et doit y avoir accès pour prodiguer des soins);
* traitement des paiements;
* recherche.

#### Enregistrement d’utilisateurs occupant plusieurs rôles

Si un mandataire ou un fournisseur de services électroniques a plus d’une fonction (clinicien et gestionnaire des risques, par exemple), l’approbateur peut lui donner accès à la [solution de DSE] pour qu’elle recueille des renseignements personnels sur la santé et puisse ainsi prodiguer ou contribuer à prodiguer des soins de santé et doit veiller à ce que l’utilisateur final soit au courant de ses autorisations et obligations..

Suivez les procédures spécifiques établies par le programme d’enregistrement et d’inscription de ONE ID.

Veuillez noter que les ententes d’échange de données avec les dépositaires de renseignements sur la santé précisent que l’accès peut seulement être accordé à des fins précises.

## Norme sur les réseaux et les opérations

Cette norme traite de la façon dont l’information est consultée et transmise entre les appareils et dans le réseau. Vous devez mettre en place des mesures de contrôle pour sécuriser votre infrastructure réseau et établir des procédures pour sécuriser la gestion et le fonctionnement continus des services d’identification et des terminaux d’envoi des données. Pour obtenir de plus amples renseignements et de l’assistance, vous pouvez communiquer avec votre fournisseur de services électroniques, au besoin.

### Zones réseau

L’accès aux renseignements personnels sur la santé s’accompagne de la responsabilité d’empêcher les utilisateurs non autorisés d’y avoir accès. Les périphériques réseau (p. ex., pare-feu, routeurs et commutateurs) doivent être installés de façon à séparer votre réseau interne des réseaux non sécuritaires. Il s’agit de l’établissement de zones réseau qui divisent les différents milieux informatiques de manière sécuritaire. La division des réseaux peut, entre autres, s’appuyer sur les critères suivants :

* la classification de l’information transmise sur le réseau;
* le niveau d’assurance requis.

Une façon de protéger votre zone réseau est d’offrir un réseau pour les invités (p. ex., réseau sans fil gratuit) aux patients et aux visiteurs. Ce réseau devrait être séparé du réseau de votre établissement afin d’empêcher les personnes non autorisées d’accéder aux données.

D’autres mesures de séparations pourraient être nécessaires, par exemple, si un sous-traitant utilise le réseau de votre établissement. Dans ce cas, les réseaux devraient être séparés pour veiller à ce que [la solution de DSE] soit utilisée dans un environnement sécuritaire.

### Passerelles de sécurité

Le trafic entre les différentes zones du réseau (réseau interne et réseau pour les invités) doit être séparé par une passerelle de sécurité, généralement, un pare-feu doté des règles configurées pour protéger le réseau. Habituellement, il faut déployer un pare-feu configuré pour protéger les ordinateurs internes des menaces.

Examinez la configuration des passerelles de sécurité de votre organisme au moins une fois par année. Ce processus devrait garantir que :

* les règles visant le réseau (autorisation et refus) sont légitimes;
* les règles superflues, désuètes ou contradictoires sont analysées et corrigées;
* les appareils du réseau superflus ou désuets (p. ex., ordinateurs) sont retirés.

Pour en savoir plus, consultez les [exigences en matière de configuration du système](https://www.ehealthontario.ca/portal/server.pt/gateway/PTARGS_32_55520_217_0_-1_47/http%3B/wcicollab.phportal.prod.ont.gss%3B11930/collab/docman/download/259158/0/0/0/CO_Configurations%20Requirements%20.pdf).

### Protection contre les programmes malveillants

Des logiciels de détection des programmes malveillants et de réparation (p. ex., logiciels antivirus), ou des solutions équivalentes :

* devraient être installées pour les outils, les processus et les postes de travail approuvés par le dépositaire de renseignements sur la santé utilisés pour accéder à [la solution de DSE] pour protéger les renseignements personnels sur la santé contre les programmes malveillants qui pourraient compromettre les données.
* Il faut garder les antivirus à jour pour détecter les maliciels qui pourraient compromettre le réseau et les renseignements personnels sur la santé. Souvent, ces logiciels peuvent être configurés pour vérifier automatiquement si des mises à jour sont disponibles, et pour analyser les outils approuvés par le dépositaire de renseignements sur la santé.
* Les autres solutions de protection contre les programmes malveillants comprennent l’élaboration d’une liste blanche d’applications ou l’utilisation de la version légère d’un client pour restreindre les fonctions accessibles en écriture. Elles pourraient interdire l’accès à des sites inconnus ou qui comprennent ou pourraient comprendre des applications ou des programmes malveillants.

## Norme sur la gestion des menaces et des risques

L’évaluation de la menace et des risques est une bonne façon de comprendre les risques et les menaces pour la sécurité du système d’information de votre organisme et des renseignements personnels sur la santé traités. Vous pouvez utiliser l’évaluation de la menace et des risques pour déterminer le degré de protection nécessaire d’après les possibilités qu’un incident se produise, et les répercussions qu’il pourrait avoir.

L’équipe responsable de la protection de la vie privée et de la sécurité du bureau de [la solution de DSE] effectuera les évaluations de la menace et des risques dans [la solution de DSE], et peut fournir les résultats de ces évaluations et les plans de remédiation sur demande.

Pour demander une évaluation de la menace et des risques des solutions de cyberSanté Ontario, écrivez à the[security@ehealthontario.on.ca](mailto:security@ehealthontario.on.ca).

### Protection des documents sur l’évaluation de la menace et des risques reçus

Lorsque vous recevez une évaluation de la menace et des risques de l’équipe responsable de la protection de la vie privée et de la sécurité du bureau de [la solution de DSE], vous devez restreindre l’accès à l’évaluation et aux documents à l’appui, et veiller à ce que l’évaluation soit traitée de manière sécuritaire, comme tout autre renseignement confidentiel de votre organisme.

Voici des exemples de façons de protéger une évaluation de la menace et des risques :

* Si elle est enregistrée sur un appareil mobile (p. ex., ordinateur portable, iPad, tablette ou téléphone cellulaire) ou un appareil de stockage mobile (p. ex., clé USB), veillez à ce que ces appareils soient chiffrés.
* Si l’évaluation de la menace et des risques est enregistrée sur votre réseau interne, l’accès doit être réservé aux personnes qui en ont besoin (p. ex., responsable de la protection de la vie privée/de la sécurité et personne légalement responsable).
* N’enregistrez pas l’évaluation de la menace et des risques sur un site d’hébergement de fichiers externe, comme Google Drive ou Dropbox.
* Veillez à ce que les copies papier soient rangées dans une armoire ou un tiroir lorsqu’elles ne sont pas utilisées ou lorsqu’elles sont laissées sans surveillance.
* Lorsque vous n’avez plus besoin des copies papier, assurez-vous de vous en départir de manière sécuritaire (p. ex., utiliser une déchiqueteuse, ou les déposer dans un contenant de documents qui seront déchiquetés par un fournisseur autorisé).

# Annexe A : Index des ressources

| **Séq.** | **Type** | **Document(s)** | **Commentaires** |
| --- | --- | --- | --- |
| **Partie A** | | | |
| 1. | Guide de sécurité (le présent document) | Guide de sécurité des DSE à l’intention des [organismes](http://www.ehealthontario.on.ca/images/uploads/support/EHR_Security_Reference_Guide_for_Viewing_Organizations_FR.docx) ayant seulement des droits de visualisation qui ont un compte ONE ID ou ClinicalConnect | Principale référence fournie lors du webinaire de formation.   * Élaboration de votre programme de sécurité de l’information. * Étapes du processus de déploiement * Rôles, responsabilités et principaux termes * Politique et normes de sécurité des DSE |
| 2. | Webinaire | [Webinaire sur l’utilisation sécuritaire des DSE à l’intention des organismes qui utilisent ONE ID ou ClinicalConnect pour accéder à la solution](https://www.ehealthontario.on.ca/images/uploads/support/EHR-security-webinar-for-viewing-organizations/story.html) | Introduction à la sécurité et aperçu pour les organismes ayant seulement des droits de visualisation qui utilisent [la solution de DSE]. Le webinaire comprend :   * un aperçu de la structure de gouvernance de la protection de la vie privée et de la sécurité; * un aperçu de la politique sur la sécurité des DSE comprenant :   1. des conseils sur la préparation;   2. les étapes de l’évaluation; * les principaux diagrammes de processus; |
| 3. | Politique et normes | [Politique tout-en-un sur la sécurité des DSE à l’intention des organismes ayant seulement des droits de visualisation qui ont un compte ONE ID ou ClinicalConnect](http://www.ehealthontario.on.ca/images/uploads/support/EHR_All_Security_Policy_for_Viewing_Organizations_FR.pdf) | Document tout-en-un conçu pour les organismes ayant des droits de visualisation qui comprend un résumé de toutes les politiques qui s’appliquent. |
| 4. | Modèles à l’appui | 1. Modèle de politique de sécurité de l’information 2. Modèle de gestion des incidents | 1. Document destiné aux dépositaires de renseignements sur la santé lorsque l’organisme ne possède pas de politique de sécurité de l’information. Il peut être servir de politique de sécurité avec un minimum d'efforts. Ce document est conforme à la Politique et aux normes de sécurité des DSE. 2. Document destiné aux dépositaires de renseignements sur la santé dans lequel ils consignent les incidents de sécurité de l’information. Il comprend des champs qui servent à noter les renseignements exigés en vertu de la Politique sur la gestion des incidents de sécurité de l’information. |
| 5. | Autre | [Exigences en matière de configuration du système](https://www.ehealthontario.ca/portal/server.pt/gateway/PTARGS_32_55520_217_0_-1_47/http%3B/wcicollab.phportal.prod.ont.gss%3B11930/collab/docman/download/259158/0/0/0/CO_Configurations%20Requirements%20.pdf) | Listes des configurations locales minimales et recommandées de ConnexionOntario. |

| **Séq.** | **Type** | **Document(s)** | **Commentaires** |
| --- | --- | --- | --- |
| **Partie B** | | | |
| 5.a | Module d’apprentissage électronique | [Formation sur la protection de la vie privée et la sécurité de ConnexionOntario pour le personnel de soutien technique](https://www.ehealthontario.on.ca/images/uploads/initiatives/resources/ConnectingOntario_Technical_Support_Privacy_and_Security_Training/story.html) | Formations sur le soutien technique (testeurs, administrateurs, services de dépannage, etc.) |
| 5.b | Module d’apprentissage électronique | [Privacy and Security Training for Clinical End Users of Ontario’s Electronic Health Record](file:///C:/Users/mark.carter/Documents/InfoSec/Connecting%20Ontario/Task%20Force/Plain%20Language/ges/uploads/initiatives/resources/Privacy_and_Security_Training_for_Clinical_End_Users_of_Ontario_EHR/story.html) | Formation destinée aux utilisateurs finaux (les personnes qui utilisent la solution) |
| 5.c | Document de référence | Privacy & Security Training for Local Registration Authorities (LRAs) | Formation indépendante pour les autorités locales d’enregistrement |
| 5.d | Document de référence | [Formation de ONE ID pour les autorités locales d’enregistrement](http://www.ehealthontario.on.ca/fr/support-topics/one-id-lra/overview/) | Formation offerte par l’équipe de ONE ID qui donne un aperçu des processus particuliers de ONE ID |
| 5.e | Webinaire | [Formation sur la protection de la vie privée et la sécurité pour les responsables de la protection de la vie privée et de la sécurité](http://www.ehealthontario.on.ca/images/uploads/initiatives/resources/Privacy_and_Security_Training_for_Clinical_End_Users_of_Ontario_EHR/story.html) | Formation offerte en personne ou sur WebEx qui présente les responsabilités des responsables de la protection de la vie privée et de la sécurité qui utilisent [la solution de DSE] |

| **Séq.** | **Type** | **Document(s)** | **Commentaires** |
| --- | --- | --- | --- |
| **Partie C** | | | |
| 6 | Évaluation | [Évaluation de sécurité des DSE pour les organismes qui utilisent ONE ID ou ClinicalConnect](http://www.ehealthontario.on.ca/images/uploads/support/EHR_Security_Assessment_for_Viewing_Organizations_FR.docx) | Outil d’évaluation de la sécurité utilisé pour déterminer si un organisme respecte la Politique et les normes de sécurité des DSE. L’évaluation est présentée à cyberSanté Ontario dans le cadre du processus d’enregistrement. |

# Annexe B : MODÈLE d’entente de confidentialité

Entente de confidentialité

Dans le cadre de mes fonctions dans cet établissement, je reconnais l’importance de protéger la confidentialité et l’intégrité des renseignements personnels ou des renseignements personnels sur la santé auxquels j’ai accès. Je m’engage à ne pas les recueillir, les utiliser ou les communiquer à une autre personne ou à un autre organisme, sauf dans le cadre de la prestation de mes services.

De plus, je, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ :

1. reconnais que j’ai reçu, lu et compris la politique de sécurité de l’établissement;
2. reconnais que j’ai reçu, lu et compris le guide de référence rapide sur la sécurité, ainsi que la déclaration des responsabilités qui m’incombent en matière de protection de la confidentialité des renseignements;
3. accepte que la politique de l’établissement et les instructions connexes fassent partie de mes conditions d’emploi ou de mon contrat, et que toute violation de la présente entente puisse entraîner des mesures disciplinaires pouvant aller jusqu’au congédiement ou à la résiliation de mon contrat;
4. accepte de signaler toute violation de la politique de sécurité de l’établissement ou des directives connexes dont je suis témoin à la personne responsable de la sécurité, notamment la collecte, l’utilisation, la divulgation ou l’élimination non autorisées de renseignements personnels sur la santé en vertu de la politique de sécurité de l’établissement, et de ses modifications.

# Annexe C : MODÈLE de rapport d’incident lié à la sécurité



# Annexe D : MODÈLE de politique de sécurité pour les organismes ayant seulement des droits de visualisation



# Annexe E : MODÈLE de liste de fournisseurs de services électroniques

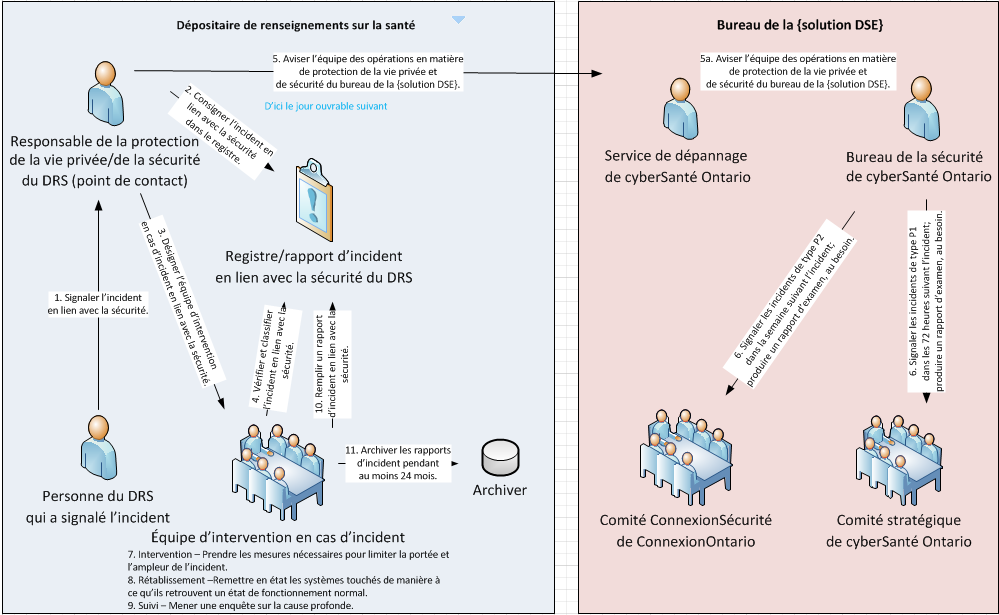


# 

# Annexe F : Diagrammes d’incident

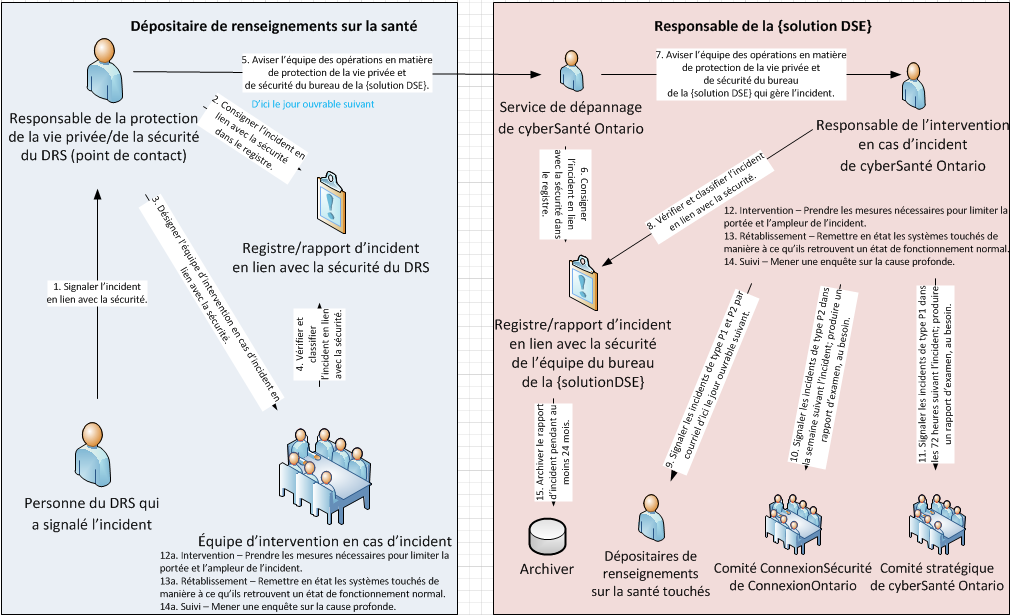
Voici deux diagrammes d’incident typiques : 1) les incidents gérés par le dépositaire de renseignements sur la santé, qui sont isolés et n’affectent pas les autres dépositaires de renseignements sur la santé, comme montré dans la figure 5; et 2) les incidents gérés par le bureau de l’équipe de [la solution de DSE], qui affectent les autres dépositaires de renseignements sur la santé, comme montré dans la figure 6.

**1. Incident géré par le dépositaire de renseignements sur la santé**



**Figure 5 – Incident géré par le dépositaire de renseignements sur la santé**

**2. Incident géré par l’équipe responsable de la protection de la vie privée et de la sécurité de [la solution de DSE]**



**Figure 6 – Incident géré par l’équipe du bureau de [la solution de DSE]**

1. Si, à tout moment au cours du processus de gestion de l’incident, le dépositaire de renseignements sur la santé constate que l’incident a entraîné une atteinte à la confidentialité, l’incident doit être traité conformément à la *Politique de gestion des atteintes à la confidentialité* qui fait partie de la [***Politique de confidentialité des DSE***](http://www.ehealthontario.on.ca/images/uploads/support/EHR_Privacy_Policies_FR.pdf).

# Annexe G : Définition des rôles et responsabilités

**Tableau 1 – Rôles et responsabilités des dépositaires de renseignements sur la santé relatifs à [la solution de DSE]**

| Rôles des dépositaires de renseignements sur la santé | Définitions et responsabilités |
| --- | --- |
| Approbateur | Toute personne qui a le pouvoir d’accorder un accès à [la solution de DSE] aux mandataires et aux fournisseurs de services électroniques. Habituellement, les personnes légalement responsables autorisent des gestionnaires, par exemple, à être approbateurs; cette tâche peut aussi être déléguée à l’autorité locale d’enregistrement.  **Responsabilités**   * Approuver l’accès à [la solution de DSE] des intervenants qui remplissent les critères énoncés dans les ententes. |
| Autorité locale d’enregistrement | Personne autorisée par la personne légalement responsable d’un dépositaire de renseignements sur la santé à gérer le processus d’inscription et d’enregistrement des mandataires et des fournisseurs de services électroniques du dépositaire de renseignements sur la santé et à leur accorder l’accès à [la solution de DSE] en appliquant les processus, les procédures et les politiques de contrôle de l’accès et en utilisant le système de gestion de l’identité. Les autorités locales d’enregistrement sont enregistrées par l’équipe de [la solution de DSE] ou leurs représentants, et inscrivent et enregistrent les mandataires et les fournisseurs de services électroniques au nom de l’équipe de [la solution de DSE].  **Responsabilités**   * Inscrire et enregistrer les mandataires et les fournisseurs de services électroniques d’un dépositaire de renseignements sur la santé. * Vérifier l’identité des mandataires et des fournisseurs de services électroniques qui demandent un accès. |
| Dépositaire de renseignements sur la santé | Habituellement, professionnel de la santé qui a la garde ou le contrôle de renseignements personnels sur la santé par suite ou à l’égard de l’exercice de ses pouvoirs ou de ses fonctions.  **Responsabilités**   * Protéger les renseignements personnels sur la santé en veillant à ce qu’ils soient : * exacts et à jour pour les fins auxquelles ils sont utilisés; * protégés contre le vol, la perte, l’utilisation non autorisée ou la divulgation; * protégés contre la copie, la modification et l’élimination non autorisées; * conservés, transmis et supprimés de manière sécuritaire. * En cas de vol ou de perte des renseignements personnels sur la santé, ou si une personne non autorisée y a accès, aviser les patients concernés dès que possible. * Veiller à ce que les mandataires et les fournisseurs de services électroniques qui ont accès à [la solution de DSE] signent un accord d’utilisateur final qui comprend des dispositions sur la confidentialité et la responsabilité. * Élaborer, mettre en œuvre et tenir à jour une politique de sécurité de l’information qui établit les exigences, attribue les responsabilités et démontre l’engagement de l’organisme en matière de protection des renseignements personnels sur la santé. * Désigner un responsable de la sécurité de l’information qui veillera à ce que le personnel, les mandataires et les fournisseurs de services électroniques qui ont accès aux services de [la solution de DSE] soient conformes. |
| Fournisseur de services électroniques/  fournisseur de services de TI/ administrateur de système de TI | Personne ou organisme qui fournit des biens et des services permettant à un dépositaire de renseignements sur la santé de recueillir, d’utiliser, de modifier, de divulguer, de conserver ou d’éliminer des renseignements personnels sur la santé, notamment le fournisseur d’un réseau d’information sur la santé. Il peut s’agir de votre administrateur de système de TI ou d’un tiers qui offre du soutien technique.  Par exemple, une personne ou une entreprise qui offre des services de TI à un cabinet de médecin, comme l’installation et l’entretien des ordinateurs, l’installation de nouveaux logiciels et des services de connectivité au réseau.  **Responsabilités**   * Aider le dépositaire de renseignements sur la santé à se conformer aux exigences de la *LPRPS* et de la politique de sécurité des DSE. * Signer une entente de confidentialité avec l’établissement avant d’accéder aux renseignements confidentiels, le cas échéant. * Avant de commencer le travail, lire la Politique et les normes de sécurité des DSE et signer l’*Annexe B : MODÈLE d'entente de confidentialité,* si elle est utilisée. * Placer les ordinateurs dans un lieu sûr pour réduire les risques de modification, de perte, d’accès, de vol, de consultation ou de divulgation par une personne non autorisée. * Veiller à ce que chaque utilisateur ait un nom d’utilisateur unique et choisisse son propre mot de passe. * Indiquer aux membres du personnel d’utiliser un mot de passe fort, qui compte au moins huit caractères et comprend une combinaison de lettres majuscules et minuscules, de chiffres et de caractères spéciaux. * Mettre en place des dispositifs de sécurité, comme des mots de passe et le verrouillage de l’écran de veille. * Installer des solutions cryptographiques et gérer la cryptographie des disques durs, le cas échéant. Consulter la feuille-info [*Le chiffrement fort dans les soins de santé*](https://www.ipc.on.ca/french/resources/educational-material/educational-material-summary/default.aspx?id=969) du CIPVP. * Installer des logiciels de sécurité, comme un logiciel antivirus, un filtre anti-pourriel, un anti-logiciel espion ou un pare-feu personnel d’un fournisseur reconnu, et les garder à jour. * Apporter des correctifs de sécurité et faire des mises à jour régulièrement. * Connecter les ordinateurs à un système d’alimentation sans coupure (ASC), au besoin. * Veiller à ce que le responsable de la sécurité de tout l’établissement comprenne les dispositifs de sécurité installés et connaisse les mesures à appliquer en cas d’incident. |
| Mandataire (utilisateur final) | Personne qui, avec l’autorisation du dépositaire de renseignements sur la santé, agit au nom du dépositaire en ce qui concerne les renseignements personnels sur la santé. Par exemple, un mandataire peut être un employé ou un entrepreneur qui effectue les tâches d’une autorité locale d’enregistrement, ou un médecin qui s’occupe des patients au nom du dépositaire de renseignements sur la santé.  **Responsabilités**   * Lire et respecter les politiques et les procédures sur la protection des renseignements confidentiels établies par le dépositaire de renseignements sur la santé. * Lire, signer et respecter les conditions de l’*Annexe B : MODÈLE d'entente de confidentialité,* si votre organisme l’utilise. * Suivre les pratiques en matière de rangement du bureau, particulièrement dans les lieux de travail laissés sans surveillance. * Verrouiller les classeurs laissés sans surveillance, ainsi que les appareils mobiles, comme les ordinateurs portables. * Interroger les inconnus qui se trouvent dans les aires à accès restreint. * Protéger les renseignements et les ordinateurs utilisés hors de l’établissement, conformément à la feuille-info [*Le chiffrement des renseignements personnels sur la santé dans les appareils mobiles*](https://www.ipc.on.ca/French/Resources/Educational-Material/Educational-Material-Summary/?id=613) du Commissaire à l’information et à la protection de la vie privée/Ontario (CIPVP). * Éviter de divulguer accidentellement des renseignements confidentiels en discutant, en utilisant un écran d’ordinateur dont le contenu peut être visible par une personne non autorisée ou en laissant un bureau sans surveillance. * Éliminer les copies papier et électroniques des renseignements personnels sur la santé conformément à la feuille-info [*La destruction sécurisée des renseignements personnels*](https://www.ipc.on.ca/french/resources/educational-material/educational-material-summary/default.aspx?id=451)du CIPVP. * Avant d’envoyer une télécopie, s’assurer que le numéro est toujours valide et qu’il est bien composé. * Utiliser le système seulement pour fournir des soins de santé ou aider à le faire. * Signaler les incidents en lien avec la sécurité au responsable de la sécurité. |
| Personne légalement responsable | Souvent, un administrateur général de l’organisme, p. ex., le directeur de l’information.  **Responsabilités**   * Cette personne est légalement responsable du processus d’inscription pour son dépositaire de renseignement sur la santé. Elle a pour rôle d’autoriser les approbateurs et les autorités locales d’enregistrement à s’occuper du processus d’inscription au nom du dépositaire de renseignements sur la santé. |
| Responsable de la sécurité | Membre du personnel désigné par l’organisme qui a la responsabilité générale de gérer le programme de sécurité au quotidien, notamment en signalant les incidents au bureau de l’équipe de [la solution de DSE]. Dans un milieu de travail, le responsable de la sécurité peut être une infirmière, un assistant de bureau de médecin ou un autre professionnel de la santé qui s’est vu confier ces responsabilités.  **Responsabilités**   * Veiller à ce que votre organisme respecte les exigences en matière de sécurité en tout temps. * Communiquer avec le bureau de l’équipe de [la solution de DSE] en cas d’incident. * Fournir le soutien nécessaire pour mener les enquêtes, au besoin, et veiller à ce que les mesures de rétablissement nécessaires soient appliquées. * Veiller à ce que la politique de sécurité soit affichée visiblement sur les lieux de travail afin que le personnel et les patients puissent la consulter, au besoin. * Veiller à ce que le personnel et les entrepreneurs connaissent la politique de sécurité, et sachent l’interpréter et la mettre en œuvre. * Veiller à ce que le personnel ait suivi une formation sur ses responsabilités en matière de sécurité. * Lorsqu’elles sont utilisées, recueillir et classer les ententes de confidentialité remplies et signées (voir l’[*Annexe B : MODÈLE d’entente de confidentialité*](#_Appendix_B:_Confidentiality)*)* des mandataires, du personnel et des fournisseurs de services électroniques et de TI. * Veiller à ce que les renseignements personnels et les renseignements personnels sur la santé soient éliminés conformément aux normes de sécurité énoncées dans la feuille-info [*La destruction sécurisée des renseignements personnels*](https://www.ipc.on.ca/french/resources/educational-material/educational-material-summary/default.aspx?id=451)du CIPVP*.* * Veiller à ce que le personnel ait accès à la machine à détruire les documents afin d’éliminer les renseignements personnels sur la santé qui ne sont plus nécessaires. * Expliquer au personnel comment créer des mots de passe forts faciles à mémoriser, mais difficiles à deviner, et lui rappeler de ne jamais les divulguer. * S’assurer que le personnel comprend qu’il ne doit pas installer de logiciels non autorisés, ni connecter des appareils non autorisés à ses ordinateurs ou utiliser les appareils à des fins non autorisées. * Révoquer ou modifier adéquatement l’accès (appareils, réseau, système et application) et changer les mots de passe communs dès que les employés quittent leur poste ou qu’ils ont de nouvelles responsabilités. * Indiquer au fournisseur de services de TI d’installer des dispositifs de sécurité sur tous les ordinateurs de l’établissement, y compris des solutions cryptographiques fortes, des correctifs de sécurité et des logiciels antivirus. * Veiller à ce que le fournisseur de services de TI fournisse une description écrite des services offerts. * Surveiller et effectuer des vérifications ponctuelles régulières pour s’assurer que le personnel suit la politique de sécurité. Si ce n’est pas le cas, prendre les mesures nécessaires. |

**Tableau 2 – Rôles et responsabilités relatifs à [la solution de DSE] non applicables aux dépositaires de renseignements sur la santé (souvent rattachés à cyberSanté Ontario ou à ses partenaires de prestation)**

| Rôles externes | Définitions et responsabilités |
| --- | --- |
| Autorité d’enregistrement | Entité supérieure généralement responsable de s’occuper de la gestion de l’enregistrement et de l’identité et d’enregistrer les autorités locales d’enregistrement.  [la solution de DSE] ou ses représentants agiront à titre d’autorité d’enregistrement pour tous les mandataires et fournisseurs de services électroniques qui demandent un accès à la solution (ONE ID agit à titre d’autorité d’enregistrement). |
| Bureau de l’équipe de [la solution de DSE] | Ressources contractuelles internes et externes qui soutiennent [la solution de DSE].  **Responsabilités**  Occuper une fonction centrale qui consiste à coordonner les activités comme la publication des communiqués, la supervision générale des incidents en lien avec la protection de la vie privée et la sécurité, la gestion de l’infrastructure et du temps utilisable de [la solution de DSE]. |
| Comité ConnexionSécurité | Tribune provinciale sur la sécurité formée de représentants supérieurs de la sécurité provenant des régions et de cyberSanté Ontario.  **Responsabilités**   * Établir un cadre de gouvernance de la sécurité de l’information fonctionnel et utile pour les organisations qui utilisent les DSE. |
| Comité de protection de la vie privée ConnectingPrivacy | Comité formé de mandataires des dépositaires de renseignements sur la santé participants.  **Responsabilités**   * Appuyer la structure de gestion de la confidentialité et de la sécurité de l’information de [la solution de DSE]. |
| Équipe des opérations en matière de protection de la vie privée et de sécurité de [la solution de DSE] | Équipe composée de mandataires de [la solution de DSE] qui s’occupent des mesures, des initiatives et des processus liés à la confidentialité et à la sécurité de la solution.  **Responsabilités**   * Soutenir l’évaluation de la protection de la vie privée et de la sécurité. * Soutenir la coordination des incidents en lien avec la protection de la vie privée et la sécurité auprès des dépositaires de renseignements sur la santé et des autres intervenants de [la solution de DSE]. * Soutenir l’évaluation des risques et des menaces. * Soutenir les activités liées à la protection de la vie privée et à la sécurité. |
| Organisme de surveillance compétent | Cadres supérieurs qui supervisent l’ensemble des aspects de [la solution de DSE].  **Responsabilités**   * Prendre des décisions sur les dérogations à la politique en matière de sécurité. * Examiner les documents en lien avec la sécurité, p. ex, évaluations de la menace et des risques et des incidents majeurs, pour s’assurer que les mesures nécessaires sont appliquées. |

**Avis de droit d’auteur**

© cyberSanté Ontario, 2018.

**Tous droits réservés**

Il est interdit de reproduire le présent document, en totalité ou en partie, de quelque manière que ce soit, y compris en le photocopiant ou en le transférant en format électronique sur un ordinateur, sans d’abord obtenir une autorisation écrite de cyberSanté Ontario. Les renseignements présentés dans le présent document sont la propriété de cyberSanté Ontario, et il est interdit de les utiliser ou de les divulguer, sauf autorisation écrite expresse de cyberSanté Ontario.

**Marques de commerce**

Les autres noms de produits mentionnés dans le présent document peuvent être des marques de commerce ou des marques de commerce déposées, et sont ici reconnus comme étant la propriété de leurs entreprises respectives.