cyberSanté Ontario
Travaille pour vous

Politique tout-en-un sur la sécurité des dossiers de santé électroniques

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

Version : v2.1

Ontario
cyberSanté Ontario

Table des matières

Introduction

Objectif

Le présent document vise principalement à établir les exigences des politiques de sécurité du dossier de santé électronique (DSE) pour les organismes ayant seulement des droits de visualisation lors de l'accès à la [solution DSE].

Les exigences contenues dans les politiques visent à protéger la confidentialité, l'intégrité et la disponibilité des renseignements personnels sur la santé stockés ou traités dans la [solution DSE].

Les numéros de contrôle originaux sont inscrits de la manière suivante {1.1} afin de faciliter les activités de conformité.

Portée

Les politiques nommées dans le présent document s'appliquent à :

- tous les dépositaires de renseignements sur la santé, soit les organismes ayant seulement des droits de visualisation dans le cadre de la [solution DSE], ainsi que leurs mandataires et leurs fournisseurs de services électroniques pouvant consulter la solution ou y ayant accès.

Voici les politiques de sécurité en vigueur pour les organismes ayant seulement des droits de visualisation :

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

La présente politique doit être lue conjointement avec les politiques en matière de protection de la vie privée du DSE et les procédures qui y sont associées, dans leur version modifiée de temps à autre.

La Politique de confidentialité du D, ainsi que les politiques conjointes de confidentialité et de sécurité mentionnées dans le présent document, sont disponibles sur le site Web de cyberSanté Ontario : https://www.ehealthontario.on.ca/images/uploads/regional_partners/cGTA/privacy_policies_and_procedures/ehr_privacy_policies-fr.pdf.

Glossaire

[la solution de DSE] : [la solution de DSE] et les systèmes de soutien sont destinés au stockage et à la consultation par voie électronique de certains renseignements personnels sur la santé provenant des systèmes des dépositaires de renseignements sur la santé (parfois indisponibles dans les services d'archives provinciaux ou régionaux prévus) en vue de servir de dépôt unique et de réduire la charge des systèmes sources. Ce terme n'englobe pas les systèmes d'information et les technologies de l'information des dépositaires participants.

Approbateur : Toute personne ayant le pouvoir d'autoriser l'accès des mandataires et des fournisseurs de services électroniques à [la solution de DSE]. 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. À noter que cette définition s'applique dans le cadre de la présente politique et de [la solution de DSE].

Autorité d'enregistrement : Personne ou entité responsable d'enregistrer les autorités locales d'enregistrement. L'équipe de [la solution de DSE] ou ses délégués agiront à titre d'autorité d'enregistrement pour tous les dépositaires de renseignements sur la santé dont les mandataires et les fournisseurs de services ont accès à [la solution de DSE] conformément au processus de contrôle, aux procédures, aux politiques et au système de gestion de l'identité du dépositaire.

Autorité locale d'enregistrement : Personne autorisée par la personne légalement responsable du dépositaire de renseignement sur la santé à gérer le processus d'enregistrement ou d'inscription afin que le mandataire et le fournisseur de services électroniques du dépositaire puissent avoir accès à [la solution de DSE] conformément au processus de contrôle, aux procédures, aux politiques et au système de gestion de l'identité. Les autorités locales d'enregistrement, inscrites auprès de l'équipe de [la solution de DSE] ou de ses délégués, enregistrent et inscrivent les mandataires et les fournisseurs de services électroniques au nom de [la solution de DSE]. À noter que cette définition s'applique dans le cadre de la présente politique et de [la solution de DSE].

Comité ConnexionSécurité : Forum sur la sécurité provincial composé des hauts représentants de la sécurité des régions et de cyberSanté Ontario. Il s'agit d'un groupe décisionnel dont la responsabilité est d'établir un cadre de gouvernance fonctionnel et utilisable sur la sécurité de l'information pour les organismes qui utilisent le DSE.

Devrait/devraient : Termes employés lorsque les utilisateurs, dans certains cas, peuvent avoir des raisons valables de ne pas respecter l'exigence. Toutefois, le responsable de la mise en œuvre doit être conscient des conséquences de ce geste et envisager d'instaurer des mesures de contrôle compensatoires.

Équipe des opérations en matière de protection de la vie privée et de sécurité : 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].

Fournisseur de services électroniques : Personne qui fournit des biens ou des services en vue de permettre à un dépositaire de renseignements sur la santé, par voie électronique, 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.

Mandataire : Relativement à un dépositaire de renseignements sur la santé, s'entend d'une personne, que celle-ci ait ou non l'autorité de le lier, qu'elle soit ou non employée par lui et qu'elle soit ou non rémunérée, qui agit pour lui ou en son nom avec son autorisation, à ses fins à lui et non aux siennes, à l'égard de renseignements personnels sur la santé. Par exemple, il peut s'agir d'un organisme, d'un employé ou d'un entrepreneur qui valide l'identité des utilisateurs du DSE au nom d'un dépositaire de renseignements sur la santé. Un mandataire peut offrir des services de correction des données de ses terminaux d'envoi de données pour un dépositaire.

Obligatoire ou doit/doivent : Termes désignant des exigences non facultatives.

Organisme ayant seulement des droits de visualisation : Organisme qui peut visualiser les données de [la solution de DSE] aux fins autorisées. L'organisme se sert des données d'identification de ONE ID ou d'un fournisseur d'identité (p. ex., hôpital ou organisme partenaire ou fournisseur de service de [la solution de DSE]) pour pouvoir accéder aux renseignements de 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*.

Organisme de surveillance compétent : Organisme de surveillance compétent composé de cadres supérieurs veillant sur chaque aspect de [la solution de DSE]. Voir la section *Structure d'administration de la politique*.

Personne légalement responsable : Souvent l'administrateur général d'un organisme, le directeur de l'information par exemple. Cette personne est légalement responsable du processus d'inscription du dépositaire de renseignements sur la santé. Elle est chargée d'autoriser l'approbateur et l'autorité locale d'enregistrement à agir pour le compte du dépositaire lors de l'inscription et du processus d'inscription.

Peut/peuvent : Exigence qui n'est en fait qu'une recommandation, ou une liste d'exemples qui ne se veut pas exhaustive.

Technologie de l'information : Tout bien (matériel ou logique) servant à l'acquisition, au stockage, à la manipulation, à la gestion, au transfert, au contrôle, à l'affichage, à la commutation, à l'échange, à la transmission ou à la réception automatiques de données ou de renseignements. Il peut s'agir par exemple de matériel, de logiciels, de micrologiciels, d'équipement auxiliaire ou de ressources connexes.

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.

Application

Tous les cas de non-conformité doivent être examinés par l'organisme de surveillance compétent.

L'organisme de surveillance compétent a le pouvoir d'imposer des sanctions (allant jusqu'à la révocation du privilège d'accès des mandataires ou des ententes conclues avec les dépositaires de renseignements sur la santé) ainsi que des mesures correctives.

Structure d'administration de la politique

Solution de DSE	Organisme de surveillance compétent
Répertoire ConnexionOntario des données cliniques (RDC)	Comité stratégique de cyberSanté Ontario

Politique de sécurité de l'information

(✓) : À faire

Principes

Utilisation acceptable des données et des technologies de l'information

- ✓ L'équipe de [la solution de DSE] et les dépositaires de renseignements sur la santé doivent définir les exigences en matière d'utilisation acceptable des données et des technologies de l'information que doivent respecter les mandataires et les fournisseurs de services électroniques de [la solution de DSE], ainsi que les dépositaires de renseignements sur la santé, leurs mandataires et leurs fournisseurs de services électroniques qui participent à [la solution de DSE]. {1.1}

  Consultez la Norme d'utilisation acceptable des données et des technologies de l'information à ce sujet.

Cryptographie

- ✓ Les dépositaires de renseignements sur la santé doivent chiffrer leurs systèmes d'information pertinents afin de protéger la confidentialité et l'intégrité des renseignements personnels sur la santé lors de la participation à [la solution de DSE]. {1.6}

  Consultez la Norme sur la cryptographie à ce sujet.

Fournisseurs de services électroniques

- ✓ Les dépositaires de renseignements sur la santé doivent s'assurer que les fournisseurs de services électroniques qui auront accès aux services de gestion d'identité ou aux terminaux d'envoi de données, ou qui gèrent ou soutiennent ces systèmes, disposent de mesures de contrôle adéquates en matière de sécurité de l'information pour préserver la confidentialité, l'intégrité et la disponibilité des renseignements. {1.16}

  Consultez la Norme sur les fournisseurs de services électroniques à ce sujet.

Gestion de l'information et des éléments d'actif

- ✓ L'équipe de [la solution de DSE] doit catégoriser et définir les exigences en matière de protection des renseignements personnels sur la santé se trouvant dans [la solution de DSE] de manière à assurer la confidentialité, l'intégrité et la disponibilité de ces données en format papier et électronique tout au long de leur cycle de vie. {1.7}

  Consultez la Norme sur la gestion de l'information et des éléments d'actif à ce sujet.

Gestion des incidents de sécurité de l'information

- ✓ L'équipe de [la solution de DSE] et les dépositaires de renseignements sur la santé doivent mettre en place un processus de gestion visant à déceler et à régler rapidement et efficacement les problèmes relatifs à la sécurité de l'information liés à la participation dans [la solution de DSE] ou de [la solution de DSE], et ce, tout en réduisant leur incidence et les risques que la situation se reproduise. {1.21}

  Consultez la Norme sur la gestion des incidents de sécurité de l'information à ce sujet.

Formation sur la sécurité de l'information

- ✓ L'équipe de [la solution de DSE] et les dépositaires de renseignements sur la santé doivent favoriser une culture de sécurité de l'information. Pour ce faire, ils peuvent mettre en œuvre un programme de sensibilisation et d'éducation destiné à aider tous les utilisateurs qui participent à [la solution de DSE] à comprendre leurs obligations dans ce domaine. {1.2}

  Consultez la Politique sur la formation en protection de la confidentialité et de la sécurité à ce sujet.

Réseaux et opérations

- ✓ Les dépositaires de renseignements sur la santé doivent mettre en place des mesures de contrôle pour sécuriser leur infrastructure réseau et établir des procédures pour sécuriser la gestion et le fonctionnement continus des services de gestion d'identité et des points d'accès des données de contribution. {1.12}

  Consultez la Norme sur les réseaux et les opérations à ce sujet.

Assurance de protection de la vie privée et de sécurité

- ✓ Les dépositaires de renseignements sur la santé doivent cerner et atténuer les risques en matière de protection de la vie privée et de sécurité, ainsi que les cas de non-conformité relatifs à [la solution de DSE], notamment au moyen d'auto-évaluations de l'état de préparation à la protection de la vie privée et à la sécurité, et de mesures d'audit, de contrôle et d'assurance de la conformité des mandataires et des fournisseurs de services électroniques. {1.22}

  Consultez la Politique harmonisée d'assurance de protection de la vie privée et de sécurité (Privacy and Security Harmonized Assurance Policy) à ce sujet.

Gestion des risques

Consultez la Norme sur la gestion des menaces et des risques à ce sujet.

Responsabilités des dépositaires de renseignements sur la santé

Tous les dépositaires de renseignements sur la santé doivent :

- ✓ élaborer, mettre en œuvre et tenir à jour une politique de sécurité de l'information pour leur organisme, laquelle appuie les principes énoncés dans la présente politique et les autres politiques, normes et documents à l'appui applicables dans ce domaine; {3.4.1}

- ✓ nommer un responsable de la sécurité de l'information qui aura pour mandat d'assurer le respect des principes définis dans la présente politique. Ce responsable peut être la personne-ressource nommée conformément à l'article 15 de la *Loi de 2004 sur la protection des renseignements personnels sur la santé*, ou la personne-ressource de l'établissement indiquée dans l'accord de participation; {3.4.2}

- ✓ veiller à ce que les mandataires et les fournisseurs de services électroniques ayant accès aux services de [la solution de DSE] soient informés adéquatement de leurs responsabilités en matière de sécurité de l'information; {3.4.3}

- ✓ faire signer un contrat d'utilisateur final comprenant des clauses de confidentialité aux mandataires et aux fournisseurs de services électroniques avant de leur donner accès à [la solution de DSE]; {3.4.4}

- ✓ tenir les mandataires et les fournisseurs de services électroniques responsables de l'accès inapproprié ou non autorisé à [la solution de DSE] ou à ses systèmes d'information, ainsi que de la collecte, de l'utilisation, de la divulgation, de l'élimination, de la modification et du brouillage inappropriés ou non autorisés des renseignements. {3.4.5}

Norme d'utilisation acceptable des données et des technologies de l'information

(✓) : À faire, (X) : À ne pas faire

Les dépositaires de renseignements sur la santé, leurs mandataires et leurs fournisseurs de services électroniques (« tous les utilisateurs ») doivent respecter les exigences suivantes :

- ✓ Toujours se servir des données d'identification qui leur ont été assignées pour participer à [la solution de DSE]. {1.1}

- ✓ Respecter les modalités d'utilisation de [la solution de DSE]. {1.7}

- ✓ Utiliser les outils et les processus de [la solution de DSE] ou ceux approuvés par le dépositaire de renseignements sur la santé pour accéder à [la solution de DSE]. {1.9}

- ✗ Ne jamais laisser une autre personne se servir de leurs données d'identification pour participer à [la solution de DSE]. Tous les utilisateurs sont responsables des actions exécutées sur [la solution de DSE] avec leur nom d'utilisateur. {1.2}

- ✗ Participer à [la solution de DSE] uniquement si leurs fonctions l'exigent, s'ils y sont expressément autorisés ou s'il est nécessaire de le faire (p. ex., pour fournir des soins de santé ou faciliter leur prestation), et ce, conformément aux politiques de confidentialité liées à [la solution de DSE] ou à celles de leurs dépositaires de renseignements sur la santé respectifs. {1.3}

- ✗ Ne jamais désactiver, outrepasser ou contourner intentionnellement les mesures de contrôle de la sécurité de l'information lors de la participation à [la solution de DSE]. {1.4}

- ✗ Ne jamais tenter d'exploiter des failles de sécurité potentielles de [la solution de DSE], même pour vérifier si elles existent vraiment, à moins cela ne fasse partie des tâches et responsabilités qui leur sont assignées dans le cadre de leur travail et qu'ils y aient expressément été autorisés à le faire. {1.5}

- ✗ Ne jamais réaliser sciemment une action qui nuira au fonctionnement normal de [la solution de DSE], ou tenter de perturber la [solution DES] en la rendant intentionnellement indisponible ou en portant atteinte à l'intégrité des données sont stockées ou traitées pour la participation à [la solution de DSE]. {1.6}

- ✗ Ne jamais prendre en photo des données affichées dans [la solution de DSE]. {1.10}

Tous les utilisateurs devraient respecter l'exigence suivante :

- ✓ Verrouiller leur appareil informatique quand ils le laissent sans surveillance dans les installations des dépositaires de renseignements sur la santé et qu'une session de [la solution de DSE] y est ouverte. {1.8}

Envoi de renseignements personnels sur la santé par courriel[1]

Tous les utilisateurs doivent respecter les exigences suivantes :

- ✓ Envoyer des renseignements personnels sur la santé au bureau de l'équipe de [la solution de DSE] par courriel uniquement si cela est nécessaire pour offrir des soins de santé ou faciliter leur prestation ou dans le cadre du fonctionnement de [la solution de DSE], et s'il est acceptable de le faire selon les politiques ou procédures relatives à [la solution de DSE] ou celles de leurs dépositaires de renseignements sur la santé respectifs. {1.11}

- ✓ Chiffrer les courriels contenant des renseignements personnels sur la santé, utiliser une solution de transfert de fichiers sécuritaire ou se servir d'un système de courriel sécuritaire et approuvé par leurs dépositaires de renseignements sur la santé respectifs ou [la solution de DSE]. {1.12}

[1] Cette section ne s'applique qu'à l'envoi par courriel de renseignements personnels sur la santé à l'équipe de la [solution DSE]. Elle ne vise pas les pratiques d'envoi de courriel à l'interne des dépositaires de renseignements sur la santé.

- ✓ Ne jamais envoyer de renseignements personnels sur la santé provenant de [la solution de DSE] à l'aide de comptes de courriel externes (p. ex., Hotmail ou Gmail), ou les faire envoyer à ce type de comptes. {1.13}

Création et protection de mots de passe[2]

Tous les utilisateurs devraient respecter l'exigence suivante :

- ✓ Dans la mesure du possible, utiliser des phrases (p. ex., « Ja1meLaP!zza ») comme mots de passe pour participer à [la solution de DSE]. {1.14}

Tous les utilisateurs doivent respecter les exigences suivantes :

- ✓ Pour participer à [la solution de DSE], toujours créer des mots de passe composés d'au moins huit caractères, lesquels entrent dans au moins trois des catégories suivantes : {1.15}
    - chiffre, {1.15.1}
    - lettre majuscule, {1.15.2}
    - lettre minuscule, {1.15.3}
    - caractère spécial. {1.15.4}
- ✓ Pour participer à [la solution de DSE], choisir des mots de passe facilement mémorisables, mais difficiles à deviner par d'autres personnes. {1.17}
- ✓ Pour participer à [la solution de DSE], employer des mots de passe différents de ceux d'autres comptes (p. ex., compte de courriel de l'établissement ou compte bancaire personnel). {1.19}
- ✓ Mémoriser les mots de passe servant à participer à [la solution de DSE]. Tous les utilisateurs doivent éviter de tenir un registre de leurs mots de passe (p. ex., les inscrire sur une feuille ou dans un fichier), sauf : {1.20}
    - si ceux-ci peuvent être stockés de manière sécuritaire; {1.20.1}
    - si le nom d'utilisateur n'est pas noté, ou s'il n'est pas indiqué qu'il s'agit du mot de passe de [la solution de DSE]. {1.20.2}
- ✓ Garder secrets les mots de passe permettant de participer à [la solution de DSE] et ne jamais les révéler à qui que ce soit, pas même à un administrateur du système, à un employé d'un service de dépannage ou à un gestionnaire. {1.21}
- ✓ Changer immédiatement le mot de passe servant à participer à [la solution de DSE] s'ils soupçonnent ou découvrent que celui-ci a été divulgué ou compromis, et signaler l'incident lié à la sécurité de l'information au premier point de contact responsable (p. ex., service de dépannage ou responsable de la protection de la

[2] Cette section ne s'applique qu'aux mots de passe permettant d'accéder directement à la [solution DSE].

vie privée). Voir la section *Signalement des incidents liés à la sécurité de l'information de [la solution de DSE]* ci-après. {1.22}

- ✓ Toujours modifier le mot de passe initial fourni pour la première connexion à [la solution de DSE] en suivant les directives du fournisseur d'identité. {1.24}

- ✗ Ne jamais créer de mots de passe utilisés pour participer à [la solution de DSE] qui comportent : {1.16}
    - une partie ou la totalité de leur nom d'utilisateur; {1.16.1}
    - des renseignements personnels faciles à obtenir (p. ex., nom de membres de la famille ou d'animaux de compagnie, dates de naissance, anniversaires, passe-temps); {1.16.2}
    - trois caractères consécutifs (p. ex., AAA). {1.16.3}

- ✗ Ne jamais modifier de manière facilement prévisible les mots de passe utilisés pour participer à [la solution de DSE](p. ex., changer « Ja1meLaP!zza1 » pour « Ja1meLaP!zza2 »). {1.18}

- ✗ Ne jamais intégrer le nom d'utilisateur ou le mot de passe permettant de participer à [la solution de DSE] dans un processus d'identification unique (p. ex., macro-instruction ou touche de fonction programmable), sauf pour les systèmes de gestion de l'identification approuvés pour [la solution de DSE]. {1.23}

Travail à distance

Tous les utilisateurs doivent respecter les exigences suivantes :

- ✓ Utiliser une solution d'accès à distance approuvée par l'équipe de [la solution de DSE] ou les dépositaires de renseignements sur la santé (p. ex., réseau privé virtuel ou terminal) pour se connecter à distance à [la solution de DSE]. {1.25}

- ✓ Suivre la procédure de déconnexion adéquate lors d'un accès à distance à [la solution de DSE] (p. ex., si la solution d'accès à distance dispose d'une fonction de déconnexion, utiliser cette dernière au lieu de simplement fermer l'application). {1.26}

- ✓ Lorsqu'il est nécessaire de laisser un appareil informatique mobile dans un véhicule, tous les utilisateurs doivent le placer hors de vue et verrouiller le véhicule. {1.29}

- ✓ 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. Le chiffrement intégral du disque de l'appareil sans fil est la méthode privilégiée; toutefois, l'implantation du chiffrement conteneurisé du disque partagé et de l'appareil de l'entreprise est aussi acceptable. {1.30}

- ✗ Ne jamais participer à [la solution de DSE] dans un lieu où des personnes non autorisées peuvent voir les renseignements affichés à l'écran (p. ex., cafés Internet, transports en commun et autres lieux publics). {1.27}

- ✗ Ne jamais laisser un appareil informatique mobile pouvant participoer à [la solution de DSE] sans surveillance dans un endroit public. {1.28}

Signalement des incidents liés à la sécurité de l'information de [la solution de DSE]

Tous les utilisateurs doivent respecter les exigences suivantes :

- ✓ Signaler immédiatement les incidents présumés ou constatés relativement à la sécurité de l'information de [la solution de DSE] au premier point de contact responsable (p. ex., service de dépannage ou responsable de la protection de la vie privée). Sinon, le dépositaire de renseignements sur la santé peut demander aux mandataires de signaler l'incident à leur gestionnaire ou superviseur, lequel avisera ensuite le premier point de contact. {1.31}

  Voici des exemples d'incidents liés à la sécurité de l'information :

  - Divulgation non autorisée de renseignements personnels sur la santé.
  - Vol ou perte de technologies de l'information contenant des renseignements personnels sur la santé ou participant à [la solution de DSE] (même si elles sont chiffrées).
  - Contamination par virus ou logiciel malveillant d'un appareil qui participe à [la solution de DSE].
  - Tentatives (réussies ou ratées) d'accès non autorisé à [la solution de DSE].
  - Mot de passe compromis (c'est-à-dire qu'une autre personne connaît votre mot de passe permettant de participer à [la solution de DSE]).

- ✓ Offrir leur entière collaboration au bureau de l'équipe de [la solution de DSE], à ses mandataires ou à ses fournisseurs de services électroniques dans le cadre de toute enquête sur des incidents liés à la sécurité de l'information. {1.32}

Norme sur la cryptographie

(✓) : À faire

- ✓ Les dépositaires de renseignements sur la santé ne doivent utiliser que les algorithmes cryptographiques approuvés pour [la solution de DSE]. La liste des algorithmes cryptographiques approuvés se trouve à *l'Annexe A : Algorithmes cryptographiques approuvés*. {1.1}

- ✓ Les dépositaires de renseignements sur la santé doivent veiller à ce que chaque clé cryptographique ou élément de clé ait le moins de responsables possible. {1.35}

Norme sur les fournisseurs de services électroniques

(✓) : À faire

- ✓ Les dépositaires de renseignements sur la santé devraient classer leurs fournisseurs de services électroniques en fonction de leur type (p. ex., fournisseur de services applicatifs, de service de réseau ou de services de stockage) ainsi que selon l'importance des services qu'ils offrent. {1.1}

- ✓ Les dépositaires de renseignements sur la santé doivent évaluer les risques à la sécurité de l'information et à la protection de la vie privée que posent les nouveaux fournisseurs de services électroniques pour [la solution de DSE] avant de conclure tout contrat avec ces derniers. {1.2}

- ✓ Les dépositaires de renseignements sur la santé doivent établir et définir les systèmes d'information et les services qu'offrira le nouveau fournisseur de services électroniques ou le faire lors du renouvellement de l'entente de service. Une entente de service devrait comprendre : {1.3}

    - les rôles et responsabilités qui figurent dans la *LPRPS* et dans les politiques et procédures en matière de confidentialité et de sécurité de l'information mises en place pour [la solution de DSE]; {1.3.1}
    - les rôles et responsabilités en ce qui a trait à la mise en place, à la tenue à jour et à la gestion des systèmes ou des services d'information offerts; {1.3.2}
    - le degré d'importance des services; {1.3.3}
    - les dates et heures auxquels le service est requis; {1.3.4}
    - les exigences de capacité des systèmes et des réseaux; {1.3.5}
    - la durée d'interruption acceptable maximale et les objectifs en matière de niveaux de service; {1.3.6}
    - les rapports sur le niveau de service et leur fréquence; {1.3.7}
    - les limites de temps à ne pas dépasser (c.-à-d. la durée de panne de service après laquelle la situation devient inacceptable pour le dépositaire de renseignements sur la santé); {1.3.8}
    - les sanctions à imposer si un fournisseur de services électroniques ne réussit pas à assurer le niveau de service convenu ou ne respecte pas ses rôles et responsabilités; {1.3.9}
    - les mesures de contrôle minimales pour protéger la vie privée et assurer la sécurité de l'information; {13.10}
    - les produits livrables attendus; {1.3.11}
    - les représentants de chaque fournisseur de services électroniques. {1.3.12}

- ✓ Les dépositaires de renseignements sur la santé doivent exiger des nouveaux fournisseurs de services électroniques qu'ils mettent en œuvre des mesures de contrôle pour protéger la vie privée et assurer la sécurité de l'information avant de leur donner accès à [la solution de DSE]. {1.3}

- ✓ Les dépositaires de renseignements sur la santé devraient établir une marche à suivre générale pour mettre fin aux ententes qui les lient aux fournisseurs de services électroniques et qui porte notamment sur : {1.5}

    - la désignation des personnes responsables de mettre fin à la relation; {1.5.1}
    - la révocation des droits d'accès au matériel informatique et aux logiciels de l'organisation; {1.5.2}
    - le retour, le transfert ou la destruction de tous les éléments d'actif (supports de sauvegarde, documents, matériel et dispositifs d'authentification, par exemple). {1.5.3}

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

(✓) : À faire

- ✓ Les dépositaires de renseignements sur la santé doivent veiller à ce que tous les renseignements personnels sur la santé transmis au bureau de l'équipe de [la solution de DSE] ou à [la solution de DSE] le soient de manière sécuritaire (p. ex., courrier électronique sécurisé, chiffrement, tunnel d'un réseau privé virtuel). {1.1}

Norme sur la gestion des incidents de sécurité de l'information

(✓) : À faire

- ✓ Les dépositaires de renseignements sur la santé doivent mettre en place un processus de gestion des incidents de sécurité de l'information (« les incidents ») pour [la solution de DSE] qui traite de toutes les phases du processus de gestion des incidents : {1.1}
    - détection/triage
    - intervention
    - rétablissement
    - suivi

  (Voir le diagramme de l'*Annexe H : Processus de gestion des incidents de sécurité de l'information*.)

- ✓ Si, à tout moment au cours du processus de gestion des incidents, un dépositaire de renseignements sur la santé se rend compte que l'incident a entraîné une violation de la vie privée, il doit alors se référer à la Politique de gestion des incidents et des violations touchant la protection de la vie privée pour le résoudre. {1.2}

Détection/triage

- ✓ Les dépositaires de renseignements sur la santé doivent établir un point de contact auquel seront signalés les incidents liés à [la solution de DSE] qui ont eu lieu ou dont on soupçonne l'existence. Le plus souvent, c'est le soutien technique qui fait office de point de contact. {1.3}

- ✓ Les dépositaires de renseignements sur la santé doivent veiller à ce que leurs mandataires et leurs fournisseurs de services électroniques sachent qu'ils doivent signaler sur-le-champ tout incident réel ou présumé. {1.4}

- ✓ Le point de contact doit créer un billet d'incident ou consigner l'incident dans un journal chaque fois qu'un incident en lien avec [la solution de DSE] est signalé. Le billet doit au moins contenir les éléments suivants : {1.5}
    - L'heure et la date de l'incident signalé. {1.5.1}
    - Le nom et les coordonnées du mandataire ou du fournisseur de services électroniques qui a signalé l'incident. {1.5.2}
    - Une description de l'incident (p. ex., type d'incident et façon dont il a été détecté). {1.5.3}
    - Les conséquences de l'incident. {1.5.4}
    - Les mesures adoptées pour contenir l'incident soit par le mandataire ou le fournisseur de services électroniques qui a signalé l'incident, soit par le point de contact. {1.5.5}
- ✓ Les dépositaires de renseignements sur la santé doivent nommer un chef ou une équipe d'intervention en cas d'incident chargé de s'occuper des activités de triage, d'intervention, de rétablissement et de suivi des incidents relatifs à [la solution de DSE] ou à l'équipe qui en est responsable. Ce chef ou cette équipe peut aussi être le point de contact. {1.6}
- ✓ Le point de contact doit faire parvenir tous les billets d'incidents liés à [la solution de DSE] ou à l'équipe qui en est responsable au chef ou à l'équipe d'intervention qui sera responsable d'examiner chaque billet et les documents à l'appui pour vérifier si un incident a bel et bien eu lieu. {1.7}
- ✓ Le chef ou l'équipe d'intervention doit classer les incidents liés à [la solution de DSE] qui ont réellement eu lieu en fonction de leur gravité (voir l'*Annexe B : Cote de gravité et de priorité des incidents*). {1.8}
- ✓ Le chef ou l'équipe d'intervention doit rédiger un rapport d'incident (voir l'*Annexe C : Contenu du rapport d'incident*). {1.9}
- ✓ Les dépositaires de renseignements sur la santé doivent s'assurer que selon leur processus de gestion des incidents, le chef ou l'équipe d'intervention en cas d'incident a l'obligation de signaler, par courriel ou téléphone, d'ici la fin du jour ouvrable suivant, tout incident avéré de gravité 1 ou 2 (selon l'*Annexe B : Cote de gravité et de priorité des incidents*) à l'Équipe des opérations en matière de protection de la vie privée et de sécurité de [la solution de DSE] et à tout dépositaire touché. {1.10}

Ce signalement doit au moins comprendre les éléments suivants :

- L'heure et la date de l'incident signalé. {1.10.1}
- Le nom et les coordonnées du mandataire ou du fournisseur de services électroniques qui a signalé l'incident. {1.10.2}
- Une description de l'incident (p. ex., type d'incident et façon dont il a été détecté). {1.10.3}
- Les conséquences connues ou supposées de l'incident. {1.10.4}
- Les mesures adoptées pour contenir l'incident soit par le mandataire ou le fournisseur de services électroniques qui a signalé l'incident, soit par le point de contact, soit par le chef ou l'équipe d'intervention. {1.10.5}

✓ Si un incident survenu chez un dépositaire de renseignements sur la santé touche plusieurs dépositaires ou [la solution de DSE], l'équipe de la solution peut choisir de diriger les activités de gestion des incidents. {1.11}

✓ L'équipe à la tête des activités de gestion des incidents (c.-à-d. le dépositaire de renseignements sur la santé ou l'équipe de [la solution de DSE]) doit informer le Comité ConnexionSécurité et l'organisme de surveillance compétent : {1.12}

- de tout incident lié à [la solution de DSE] et classé gravité 1 dans les 72 heures suivant son signalement; {1.12.1}
- de tout incident lié à [la solution de DSE] et classé gravité 2 dans la semaine suivant son signalement. {1.12.2}

✓ Les dépositaires de renseignements sur la santé devraient accorder la priorité aux incidents liés à [la solution de DSE] selon la cote de gravité qui leur est attribuée. {1.13}

Intervention

✓ Le chef ou l'équipe d'intervention doit prendre des mesures pour limiter la portée et l'ampleur d'un incident. Voici quelques mesures d'atténuation ou de contrôle : {1.14}

- Effectuer une copie de sauvegarde du système d'information. {1.14.1}
- Cesser les activités. {1.14.2}
- Modifier les mots de passe ou les listes de contrôle d'accès des systèmes d'information compromis. {1.14.3}
- Restreindre la connexion. {1.14.4}

N.B. : Selon la gravité de l'incident, l'organisme devra peut-être mettre en place son plan de continuité des activités.

Rétablissement

- ✓ Les dépositaires de renseignements sur la santé doivent rétablir les systèmes d'information touchés afin qu'ils redeviennent entièrement fonctionnels. Les activités de rétablissement peuvent être les suivantes : {1.15}
    - Éliminer la cause de l'incident (suppression d'un logiciel malveillant, par exemple). {1.15.1}
    - Restaurer le système d'information et en valider l'état. {1.15.2}
    - Décider du moment de la reprise des activités. {1.15.3}
    - Surveiller les systèmes d'information pour voir s'ils fonctionnent bien et confirmer qu'il n'y a plus de données ou de systèmes compromis. {1.15.4}

Suivi

- ✓ Les dépositaires de renseignements sur la santé doivent mener une enquête pour déterminer la cause de l'incident lié à [la solution de DSE] (en effectuant une analyse par arbre de défaillances, par exemple). {1.16}
- ✓ Une fois l'incident lié à [la solution de DSE] ou à l'équipe qui en est responsable (c.-à-d. lorsque toutes les activités de rétablissement ont été mises en œuvre et que les systèmes d'information et les technologies de l'information touchés sont revenus à leur état normal), le chef ou l'équipe d'intervention doit rédiger le rapport d'incident. Lorsque les dépositaires de renseignements sur la santé mènent de longues enquêtes, l'équipe de [la solution de DSE] ou les dépositaires touchés peuvent demander à être tenus au courant des avancées de l'enquête au fur et à mesure. {1.17}
- ✓ Les dépositaires de renseignements sur la santé doivent conserver les rapports d'incident lié à [la solution de DSE] pendant au moins 24 mois. {1.18}
- ✓ Les dépositaires de renseignements sur la santé doivent remettre le rapport d'incident au bureau de l'équipe de [la solution de DSE] ou aux dépositaires de renseignements sur la santé touchés au maximum 72 heures après que ceux-ci en aient demandé une copie. {1.19}
- ✓ Les versions définitives des rapports d'incident devraient être examinées par le Comité ConnexionSécurité et, au besoin, par l'organisme de surveillance compétent. {1.20}
- ✓ Les dépositaires de renseignements sur la santé devraient prévoir une méthode pour passer en revue tous les incidents liés à [la solution de DSE] au moins une fois par mois pour déterminer 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. {1.21}

Collecte de preuves

- ✓ Les dépositaires de renseignements sur la santé devraient mettre en place des procédures pour recueillir des éléments de preuves dans le but d'intention des poursuites judiciaires ou d'imposer des mesures disciplinaires contre aux mandataires ou aux fournisseurs de services électroniques. Ces procédures devraient comprendre les mesures suivantes : {1.22}
    - l'investigation informatique des copies des éléments de preuve; {1.22.1}
    - le recours à des témoins lors de la création de copies; {1.22.2}
    - la journalisation de l'information relative à la création de copies, soit : {1.22.3}
        - le moment et l'endroit où les copies sont effectuées; {1.22.3.1}
        - le nom de la personne qui a fait les copies; {1.22.3.2}
        - les outils ou les programmes utilisés; {1.22.3.3}
        - la protection de l'intégrité de tous les éléments de preuve. {1.22.3.4}

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

Les organismes qui font affaire avec le fournisseur d'identité ONE ID devront respecter les procédures établies par ce dernier.

(✓) : À faire, (X) : À ne pas faire

Attribution et modification du statut d'une autorité locale d'enregistrement

- ✓ Chaque dépositaire de renseignements sur la santé doit veiller à qu'une personne légalement responsable ou que son délégué nomme au moins une personne à titre d'autorité locale d'enregistrement responsable de l'inscription de ses mandataires et de ses fournisseurs de services électroniques devant accéder à [la solution de DSE]. {3.1}

- ✓ La personne légalement responsable doit choisir une personne qui répond aux critères suivants : {3.1}
    - elle a le temps et les ressources nécessaires pour accomplir les tâches
    - elle occupe un poste stable (elle ne risque pas de recevoir une nouvelle affectation);
    - elle possède les qualifications d'assurance de deuxième niveau de la norme pour les fournisseurs d'identités fédérées;
    - elle comprend l'importance du respect des politiques, surtout en ce qui concerne la sécurité de l'information et la confidentialité.
- ✓ Les modifications apportées au statut d'une autorité locale d'enregistrement peuvent être faites à la demande de la personne légalement responsable ou se faire à la discrétion de l'autorité d'enregistrement si cette dernière soupçonne ou découvre que l'autorité locale d'enregistrement ne respecte pas les politiques, procédures ou ententes applicables. {3.1.1}
- ✓ Si le statut d'une autorité locale d'enregistrement est révoqué ou suspendu, la personne légalement responsable doit demander qu'on lève la suspension avant que le statut soit rétabli. {3.1.2}

Inscription d'un mandataire ou d'un fournisseur de services électroniques ayant accès à [la solution de DSE]

Inscription

- ✓ L'autorité locale d'enregistrement doit valider l'identité de l'utilisateur final et de ses propres représentants lors de l'inscription, et avant de leur remettre leurs données d'identification. Elle peut établir elle-même les conditions d'inscription de l'utilisateur final. Toutefois, elle doit au moins :
    - valider les principaux renseignements identificateurs présentés à la section 3.1.1;
    - veiller à ce que la ou les méthodes employées répondent aux niveaux d'assurance requis;
    - veiller à ce que toute personne inscrite :
        - ait 16 ans ou plus;
        - possède suffisamment d'information permettant de valider son identité et de l'authentifier avec certitude lorsqu'elle souhaitera utiliser de nouveau les services fédérés.

  Les organismes doivent tirer profit des processus de leur fournisseur d'identité {Normes au sujet des prestataires qui assurent la gestion fédérée de l'identité : 3.1}

- ✓ L'autorité locale d'enregistrement doit recueillir les principaux renseignements identificateurs lors de l'inscription d'un utilisateur final :
    - ses nom et prénom officiels;
    - ses titres professionnels et ses numéros de permis d'exercice, le cas échéant. {Normes au sujet des prestataires qui assurent la gestion fédérée de l'identité : 3.1.1}

Assignation des données d'identifications

- ✓ L'autorité locale d'enregistrement, en collaboration avec ses fournisseurs d'identité, doit assigner à l'utilisateur final les éléments suivants :
    - un nom d'utilisateur;
    - l'information nécessaire pour définir un mot de passe et le conserver;
    - un niveau d'assurance {Normes au sujet des prestataires qui assurent la gestion fédérée de l'identité : 3.3}

Accès à l'information sensible

- ✓ Interdiction de donner accès à tout service fédéré contenant de l'information sensible, comme des renseignements personnels sur la santé ou des renseignements personnels, à moins que le futur utilisateur ne se soit fait attribuer un niveau d'assurance 2 ou 3.

Exigences relatives à l'inscription pour le niveau d'assurance 3

- ✓ L'identité doit être confirmée lorsqu'un niveau d'assurance 3 est requis. Cette vérification peut :
    - prendre la forme d'une vérification directe par une partie ayant autorité (p. ex., le Bureau de l'état civil ou l'Agence du revenu du Canada);
    - être confiée à un professionnel de confiance indépendant (p. ex., un avocat, un médecin ou un ministre).

  Ce processus peut aussi comprendre l'échange ou la confirmation de secrets partagés (des renseignements connus par le futur utilisateur et le tiers qui validera son identité). Par exemple, comme pour obtenir un passeport, un tiers pourrait devoir confirmer la durée continue pendant laquelle un futur utilisateur a vécu au Canada. {Normes au sujet des prestataires qui assurent la gestion fédérée de l'identité : 3.5.1}

Documents nécessaires pour l'inscription

- ✓ L'autorité locale d'enregistrement doit vérifier l'identité de chaque mandataire et fournisseur de services électroniques qui demande à avoir accès à [la solution de DSE]. Toutefois, il n'est pas nécessaire de revalider l'identité des mandataires et des fournisseurs si cela a déjà été fait par le dépositaire de renseignements sur la santé conformément aux exigences du niveau d'assurance 2 de [la solution de DSE]. L'autorité locale d'enregistrement doit tout de même s'assurer que la personne qui demande l'accès est la même que celle qui a reçu l'autorisation. {Normes au sujet des prestataires qui assurent la gestion fédérée de l'identité : 3.6}
    - Par exemple : Si le processus d'intégration d'un dépositaire de renseignements sur la santé nécessite la présentation par un mandataire d'au moins deux pièces d'identité, dont une de la liste de pièces d'identité principales (voir l'*Annexe G : Pièces d'identité acceptées*) et une de la liste de pièces d'identité principales ou secondaires (voir l'*Annexe G : Pièces d'identité acceptées*), ET que le dépositaire possède de l'information sur ces documents (p. ex., dans le dossier du mandataire), dans ce cas, l'autorité locale d'enregistrement n'a pas besoin de revalider l'identité du mandataire. Toutes les demandes d'accès à [la solution de DSE] doivent être approuvées par un approbateur.

Documents nécessaires pour l'inscription au niveau d'assurance 3

- ✓ Pour s'inscrire au niveau d'assurance 3 :
    - la photo de l'utilisateur final doit apparaître sur toutes ses pièces d'identité;
    - une copie de la pièce d'identité doit être conservée au dossier;
    - l'utilisateur final doit signer son formulaire d'inscription à la main.
- ✓ L'autorité locale d'enregistrement doit conserver une copie de chaque demande d'inscription des mandataires et des fournisseurs de services électroniques ayant accès à [la solution de DSE]. {3.1.2}

Suspension

- ✓ Le dépositaire de renseignements sur la santé peut suspendre un compte si :
    - o des renseignements découverts ou révélés portent raisonnablement à croire que l'information, la documentation ou tout autre élément soumis ou action posée durant le processus d'inscription était trompeur, faux ou frauduleux;
    - o un utilisateur final ne s'est pas conformé aux politiques, aux normes et aux ententes de la fédération ou aux conditions de tout service fédéré;
    - o la suspension est demandée par un fournisseur d'identité ou un utilisateur final pour quelque raison que ce soit (p. ex., un congé). {Normes au sujet des prestataires qui assurent la gestion fédérée de l'identité : 2.1.1}
- ✓ Un compte suspendu par un dépositaire de renseignements sur la santé en raison de présentation d'information trompeuse, fausse ou frauduleuse ne doit pas être utilisé ou réactivé à moins que l'on confirme que l'information, la documentation ou tous autres faits importants pertinents sont vrais, justes et complets. {Normes au sujet des prestataires qui assurent la gestion fédérée de l'identité : 2.1.3}
- ✓ Le fournisseur d'identité doit noter les raisons de la suspension et toutes actions entreprises par la suite, y compris l'enquête, et conserver cette information dans un dossier. {2.1.4}

Révocation

- ✓ Le dépositaire de renseignements sur la santé doit révoquer l'accès au compte d'un utilisateur final si :
    - o la personne n'a plus besoin du compte (p. ex., en cas de décès, de démission ou de retraite);
    - o le compte visé existe en double;
    - o l'information, la documentation ou tout autre élément fourni ou action posée lors de l'inscription était trompeur, faux ou frauduleux;
    - o l'identité a été compromise de quelque façon que ce soit (p. ex., vol d'identité);
    - o l'utilisateur final en fait la demande. {Normes au sujet des prestataires qui assurent la gestion fédérée de l'identité : 2.2.1}
- ✓ Le fournisseur d'identité doit noter les raisons de la révocation et toutes actions entreprises par la suite, dont l'enquête, et conserver cette information dans un dossier. {Normes au sujet des prestataires qui assurent la gestion fédérée de l'identité : 2.2.2}

Réinscription

- ✓ Une fois que leur accès à [la solution de DSE] a été révoqué, les mandataires et les fournisseurs de services électroniques doivent se réinscrire pour ravoir accès à [la solution de DSE]. {2.3}

- ✓ Pour connaître le processus de réinscription des mandataires et des fournisseurs de services électroniques ayant accès à [la solution de DSE], consulter l'*Annexe D : Inscription d'un mandataire ou d'un fournisseur de services électroniques ayant accès à* . {2.4}

Critères d'admissibilité

- ✓ La personne légalement responsable doit choisir des personnes, des groupes ou des titulaires de postes qui ont le pouvoir d'agir à titre d'approbateurs. {3}

- ✓ L'approbateur ne doit accorder accès aux composantes cliniques de [la solution de DSE] qu'aux mandataires 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 qui peuvent être déclarés comme des mandataires ayant ce but :

  - o les professionnels de la santé reconnus qui voient des patients.
  - o les résidents qui prodiguent des soins aux patients.
  - o le personnel administratif qui sort les dossiers pour les médecins.
  - o les commis d'unité qui examinent les résultats pour déceler le trouble du patient pour les médecins.

- ✓ L'approbateur ne doit accorder l'accès aux composants administratifs de [la solution de DSE] qu'aux mandataires et aux fournisseurs de services électroniques qui en ont besoin pour la raison suivante :

  - o offrir 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, administrateurs de système, mandataires et fournisseurs de services électroniques). Ces derniers ne doivent pas avoir accès aux fonctions destinées aux personnes qui dispensent des soins de santé ou qui aident à le faire (comme les cliniciens).

  Par exemple, les administrateurs de système peuvent demander accès à la liste de gestion des files d'erreurs pour corriger et traiter les messages, les responsables de la protection de la vie privée, aux rapports sur la confidentialité pour produire des rapports de vérification, et les spécialistes de mise en correspondance des données, aux fonctions terminologiques de mise en correspondance de la terminologie et des codes. Ces personnes ne doivent pas avoir accès aux fonctions destinées à ceux qui dispensent des soins de santé ou qui aident à le faire (c.-à-d. les cliniciens).

- ✓ Les approbateurs ne doivent pas donner accès à [la solution de DSE] si quelqu'un en fait la demande pour d'autres fins que celles de dispenser ou d'aider à dispenser des soins de santé, c'est-à-dire : {2.8}
    - pour la planification, l'évaluation ou la surveillance de programme;
    - pour la gestion du risque ou d'erreurs;
    - pour l'amélioration de la qualité des soins, des programmes et des services;
    - pour la formation (à moins qu'il s'agisse d'un étudiant ou d'un résident qui a besoin des accès pour prodiguer des soins);
    - pour le traitement des paiements.
- ✗ L'approbateur ne doit pas donner accès à [la solution de DSE] pour des fins de recherche.
- ✓ Si un mandataire ou un fournisseur de services électroniques a plus d'une fonction (p. ex., à la fois clinicien et gestionnaire des risques), l'approbateur peut lui donner accès à [la solution de DSE] à des fins de collecte de renseignements personnels sur la santé pour dispenser ou aider à dispenser des soins de santé, et doit s'assurer que l'utilisateur final soit au courant de ses autorisations et de ses obligations.

Norme sur les réseaux et les opérations

(✓) : À faire

Zones réseau

- ✓ Les dépositaires de renseignements sur la santé devraient créer des zones de réseau et les gérer de manière à tenir compte des divers environnements informatiques. La séparation des réseaux peut, entre autres, se faire en fonction des facteurs suivants : {1.3}
    - le type d'information transmis sur le réseau; {1.3.1}
    - le niveau d'assurance requis. {1.3.2}
- ✓ Les dépositaires de renseignements sur la santé devraient contrôler le trafic entre les zones de réseau en utilisant une passerelle de sécurité aux limites des zones. {1.4}

Passerelles de sécurité

- ✓ Les dépositaires de renseignements sur la santé devraient mettre sur pied un processus visant à réexaminer la configuration des passerelles de sécurité au moins une fois par année. Ce processus devrait englober les points suivants : {1.6}
    - l'examen de l'ensemble de règles des passerelles de sécurité; {1.6.1}
    - la suppression des règles désuètes ou inutiles; {1.6.2}
    - la correction des règles conflictuelles; {1.6.3}
    - la suppression des doublons et des éléments inutilisés (p. ex., réseaux ou systèmes informatiques). {1.6.4}

Protection contre les programmes malveillants

- ✓ Des logiciels de détection de programmes malveillants ou de réparation, ou des solutions équivalentes, devraient être mis en place dans les outils, les processus et les postes de travail approuvés par les dépositaires de renseignements sur la santé pour les protéger des programmes malveillants. D'autres solutions comme 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 peuvent être mises en place. Toute question quant à la possibilité de recourir à une autre solution doit être adressée au chef de la sécurité de [la solution de DSE] qui pourrait avoir à la présenter au Comité ConnexonSécurité. {1.20}

- ✓ Les dépositaires de renseignements sur la santé devraient garder leurs logiciels de détection de programmes malveillants ou de réparation à jour. {1.22}

Norme sur la gestion des menaces et des risques

(✓) : À faire

- ✓ Les dépositaires de renseignements sur la santé peuvent demander les sommaires des résultats des évaluations de la menace et des risques (EMR) de [la solution de DSE]. {1.3}

- ✓ Lorsqu'un dépositaire de renseignements sur la santé reçoit les résultats d'une EMR de l'équipe de [la solution de DSE], il doit restreindre l'accès à ces résultats et à tout document connexe et veiller à ce qu'ils soient traités de manière sécuritaire. {1.4}

Références

Politiques et normes sur les DSE de cyberSanté Ontario

- Politique de sécurité de l'information
- Norme d'utilisation acceptable des données et des technologies de l'information
- Norme sur le contrôle de l'accès aux systèmes et les processus de gestion d'identité connexes
- Norme sur les fournisseurs d'identités et Manuel de procédures relatives à l'admissibilité
- Norme sur la continuité des activités
- Norme sur la cryptographie
- Norme sur les fournisseurs de services électroniques
- Norme sur la gestion des incidents de sécurité de l'information
- Norme sur la gestion de l'information et des éléments d'actif
- Norme sur les réseaux et les opérations
- Norme sur la journalisation de sécurité et la surveillance
- Norme sur le cycle de développement de systèmes
- Norme sur la sécurité matérielle
- Norme sur la gestion des menaces et des risques
- Politique de confidentialité – Dossier de santé électronique

Annexes

Annexe A : Algorithmes cryptographiques approuvés

Algorithmes	Longueur minimale de la clé	Utilisation appropriée
Algorithmes à clé symétrique		

AES (Norme de chiffrement avancé)	128 bits	Chiffrement de données :
		• Clé de session
		• Stockage
		  ○ Sauvegarde
		  ○ Archives
			Chiffrement de clés :
			• Clé de session
			• Stockage
			  ○ Sauvegarde
			  ○ Archives

Skipjack	80 bits et 32 itérations	Chiffrement de données :
		• Clé de session
		• Stockage
		  ○ Sauvegarde
		  ○ Archives, moins de 5 ans	

Triple DES	112 bits	Chiffrement de données :
		• Clé de session
		• Stockage
		  ○ Sauvegarde
		  ○ Archives
			Chiffrement de clés :
			• Clé de session
			• Stockage
			  ○ Sauvegarde
			  ○ Archives

Algorithmes à clé asymétrique			

À courbe elliptique	160 bits	Chiffrement de données :
		• Clé de session
		• Stockage
		  ○ Sauvegarde
		  ○ Archives
		Signature numérique
			Chiffrement de clés :
			• Clé de session
			• Stockage
			  ○ Sauvegarde
			  ○ Archives
			Création d'une clé de session

RSA	2 048 bits	Chiffrement de données :
		• Clé de session
		• Stockage
		  ○ Sauvegarde
		  ○ Archives
		Signature numérique
			Chiffrement de clés :
			• Clé de session
			• Stockage
			  ○ Sauvegarde
			  ○ Archives
			Création d'une clé de session

Code d'authentification de message et algorithme de hachage			
AES MAC	128 bits	Authentification du message	
MD5[3]	128 bits et 16 itérations	Authentification du message et empreinte numérique	
SHA-1[4]	Sans objet	Authentification du message et empreinte numérique	

[3] Aucun *nouveau* code d'authentification de message et algorithme de hachage ne doivent être fondé sur l'algorithme MD5.
[4] Aucun *nouveau* code d'authentification de message et algorithme de hachage ne doivent être fondé sur l'algorithme SHA-1.

SHA-2	Sans objet	Authentification du message et empreinte numérique
Triple DES MAC	112 bits	Authentification du message
Signatures numériques		
DSA (algorithme de signature numérique)	1 024 bits	Signature numérique
DSA à courbe elliptique	160 bits	Signature numérique
RSA DSA	2 048 bits	Signature numérique
Certificats numériques		
Conforme au certificat X.509 v3	Sans objet	Mise en relation d'une clé publique à une entité précise.
Algorithmes de transport et d'agrément de clé		
Diffie-Hellman	1 024 bits	Création d'une clé de session numérique
Diffie-Hellman à courbe elliptique	160 bits	Création d'une clé de session numérique
Protocoles de chiffrement		
TLS versions 1.1 et suivantes	Sans objet	Protocole pour authentifier et chiffrer les communications des parties authentifiées.

Annexe B : Cote de gravité et de priorité des incidents

Cote de gravité

Gravité	Catégories et descriptions	Délais maximaux recommandés		
		Tri	Intervention	Retour à la normale
1	**Critique** • Site essentiel indisponible ou plusieurs sites indisponibles. • Perte de service posant d'importants risques pour les dépositaires de renseignements sur la santé participants. • Risque pour la sécurité de la santé publique, la protection de la vie privée ou la sécurité. • Conséquences graves touchant de nombreux systèmes internes ou externes, p. ex., contamination à grande échelle par un logiciel malveillant. Intervention et remise en service immédiate – mobilisation générale.	30 min	6 h	72 h
2	**Élevée** • Un seul site essentiel indisponible. • Perte de services non essentiels • Service de dépannage indisponible • Échec des mesures correctives • Dégradation du service touchant les dépositaires de renseignements sur la santé. Intervention et remise en service le plus rapidement possible – dans un délai d'un jour ouvrable.	2 h	12 h	24 h
3	**Moyenne** • Ralentissement d'une application ou d'un composant matériel. • Problèmes techniques ou fonctionnels mineurs. • Défaillance de l'application ou du composant touchant un seul client. Retour à la normale au cours des jours ouvrables suivants.	4 h	36 h	48 h
4	**Faible** • Conséquences négligeables, problème non urgent ou solutions de rechange existantes. Remise en service dans un délai d'une semaine.	24 h	36 h	15 jours

Cotes de priorité

Type d'incident	Cote de priorité	
	P2	P1
Contrôle des accès : Réservé aux incidents liés à la sécurité pouvant compromettre le contrôle des accès.		
Compromission d'un compte privilégié Par exemple, un identifiant privilégié (administrateurs du système, de la base de données ou du pare-feu) semble mener des activités ou afficher des comportements inhabituels (connexions inexpliquées ou accès inexpliqués à certains dossiers).	**X**	
Détection d'une opération d'hameçonnage visant les utilisateurs privilégiés Par exemple, de nombreux courriels suspects ciblant des utilisateurs bénéficiant d'un accès privilégié.	**X**	
Sécurité des biens : Incidents entraînant la perte ou le vol de biens, et attaque des biens causant l'interruption du service.		
Perte d'un support de données non chiffrées Par exemple, la perte d'une clé USB non chiffrée contenant des données sensibles.	**X**	
Détection d'une attaque par déni de service contre un bien essentiel Par exemple, une attaque par déni de service a été lancée contre un serveur hébergeant des applications d'affaires essentielles.	**X**	
Sécurité des données : Incidents menaçant la confidentialité des données.		
Accès à un volume de données exceptionnellement élevé sur un ou des serveurs hébergeant des données essentielles ou des applications qui traitent ou stockent des données essentielles Par exemple, l'alarme d'un système est déclenchée en raison du transfert d'un volume élevé de données (non lié à leur sauvegarde) en dehors des heures normales de travail.	**X**	
Détection d'un logiciel malveillant ou d'un virus – conséquences importantes Par exemple, une alarme est déclenchée lorsque la présence d'un virus est détectée.	**X**	
Intégrité du système et des données : Incidents liés à la compromission potentielle de l'intégrité des données et des systèmes.		
Atteinte importante à la protection des données entraînant une couverture médiatique Par exemple, une atteinte importante à la protection des données qui attire l'attention des médias.		**X**
Échec répété de la sauvegarde sur bande Par exemple, la sauvegarde sur bande a échoué lors des cinq dernières tentatives.	**X**	

Annexe C : Contenu du rapport d'incident

Les renseignements suivants doivent être intégrés au rapport d'incident lié à la sécurité de l'information.

1. Coordonnées du mandataire ou du fournisseur de services électroniques ayant signalé l'incident ET du responsable ou de l'équipe d'intervention
    - Nom
    - Unité (p. ex., service, division, équipe) (le cas échéant)
    - Courriel
    - Numéro de téléphone
    - Emplacement (p. ex., adresse postale, édifice et numéro de salle)
2. Détails sur l'incident
    - Date et heure auxquelles l'incident a été découvert.
    - Estimation de la date et de l'heure à laquelle l'incident a commencé.
    - Numéro du billet d'incident.
    - Type d'incident (p. ex., déni de service, programme malveillant, accès non autorisé, utilisation inappropriée).
    - Emplacement physique de l'incident (p. ex., ville).
    - État actuel de l'incident (p. ex., attaque toujours en cours).
    - Source ou cause de l'incident (si connue), y compris noms d'hôte et adresses IP.
    - Description de l'incident (p. ex., comment il a été détecté et ce qui s'est produit).
    - Description des ressources touchées (p. ex., réseaux, hôtes, applications ou données), y compris noms d'hôte, adresses IP et fonction des systèmes d'information.
    - Système d'exploitation, version et niveau du correctif.
    - Logiciel antivirus : installé, activé et à jour (oui ou non).
    - Facteurs atténuants
    - Estimation des répercussions techniques de l'incident (p. ex., suppression des données, panne du système ou applications indisponibles).
    - Mesures prises par le mandataire ou le fournisseur de services électroniques ayant signalé l'incident (p. ex., éteindre l'ordinateur hôte ou déconnecter l'hôte du réseau).
    - Autres organismes joints (p. ex., fournisseur du logiciel).
    - Type d'information compromis (le cas échéant).

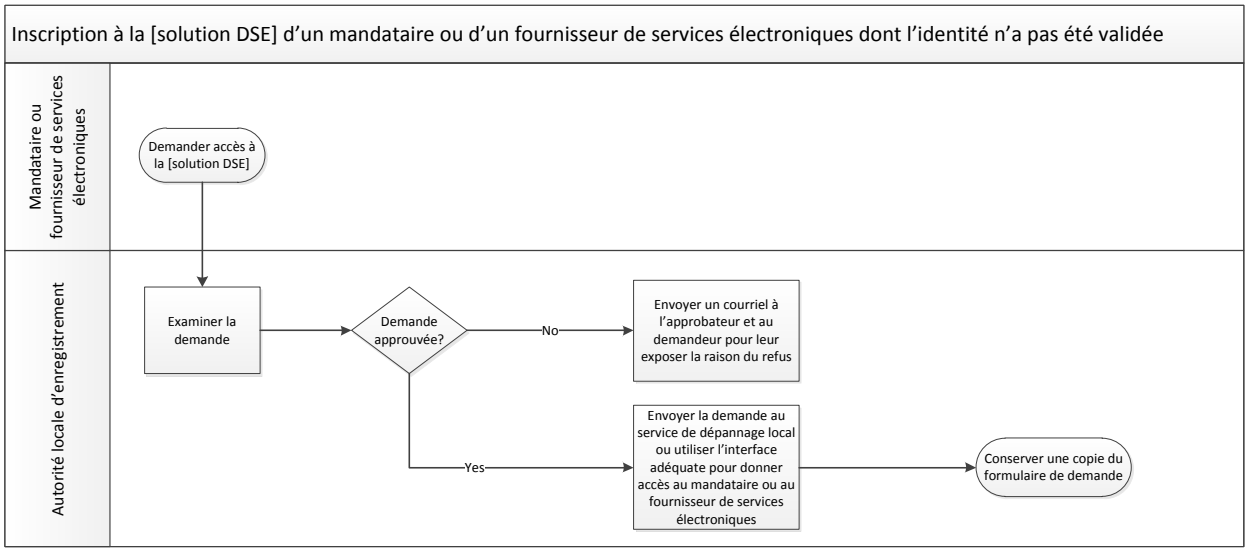
3. Commentaires généraux[5]
4. Résumé de l'incident
5. Coordonnées de toutes les parties concernées
6. Journal des interventions et des mesures d'atténuation prises par le chef ou l'équipe d'intervention
7. Liste des éléments de preuve recueillis
8. Cause de l'incident (p. ex., mauvaise configuration de l'application ou ordinateur hôte non corrigé)
9. Liste des activités de rétablissement recommandées et mises en œuvre
10. État actuel de l'intervention

[5] Recommandé, mais non obligatoire.

Annexe D : Inscription d'un mandataire ou d'un fournisseur de services électroniques ayant accès à [la solution de DSE]

Voici la marche à suivre pour inscrire un mandataire ou un fournisseur de services ayant accès à [la solution de DSE] lorsque l'identité de celui-ci a déjà été validée (p. ex., au cours du processus d'intégration du dépositaire de renseignements sur la santé). L'exemple ci-dessous s'applique à un processus sur papier. Toutefois, il est possible d'avoir recours à un flux de production électronique selon les pratiques des fournisseurs d'identité.

Étapes	Responsable	Description
1	Mandataire ou fournisseur de services électroniques	Demander accès à [la solution de DSE]. (Les dépositaires de renseignements sur la santé peuvent déterminer la manière de déposer une demande, par exemple, à l'aide d'une demande de service ou en envoyant un courriel directement à l'autorité locale d'enregistrement.) Les demandes devraient au moins comprendre les renseignements suivants sur le mandataire ou le fournisseur de services électroniques : • nom complet, • poste ou titre de l'emploi, • nom d'utilisateur, • preuve de l'approbation de l'approbateur, • raison justifiant l'accès.
2	Autorité locale d'enregistrement	Examiner la demande et la traiter si toute l'information nécessaire a été fournie.
3	Autorité locale d'enregistrement	En cas d'approbation • Envoyer la demande au service de dépannage local ou se servir de l'interface adéquate pour donner les accès à [la solution de DSE] au mandataire ou au fournisseur de services électroniques. En cas de refus • Envoyer un courriel à l'approbateur et au mandataire ou au fournisseur de services électroniques pour leur expliquer pourquoi la demande a été refusée. Conserver une copie du formulaire de demande.


Inscription à la [solution DSE] d'un mandataire ou d'un fournisseur de services électroniques dont l'identité n'a pas été validée
Mandataire ou fournisseur de services électroniques
Demander accès à la [solution DSE]
Autorité locale d'enregistrement
Examiner la demande
Demande approuvée?
No
Envoyer un courriel à l'approbateur et au demandeur pour leur exposer la raison du refus
Yes
Envoyer la demande au service de dépannage local ou utiliser l'interface adéquate pour donner accès au mandataire ou au fournisseur de services électroniques
Conserver une copie du formulaire de demande

Annexe E : Inscription d'un mandataire ou d'un fournisseur de services électroniques à [la solution de DSE] lorsque son identité n'a PAS déjà été validée

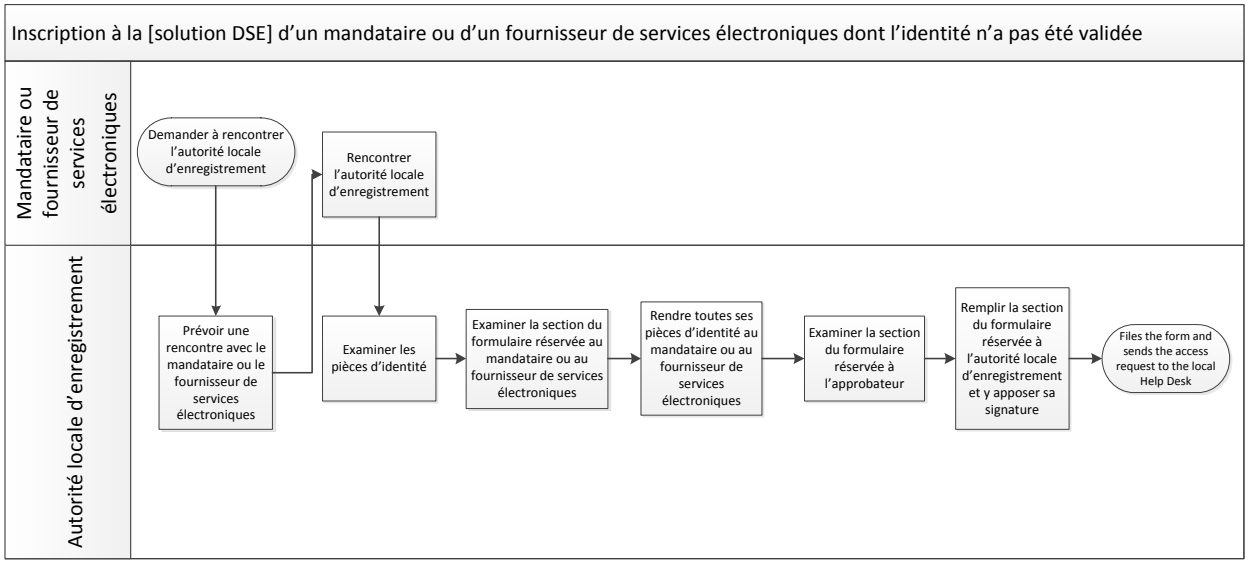
Voici la marche à suivre pour inscrire un mandataire ou un fournisseur de services à [la solution de DSE] lorsque l'identité de celui-ci n'a PAS déjà été validée. L'exemple ci-dessous s'applique à un processus sur papier. Toutefois, il est possible d'avoir recours à un flux de production électronique selon les pratiques des fournisseurs d'identité.

Étape	Responsable	Description
1	Mandataire ou fournisseur de services électroniques	Demander à rencontrer l'autorité locale d'enregistrement.
2	Autorité locale d'enregistrement	Prévoir une rencontre avec le mandataire ou le fournisseur de services électroniques.
3	Mandataire ou fournisseur de services électroniques	Apporter le *Formulaire d'enregistrement et d'inscription à [la solution de DSE] de l'utilisateur final* (voir l'annexe F) rempli et signé à la rencontre en personne avec l'autorité locale d'enregistrement, ainsi que ses documents (p. ex., pièces d'identité, permis et attestations). D'autres processus peuvent être utilisés, à condition que des mesures de sécurité adéquates soient en place.
4	Autorité locale d'enregistrement	Examiner les pièces d'identité et confirmer qu'elles sont : • originales, authentiques et valides; • conformes aux exigences pour obtenir le niveau d'assurance 2, soit[6] : o au moins une preuve provient de la liste de pièces d'identité principales (voir l'*Annexe G : Pièces d'identité acceptées*); o la seconde provient de la liste de pièces d'identité principales ou secondaires (voir l'*Annexe G : Pièces d'identité acceptées*); o au moins une pièce d'identité avec photo; o les deux pièces d'identité comportent le nom de la personne. • utilisées par le titulaire légitime de la carte (c.-à-d., la photo et les renseignements personnels qui y figurent sont ceux de la personne présente). ***N. B. :*** Pour en savoir plus sur la manière de valider l'identité d'un mandataire ou d'un fournisseur de services électroniques, consulter l'*Annexe G : Pièces d'identité acceptées*. Remettre des documents de formation pertinents au mandataire ou au fournisseur de

[6] Pour obtenir la définition du niveau d'assurance 2, voir les normes de cyberSanté Ontario au sujet des prestataires qui assurent la gestion fédérée de l'identité (eHealth Ontario Federation - *Identity Provider Standard*).

		services électroniques.
5	Autorité locale d'enregistrement	Vérifier que les sections du formulaire réservées au mandataire ou au fournisseur de services électroniques sont complètes et que : • les deux pièces d'identité permettent de confirmer les principaux renseignements indicateurs nécessaires à l'inscription (soit, les nom et prénom officiels, le sexe et la date de naissance); • les deux pièces d'identité sont valides; • la première pièce d'identité figure sur la liste de pièces d'identité principales (voir l'*Annexe G : Pièces d'identité acceptées*), et que le type de document, son numéro et sa date d'expiration (le cas échéant) sont notés sur le formulaire; **N. B. :** Si un certificat de naissance de l'Ontario est utilisé comme document principal, noter le numéro du certificat sur le formulaire; • seul le type de document de la deuxième pièce d'identité est inscrit sur le formulaire, peu importe qu'il figure sur la liste de pièces d'identité principales ou secondaires (voir l'*Annexe G : Pièces d'identité acceptées*); • le mandataire ou le fournisseur de services électroniques a signé et daté le formulaire. ** N. B. : Lorsqu'une interaction directe ou en personne a eu lieu entre le fournisseur d'identité et la personne qui s'inscrit pour valider l'identité de cette dernière, ces étapes peuvent être omises. L'interaction directe (p. ex., l'entrevue d'embauche) n'a pas à servir strictement à valider l'identité de la personne, mais cette étape doit néanmoins être réalisée conformément aux exigences des normes.
6	Autorité locale d'enregistrement	Rendre toutes ses pièces d'identité au mandataire ou au fournisseur de services électroniques.
7	Autorité locale d'enregistrement	Vérifier que la section réservée à l'approbateur est complète et que : • l'approbateur est valide (c.-à-d., qu'il figure sur la liste des approbateurs ou des personnes légalement responsables); • l'approbateur a signé et daté le formulaire (ou donné son approbation d'une autre manière, par courriel par exemple); • le type de demande est sélectionné à la partie 2b (suspension, réinscription, révocation, nouvelle inscription).
8	Autorité locale d'enregistrement	Confirmer avoir examiné le formulaire et les pièces d'identité à l'appui en : • remplissant la section réservée à l'autorité locale d'enregistrement; • signant et datant le formulaire.

9	Autorité locale d'enregistrement	Verser le formulaire au dossier et envoyer une demande au service de dépannage local pour qu'il donne accès au mandataire ou au fournisseur de services électroniques à [la solution de DSE]. L'autorité locale d'enregistrement pourrait avoir directement accès au système pour accorder les droits d'utilisation.



Annexe F : Formulaire d'enregistrement et d'inscription à [la solution de DSE] de l'utilisateur final

Voici le formulaire pour inscrire un mandataire ou un fournisseur de services électroniques à [la solution de DSE]. L'exemple ci-dessous s'applique à un processus sur papier. Toutefois, il est possible d'avoir recours à un flux de production électronique selon les pratiques des fournisseurs d'identité.

Instructions
Utiliser ces formulaires pour inscrire un nouveau mandataire ou fournisseur de services électroniques à [la solution de DSE] **si** son identité n'a **pas** déjà été validée par le dépositaire de renseignements sur la santé conformément aux exigences de vérification de [la solution de DSE]. Le fournisseur d'identité pourrait avoir recours à un flux de production électronique, s'il dispose d'un tel processus. • L'autorité locale d'enregistrement doit rencontrer le demandeur afin de vérifier ses pièces d'identité. • Remplir tous les champs selon les indications. Les champs obligatoires sont marqués d'un astérisque (*). Indiquer « Ne s'applique pas » ou « S.O. » si un champ ne s'applique pas. • L'autorité locale d'enregistrement doit remplir la partie 3. • Une fois le formulaire rempli, l'autorité locale d'enregistrement peut inscrire le demandeur afin qu'il ait accès à [la solution de DSE]. • L'autorité locale d'enregistrement doit conserver une copie du formulaire rempli.

Partie 1 – Mandataire ou fournisseur de services électroniques			
1A – Renseignements sur le mandataire ou le fournisseur de services électroniques			
Formule d'appel (•) Dr ( ) Dre ( ) M. ( ) Mme	Titre de l'emploi* *(p. ex., directeur général ou directeur de l'information)*		
Prénom officiel*	Initiale du ou des autres prénoms	Nom officiel*	
Téléphone au travail* (*indiquer le poste*)		Adresse courriel professionnelle*	
Nom de l'organisme* *(p. ex., Réseau universitaire de santé)*		Nom du site ou de l'établissement *(p. ex., Hôpital ABC)*	
Adresse professionnelle* *(numéro et rue)*		Bureau/unité/étage	
Ville*	Province*	Code postal*	
Nom d'utilisateur ou identificateur d'utilisateur du système*	Date de la demande* *(aaaa/mm/jj)*		

1B – Pièces d'identité – *Section réservée à l'**autorité locale d'enregistrement.** Pour des raisons de confidentialité, rendre les pièces d'identité au mandataire ou au fournisseur de services électroniques, et ne **PAS** en faire de copies.*

Pièce d'identité 1* – *Pièce d'identité figurant sur la liste de pièces d'identité principales. La date d'expiration doit obligatoirement être consignée pour la première pièce d'identité, le cas échéant.*

Description de la pièce d'identité*	Numéro*	Date d'expiration* (*aaaa/mm/jj*)

Pièce d'identité 2* – *Pièce d'identité figurant sur la liste de pièces d'identité principales ou secondaires. Il n'est pas obligatoire d'inscrire le numéro du document et la date d'expiration.*

Description de la pièce d'identité

1C – Avis de collecte de renseignements – *Section réservée au mandataire ou au fournisseur de services électroniques à des fins d'approbation.*

Je confirme que les renseignements susmentionnés sont exacts. J'autorise la collecte, l'utilisation et la divulgation de mes renseignements personnels dans le cadre du processus d'inscription à [la solution de DSE].

Signature du mandataire ou du fournisseur de services électroniques*	Date* (*aaaa/mm/jj*)
_____	

Partie 2 – Renseignements sur l'approbateur

2A – Renseignements sur l'approbateur : La présente section doit être remplie par l'approbateur ou l'**autorité locale d'enregistrement** au nom de l'approbateur. Inscrire le nom de l'organisme, le nom de l'établissement et l'adresse seulement s'ils diffèrent de ceux du mandataire ou du fournisseur de services électroniques. Les coordonnées (c.-à-d. téléphone au travail ou adresse courriel) sont obligatoires.

Prénom*		Nom officiel*
Titre* (p. ex., directeur général ou directeur de l'information)	Téléphone au travail* (*indiquer le poste*)	Adresse courriel professionnelle*

☐ Adresse identique à celle du mandataire ou du fournisseur de services électroniques. *(Dans ce cas, il n'est pas obligatoire de remplir les autres champs d'adresse de la présente section.)*

Nom de l'organisme* *(p. ex., Réseau universitaire de santé)*	Nom du site ou de l'établissement *(p. ex., Hôpital ABC)*
Adresse professionnelle* *(numéro et rue)*	Bureau/unité/étage

Ville*	Province*	Code postal*

Partie 2b – Type de demande

Type de demande* : Nouvelle inscription

Rôle :		
* J'autorise l'inscription du mandataire ou du fournisseur de services électroniques à [la solution de DSE]. Signature de l'approbateur (Si l'autorisation est reçue d'une autre manière, voir les cases ci-dessous.) _____		Date (*aaaa/mm/jj*)
☐ Approbation de l'approbateur reçue d'une autre manière (p. ex., courriel, note de service ou télécopieur)	Préciser la manière :	

Partie 3 – Autorité locale d'enregistrement

3A – Renseignements sur l'autorité locale d'enregistrement – Section réservée à l'**autorité locale d'enregistrement.** Inscrire le nom de l'organisme, le nom de l'établissement et l'adresse seulement s'ils diffèrent de ceux du mandataire ou du fournisseur de services électroniques. Les coordonnées (c.-à-d. téléphone au travail ou adresse courriel) sont obligatoires.

Prénom*	Nom officiel*	
Téléphone au travail* (*indiquer le poste*)	Adresse courriel professionnelle*	
☐ Adresse identique à celle du mandataire ou du fournisseur de services électroniques. *(Dans ce cas, il n'est pas obligatoire de remplir les autres champs d'adresse de la présente section.)*		
Nom de l'organisme * *(p. ex., Réseau universitaire de santé)*	Nom du site ou de l'établissement *(p. ex., Hôpital ABC)*	
Adresse au travail* *(numéro et rue)*	Bureau/unité/étage	
Ville*	Province*	Code postal*
*Je confirme que j'ai examiné les pièces d'identité du mandataire ou du fournisseur de services électroniques ainsi que la présente demande d'inscription. Signature de l'autorité locale d'enregistrement (Si l'autorisation est reçue d'une autre manière, voir les cases ci-dessous.) _____		Date* (*aaaa/mm/jj*)

Annexe G : Pièces d'identité acceptées

La carte d'assurance sociale et la carte provinciale d'assurance-maladie ne constituent **PAS** des pièces d'identité acceptables.

Dans les colonnes « Photo » et « Date d'expiration », « Inconnu » signifie que le document pourrait comporter ou non une photo ou une date d'expiration selon sa provenance ou la version du document.

Pièces d'identité principales

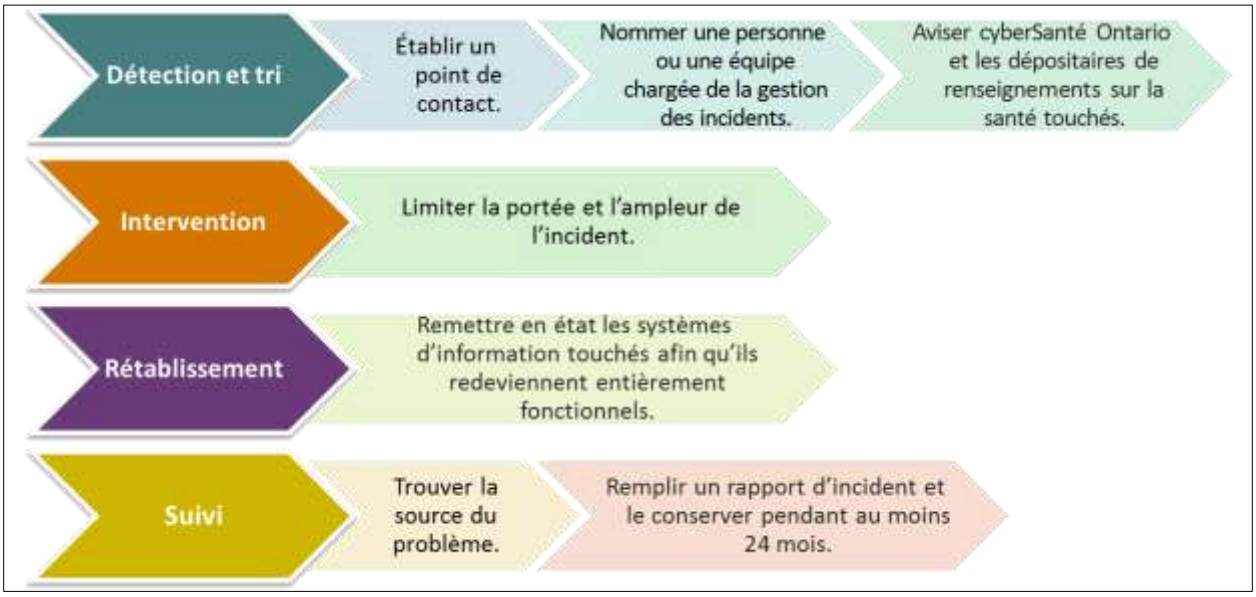
Pièces d'identité délivrées par le gouvernement	Photo	Date d'expiration
Permis de conduire (y compris les permis du système de délivrance graduelle)	Oui	Oui
Passeport canadien	Oui	Oui
Certificat de citoyenneté (document papier ou carte; mais pas les certificats commémoratifs)	Oui	Non
Acte de naissance délivré par une province ou un territoire du Canada	Non	Non
Certificat canadien d'enregistrement d'une naissance à l'étranger	Non	Non
Certificat canadien du statut d'indien ou carte de Métis	Oui	Non
Carte de résident permanent du Canada	Oui	Oui
Déclaration de naissance vivante d'une province canadienne (copie certifiée)	Non	Non
Certificat de naturalisation du Canada (document papier ou carte; mais pas les certificats commémoratifs)	Non	Non
Carte de citoyenneté délivrée par un État étranger où elles existent (p. ex., Mexique ou Europe)	Inconnu	Inconnu
Confirmation de résidence permanente (IMM 5292)	Non	Oui
CANPASS (Permis de passage de la frontière en région éloignée permettant au détenteur d'entrer au Canada à certains endroits isolés sans être obligé de se rendre à un point d'entrée, tant qu'il déclare les marchandises importées.)	Oui	Oui
NEXUS (Laissez-passer express disponible pour les personnes à faible risque ayant passé un contrôle de sécurité rigoureux [canadien et américain], comptant la prise d'empreintes digitales et de photo, ainsi qu'une entrevue individuelle avec les agents de l'immigration. Le laissez-passer doit être renouvelé tous les deux ans.)	Oui	Oui
Permis d'armes à feu	Oui	Oui
Permis d'armes à feu	Oui	Oui
Passeport valide délivré par une autorité étrangère	Oui	Oui
Pièce d'identité de demandeur du statut de réfugié d'Immigration, Réfugiés et Citoyenneté Canada	Oui	Oui
Carte-photo de l'Ontario	Oui	Oui

Pièces d'identité secondaires

Type de document	Date d'expiration?
Carte de Sécurité de la vieillesse	Non
Certificat délivré par un ministère ou un organisme gouvernemental, p. ex., certificat de mariage, de divorce ou d'adoption	Non
Lettre de la Section du statut de réfugié du Canada	Non
Autorisation d'emploi du Canada	Oui
Permis ministériel canadien	Oui
Visa d'immigrant canadien	Oui
Autorisation d'étude du Canada	Oui
Fiche relative au droit d'établissement (IMM 1000)	Oui
Attestation d'un changement de nom et preuve d'utilisation de l'ancien nom dans les 12 mois précédents.	Non
Document valide d'inscription à un ordre d'une profession de la santé, conformément à la *Loi de 1991 sur les professions de la santé réglementées.* Audiologie et orthophonie Podologie Chiropractie Hygiène dentaire Technologie dentaire Dentisterie Denturologie Diététique Massothérapie Technologie du laboratoire médical Technologie en radiation médicale Médecine Profession de sage-femme Soins infirmiers Ergothérapie Optique Optométrie Pharmacie Physiothérapie Psychologie Inhalothérapie	Inconnu
Permis ou carte de membre valide d'une association professionnelle, de n'importe quelle profession de la santé réglementée, notamment les suivantes : Association des sages-femmes de l'Ontario Denturist Association of Ontario Association des infirmières et infirmiers praticiens de l'Ontario Ontario Association of Medical Radiation Technologists Ontario Association of Naturopathic Doctors Ontario Association of Orthodontists Ontario Association of Speech-Language Association des infirmières et infirmiers de l'Ontario Ontario Opticians' Association Ontario Pharmacists' Association Ontario Physiotherapy Association Ontario Podiatric Medical Association Ontario Society of Chiropodists Ontario Society of Medical Technologists Association des infirmières et infirmiers	Inconnu

Type de document		Date d'expiration?
Pathologists and Audiologists Association chiropratique de l'Ontario Ontario Dental Association Association médicale de l'Ontario	autorisés de l'Ontario Registered Practical Nurses' Association of Ontario Société de la thérapie respiratoire de l'Ontario	
Carte d'employé fédéral, provincial ou municipal		Inconnu
Carte d'employé valide d'un organisme approbateur		Inconnu
Carte syndicale		Inconnu
Autre pièce d'identité fédérale, y compris des Forces canadiennes		Inconnu
Carte Plein air du ministère des Richesses naturelles et des Forêts		Inconnu
Carte d'identité judiciaire		Inconnu
Carte d'identité d'étudiant		Inconnu
Carte BYID (anciennement carte d'âge de la majorité)		Inconnu
Carte d'identité avec photo de l'Institut national canadien pour les aveugles (INCA)		Inconnu
Carte d'identité des corps de police		Inconnu
Carte d'identité délivrée sous le régime de la *Loi sur les droits des aveugles*		Inconnu

Annexe H : Processus de gestion des incidents de sécurité de l'information



Annexe I : Niveau d'assurance

Niveau d'assurance	Classification des renseignements	Description des niveaux d'assurance
1	Le niveau 1 est adéquat pour l'information « non classifiée » et est normalement associé à l'information publique et aux communications internes, soit les documents internes et les communications non classifiées servant généralement aux échanges entre le personnel. Si cette information était compromise, il est raisonnable de croire que cela n'entraînerait aucun dommage ni aucune perte pour les parties touchées; seules des mesures administratives seraient nécessaires pour corriger la situation. Le niveau d'assurance 1 est inadéquat pour l'accès aux **renseignements personnels sur la santé** ou aux **renseignements personnels.**	Aucune vérification de l'identité : La personne remet toute l'information d'identification nécessaire, celle-ci est automatiquement considérée comme valide. Aucune certification n'est nécessaire pour valider l'authenticité de la déclaration d'identité.
2	Le niveau 2 est adéquat pour l'information hautement confidentielle de cyberSanté Ontario et du secteur de la santé et l'information qui ne peut être utilisée que par certaines personnes autorisées. Si cette information était compromise, il est raisonnable de croire que cela causerait d'importants dommages ou d'importantes pertes financières pour la ou les parties touchées ou entraînerait des poursuites pour régler la situation.	Vérification de l'identité : L'identité d'une personne est validée dans le cadre d'un processus d'enregistrement contrôlé, et la déclaration d'identité est validée à l'aide de pièces d'identité et appuyée par certaines preuves contextuelles lorsque la situation s'y prête.
3	Le niveau 3 est adéquat pour l'information de nature extrêmement confidentielle à laquelle cyberSanté Ontario et le secteur de la santé accorde la plus haute importance. Cette information ne doit être utilisée que par les personnes désignées et autorisées. Pour déterminer si un niveau d'assurance 3 est nécessaire, l'organisme et les fournisseurs de services applicatifs doivent se demander si : ☐ les circonstances ou le contexte entourant l'accès à l'information et son utilisation nécessitent un processus de confirmation plus poussé que pour le niveau d'assurance 2.	Confirmation de l'identité : L'identité d'une personne est validée dans le cadre d'un processus d'enregistrement contrôlé, et la déclaration d'identité est validée et confirmée par une source faisant autorité (p. ex., l'émetteur de la pièce d'identité présentée).