Ontario Health

Politique de sécurité de l'information

Version: 2.8

Identificateur de document : 3541

Gestion du document

Date de la prochaine révision : Chaque année ou à la fréquence établie par le Comité ConnexionSécurité.

Historique des approbations

APPROBATEURS	DATE D'APPROBATION
Comité ConnexionSécurité	2017-02-21
Comité ConnexionSécurité	2018-03-26
Comité ConnexionSécurité	2019-07-04
Comité ConnexionSécurité	2021-03-18

Historique des modifications

NUMÉRO DE VERSION	DATE	RÉSUMÉ DES CHANGEMENTS	AUTEUR DES CHANGEMENTS
2.0	2013-12-23	Adoption de la version de novembre 2013 par le groupe de travail sur la protection de la vie privée et la sécurité de ConnexionRGT et examen.	Mark Carter
2.1	2014-08-20	Mise à jour à partir des commentaires formulés par les membres du Comité ConnexionSécurité. Ajout de la référence à la *Politique visant à garantir la conformité du DSE avec la Loi sur la confidentialité des renseignements personnels sur la santé* (en anglais), y compris les puces contextuelles.	Mark Carter
2.2	2014-09-09	Approbation de la politique à la réunion du Comité ConnexionSécurité du 9 septembre.	Mark Carter
2.3	2015-01-21	Harmonisation des libellés à la *Politique de contrôle des accès et de gestion de l'identité* (en anglais) conformément à la décision définitive de la 3e étape du Comité ConnexionSécurité.	Mark Carter
2.4	2015-10-19	Mise à jour des politiques pour refléter le changement de gouvernance. Le Comité directeur a été remplacé par l'organisme de surveillance compétent. Le Comité régional de protection de la vie privée et de sécurité ne participe plus au processus de décision en matière de dérogation. Les responsabilités en matière de gouvernance du comité ConnexionSécurité ont été ajoutées dans la section des rôles et responsabilités.	Mark Carter

NUMÉRO DE VERSION	DATE	RÉSUMÉ DES CHANGEMENTS	AUTEUR DES CHANGEMENTS
2.5	2017-02-21	Mise à jour des politiques afin d'incorporer les changements mis en œuvre lors du rafraîchissement 2017. La définition de « solution de DSE » a été ajustée. Plusieurs contrôles ont été reformulés afin d'inclure « participant » dans la solution de DSE.	Ravi Addepalli
2.6	16 mars 2018	Mise à jour de la norme afin d'inclure l'accès au DSE par les patients.	Geovanny Diaz
2.7	4 juillet 2019	Mise à jour de la politique pour ajouter la *Norme sur la gestion des menaces et des risques* et exiger des évaluations de sécurité des DSE.	Ravi Addepalli
2.8	2021-01-04	Examen du document avec des modifications mineures, mise à jour du cycle de révision tous les deux ans	Ana Fukushima

Politique de sécurité de l'information

Objectif

La présente vise à protéger la confidentialité, l'intégrité et la disponibilité de [la solution de DSE] et des renseignements personnels sur la santé stockés ou traités dans [la solution de DSE]. À cet effet, elle établit le cadre de gestion de la sécurité de l'information contenue dans [la solution de DSE] :

- en définissant les principes en matière de sécurité de l'information qui régissent :
    - les renseignements personnels sur la santé;
    - [la solution de DSE] et les systèmes d'information ou les technologies de l'information connectés à [la solution de DSE].
- en décrivant les rôles et les responsabilités visant à assurer l'application des principes énoncés dans la présente politique.

Portée

La présente politique s'applique aux responsables de [la solution de DSE], à ses mandataires, à ses fournisseurs de services électroniques et à [la solution de DSE], y compris la totalité des portails et des applications pour les patients.

Pour les dépositaires de renseignements sur la santé qui se connectent à [la solution de DSE] pour consulter, gérer ou traiter autrement des renseignements personnels sur la santé au moyen :

- **d'une technologie d'identification locale**, cette politique vise les éléments suivants :
    - L'infrastructure de gestion de l'identité et de contrôle de l'accès local des dépositaires de renseignements sur la santé (les « services d'identification ») qui sert à gérer l'authentification et les autorisations nécessaires pour accéder à [la solution de DSE] (p. ex., service d'émission de jeton de sécurité de [la solution de DSE] et Microsoft Active Directory Federation Services 2.0, etc.);
    - La connexion réseau directe au Portail de [la solution de DSE] pour les fournisseurs et aux fonctionnalités administratives, y compris les composantes du chemin de connexions (pare-feux, serveurs mandataires, etc.);
    - L'intégration du Portail de [la solution de DSE] pour les fournisseurs au système local d'information sur la santé ou aux applications de dossiers médicaux électroniques (DME) des dépositaires de renseignements sur la santé.
- **du service ONE® ID de Santé Ontario**, cette politique vise les éléments suivants :
    - La connexion réseau directe aux fonctionnalités administratives de [la solution de DSE], y compris les composantes du chemin de connexions (pare-feux, serveurs mandataires, etc.).

Pour les dépositaires de renseignements sur la santé qui, en plus de consulter l'information, créent ou saisissent des renseignements personnels sur la santé dans le Répertoire des données cliniques de [la solution de DSE] (les « établissements contributeurs »), la présente politique s'applique en outre aux éléments suivants :

- Les indicateurs de résultat des données de contribution qui fournissent des renseignements sur la santé utiles au Répertoire de données cliniques de [la solution de DSE];

- Les technologies de l'information et les processus servant à assurer la qualité des données soumises (p. ex., inventaire de la terminologie).

La présente politique ne s'applique pas aux dépositaires de renseignements sur la santé, à leurs mandataires ou à leurs fournisseurs de services électroniques qui n'utilisent pas [la solution de DSE].

Définitions

[la solution de DSE] : [la solution de DSE] et les systèmes de soutien 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.

[La solution de DSE] inclut les portails et les applications pour les patients (affiliés ou non à un dépositaire de renseignements sur la santé) qui facilitent l'accès du patient au DSE. Ces applications peuvent être :

- Commandées par le fournisseur (le fournisseur facilite la communication avec le patient)
- Fournies directement au patient (le patient a un accès direct au DSE)
- Commandées par le patient (le patient délègue l'accès à un mandataire spécial ou à d'autres délégués, p. ex., un membre de la famille ou un médecin).

Équipe de [la solution de DSE] : également appelée bureau de l'équipe; comprend des agents et des fournisseurs de services électroniques qui soutiennent [la solution de DSE], y compris les activités, les initiatives et les processus associés à la protection de la vie privée et à la sécurité.

Équipe des opérations en matière de protection de la vie privée et de sécurité de Santé Ontario : L'Équipe des opérations en matière de protection de la vie privée et de sécurité de Santé Ontario se compose 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.

Comité de protection de la vie privée et de sécurité : Le Comité de protection de la vie privée et de sécurité est formé de mandataires des dépositaires de renseignements sur la santé participants et appuie la structure de gestion de la confidentialité et de la sécurité de l'information.

Organisme de surveillance compétent : L'organisme de surveillance compétent est formé de cadres supérieurs qui supervisent tous les aspects liés à [la solution de DSE]. Voir la section intitulée Structure de la politique de gouvernance ci-dessous.

Comité ConnexionSécurité (CCS) : La tribune provinciale sur la sécurité formée de représentants supérieurs de la sécurité provenant des régions et de Santé Ontario. C'est l'organisme décisionnaire responsable de l'établissement d'un cadre de gouvernance de la sécurité de l'information fonctionnel et utile pour les organisations participant aux DSE.

Fournisseur de services électroniques : Une 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.

Sécurité de l'information : Protection des renseignements, des systèmes d'information et des technologies de l'information contre les accès non autorisés et contre la collecte, l'utilisation, la divulgation, le transfert, la perturbation, la modification et l'élimination non autorisés de données.

Système d'information : Ensemble indépendant de technologies de l'information servant à la collecte, au traitement, à la tenue à jour, à l'utilisation, à la divulgation ou à l'élimination de données.

Point(s) d'accès de données de contribution : La technologie et les processus afférents qui produisent des données versées au Répertoire de données cliniques ou interrogées pour obtenir un aperçu de la situation clinique. Habituellement, il s'agit de systèmes d'information (p. ex., système d'information d'hôpital, de laboratoire, de clinique, etc.) ayant une connexion directe à [la solution de DSE] afin d'accéder aux données cliniques.

Services d'identification : Technologie et tout service de soutien, politique, processus et procédure afférent exploité pour créer, conserver, sécuriser, valider, vérifier et gérer l'identification électronique à [la solution de DSE].

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.

Évaluation des risques et des menaces : Évaluation indépendante consistant à analyser le degré de vulnérabilité des logiciels, les menaces potentielles et les risques qui en découlent.

Évaluation de la sécurité des DSE : Auto-évaluation de la sécurité en fonction des normes de sécurité des DSE.

Doit/doivent : Ces termes indiquent des exigences non facultatives.

Préférable ou devrait/devraient : Ces termes sont 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.

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

Politique

1. Principles

Utilisation acceptable des données et des technologies de l'information

1.1. Les responsables 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 ayant accès à [la solution de DSE].

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

Formation sur la sécurité de l'information

1.2. Les responsables 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 de [la solution de DSE] à comprendre leurs obligations dans ce domaine.

Consultez à ce sujet la *Privacy and Security Training Policy.*

Gestion des risques

1.3. Les responsables de [la solution de DSE] doivent évaluer les risques associés à la sécurité de l'information pour [la solution de DSE] et réaliser une évaluation de la sécurité des DSE, en faire un suivi et atténuer les risques ou les accepter officiellement.

1.4. Les dépositaires de renseignements sur la santé devraient évaluer les risques associés à la sécurité de l'information pour les services d'identification et les indicateurs de résultat de données de contribution.

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

Cryptographie

1.5. Les responsables de [la solution de DSE] doivent chiffrer la solution de connexion pour protéger la confidentialité et l'intégrité des renseignements personnels sur la santé, le cas échéant, et vérifier l'identité des auteurs des communications.

1.6. Les dépositaires de renseignements sur la santé doivent chiffrer leurs systèmes d'information pertinents pour protéger la confidentialité et l'intégrité des renseignements personnels sur la santé accessibles par l'intermédiaire de [la solution de DSE].

Consultez à ce sujet la *Norme sur la cryptographie*.

Gestion de l'information et des biens

1.7. Les responsables de [la solution de DSE] doivent 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 protéger la confidentialité, l'intégrité et la disponibilité de ces données en format papier et électronique tout au long de leur cycle de vie.

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

Contrôle d'accès et gestion de l'identité pour l'accès au niveau du système

1.8. Les responsables de [la solution de DSE] et les dépositaires de renseignements sur la santé doivent instaurer des mesures de contrôle appropriées pour gérer l'accès et l'identité des utilisateurs et des systèmes d'information qui se connectent à [la solution de DSE]. Ces mesures de contrôle doivent permettre :

1.8.1. de définir les responsabilités relatives à la sécurité de l'information de tous les utilisateurs de [la solution de DSE];

1.8.2. de veiller à ce que seules les personnes autorisées aient accès à [la solution de DSE] et d'assurer la responsabilisation individuelle;

1.8.3. de veiller à ce que seuls les systèmes d'information autorisés aient accès à [la solution de DSE];

1.8.4. de fournir aux utilisateurs ou aux systèmes d'information autorisés seulement les droits nécessaires à l'exécution de leurs tâches, sans leur donner la possibilité d'outrepasser leurs pouvoirs.

Consultez à ce sujet la *Norme sur le contrôle de l'accès aux systèmes et les processus de gestion d'identité connexes* et la *Norme sur les fournisseurs d'identités fédérées*

Journalisation et surveillance

1.9. Les responsables de [la solution de DSE] doivent consigner et surveiller tous les accès à [la solution de DSE], ainsi que les activités des systèmes d'information dans la solution.

1.10. Les dépositaires de renseignements sur la santé doivent consigner et surveiller tous leurs accès au Portail de [la solution de DSE] pour les fournisseurs et ceux de leurs mandataires ou fournisseurs de services électroniques, ainsi que les points d'accès aux données de contribution.

Consultez à ce sujet la *Norme sur la journalisation de sécurité et la surveillance*

Réseau et fonctionnement

1.11. Les responsables de [la solution de DSE] 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 de [la solution de DSE].

1.12. 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 d'identification et des points d'accès aux données de contribution.

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

Cycle de développement de système

1.13. Les responsables de [la solution de DSE] doivent définir les exigences au chapitre du développement de systèmes d'information et de la gestion du changement, et veiller à ce que les activités de développement visant [la solution de DSE] soient conformes à ces exigences.

1.14. Les dépositaires de renseignements sur la santé devraient définir les exigences au chapitre du développement de systèmes d'information et de la gestion du changement, et veiller à ce que les activités de développement visant les services d'identification et les points d'accès aux données de contribution soient conformes à ces exigences.

Consultez à ce sujet la *Norme sur le cycle de développement de systèmes*

Fournisseurs de services électroniques

1.15. Les responsables de [la solution de DSE] doivent vérifier si les fournisseurs de services électroniques qui auront accès à la solution, ou qui gèrent ou soutiennent cette solution, 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. Les dépositaires de renseignements sur la santé doivent vérifier si les fournisseurs de services électroniques qui auront accès aux services d'identification ou aux points d'accès aux données de contribution, 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.

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

Sécurité matérielle

1.17. Les responsables de [la solution de DSE] doivent mettre en place des mesures de contrôle visant à protéger [la solution de DSE] contre les risques d'accès physique non autorisé et de dommages à l'environnement.

1.18. Les dépositaires de renseignements sur la santé doivent mettre en place des mesures de contrôle visant à protéger les services d'identification et les points d'accès aux données de contribution contre les risques d'accès physique non autorisé et de dommages à l'environnement.

Consultez à ce sujet la *Norme sur la sécurité matérielle*

Continuité des activités

1.19. Les responsables de [la solution de DSE] doivent instaurer les procédures requises pour veiller à ce que [la solution de DSE] :

1.19.1. demeure accessible, en particulier en cas de catastrophe;

1.19.2. puisse être récupéré en cas de perturbation du fonctionnement.

1.20. Les dépositaires de renseignements sur la santé devraient élaborer des plans de continuité des activités pour veiller à ce que les services d'identification et les points d'accès aux données de contribution :

1.20.1. demeurent accessibles, en particulier en cas de catastrophe;

1.20.2. puisse être récupéré en cas de perturbation du fonctionnement.

Consultez à ce sujet la *Norme sur la continuité des activités.*

Gestion des incidents de sécurité de l'information

1.21. Les responsables 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 [la solution de DSE] ou de l'information de [la solution de DSE], et ce, tout en réduisant leur incidence et les risques que la situation se reproduise.

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

Assurance de protection de la vie privée et de sécurité

1.22. 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.

1.23. Les responsables de [la solution de DSE] 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'évaluations d'incidence sur la protection de la vie privée, d'évaluations de risque, d'auto-évaluations de l'état de préparation à la protection de la vie privée et à la sécurité, d'auto-évaluations des activités opérationnelles de protection de la vie privée et de sécurité, et de mesures d'audit, de contrôle et d'assurance de la conformité des mandataires, des fournisseurs de services électroniques et des tierces parties.

Consultez à ce sujet la *Privacy and Security Harmonized Assurance Policy (en anglais).*

2. Dérogations aux exigences en matière de sécurité de l'information

2.1. politiques, les normes ou les documents à l'appui relatifs à la sécurité de l'information de [la solution de DSE] doit être approuvée par l'organisme de surveillance compétent.

2.2. Les demandes de dérogation aux exigences en matière de sécurité de l'information doivent être évaluées par l'Équipe des opérations en matière de protection de la vie privée et de sécurité de Santé Ontario, puis par l'organisme de surveillance compétent aux fins d'approbation.

2.3. Les responsables de [la solution de DSE] doivent consigner toutes les demandes de dérogation aux exigences en matière de sécurité de l'information.

2.4. Les dérogations peuvent être de n'importe quelle durée. Cependant, l'Équipe des opérations en matière de protection de la vie privée et de sécurité de Santé Ontario doit les examiner au moins tous les deux ans pour vérifier si le niveau de risque s'est accru ou si de nouveaux risques sont apparus. Si c'est le cas, la dérogation doit alors être soumise de nouveau à l'approbation de l'organisme de surveillance compétent.

2.5. L'organisme de surveillance compétent a le droit d'annuler les dérogations aux exigences en matière de sécurité de l'information. Il doit toutefois accorder au moins six mois aux participants pour leur laisser le temps de se conformer à la politique.

Consultez à ce sujet l'*Annexe A : Demandes de dérogation aux exigences en matière de sécurité de l'information*.

3. Rôles et responsabilités

Comité de protection de la vie privée et de sécurité

1.24. Le Comité de protection de la vie privée et de sécurité doit :

1.24.1. passer en revue, commenter et entériner toutes les politiques et les normes liées à la sécurité de l'information de [la solution de DSE];

Organisme de surveillance compétent

1.25. L'organisme de surveillance compétent doit :

1.25.1. approuver les politiques et les normes relatives à la sécurité de l'information;

1.25.2. approuver ou rejeter les demandes de dérogation aux exigences en matière de sécurité de l'information;

1.25.3. le cas échéant, tenir les mandataires de [la solution de DSE], les fournisseurs de services électroniques et les dépositaires de renseignements sur la santé responsables de l'accès inapproprié ou non autorisé à [la solution de DSE], aux renseignements personnels sur la santé ou à l'information associée à [la solution de DSE], ainsi que de la collecte, de l'utilisation, de la divulgation, de la modification et du brouillage inappropriés ou non autorisés des renseignements personnels sur la santé ou de l'information associée à [la solution de DSE].

Équipe des opérations en matière de protection de la vie privée et de sécurité de Santé Ontario

1.26. L'Équipe des opérations en matière de protection de la vie privée et de sécurité de Santé Ontario doit :

1.26.1. fournir du leadership et de l'orientation en matière de sécurité de l'information aux dépositaires de renseignements sur la santé;

1.26.2. élaborer, mettre en œuvre et tenir à jour un programme de sécurité de l'information qui établira des mesures de gestion, des stratégies et un cadre stratégique pour les dépositaires de renseignements sur la santé, les innovateurs et les fournisseurs de services externes;

1.26.3. créer, instaurer et tenir à jour des politiques, des normes et des documents à l'appui qui permettent de soutenir et de développer les principes énoncés dans la présente politique;

1.26.4. offrir de l'orientation aux participants concernant la formation et les activités de sensibilisation relatives à la sécurité de l'information;

1.26.5. surveiller les mesures de sécurité de l'information, les incidents dans ce domaine et l'état et l'efficacité du programme connexe, les signaler au Comité de protection de la vie privée et de sécurité ou au Comité ConnexionSécurité et lui recommander des mesures ou des améliorations;

1.26.6. examiner les dérogations aux politiques de sécurité de l'information et présenter des recommandations à ce sujet à l'organisme de surveillance compétent.

Dépositaires de renseignements sur la santé et bureau de l'équipe de [la solution de DSE]

1.27. Tous les dépositaires de renseignements sur la santé doivent :

1.27.1. 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;

1.27.2. 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* (LPRPS), ou la personne-ressource de l'établissement indiquée dans l'accord de participation;

1.27.3. informer adéquatement les mandataires et les fournisseurs de services électroniques ayant accès aux services de [la solution de DSE] de leurs responsabilités en matière de sécurité de l'information;

1.27.4. 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];

1.27.5. tenir les mandataires et les fournisseurs de services électroniques responsables de l'accès inapproprié ou non autorisé à [la solution de DSE] ou aux renseignements, 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;

Comité ConnexionSécurité

3.5.1. Approuver toutes les politiques sur la sécurité de l'information

3.5.2. Revoir les tendances dans les rapports sur de dérogation à la sécurité

Revoir les rapports d'incidents de sécurité.

Dérogations Toute dérogation à la présente politique doit être approuvée par l'organisme de surveillance compétent, qui l'autorisera seulement si elle est clairement justifiée et n'a que la portée nécessaire pour satisfaire le besoin.

Voir l'*Annexe A : Demandes de dérogation aux exigences en matière de sécurité de l'information* de la présente *Politique de sécurité de l'information.*

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 de l'accord de participation conclu avec les dépositaires de renseignements sur la santé ou les fournisseurs de services électroniques, ainsi que des mesures correctives.

Structure de la politique de gouvernance

Solution de DSE	Comité de surveillance compétent
RDC de ConnexionOntario	**Comité stratégique de Santé Ontario**
Répertoire numérique des médicaments	**Comité stratégique de Santé Ontario**
Service commun d'imagerie diagnostique	**Comité stratégique de Santé Ontario**
RDC des soins primaires	**Comité stratégique de Santé Ontario**

Références

Lois

- LPRPS
- O. Reg. 329/04, art. 6

Normes internationales

- ISO/IEC 27001:2005 – Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences
- ISO/IEC 27002:2005 – Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information
- ISO/IEC 27005:2008 – Technologies de l'information – Techniques de sécurité – Gestion des risques en sécurité de l'information
- ISO 27799:2008 – Informatique de santé – Management de la sécurité de l'information relative à la santé en utilisant l'ISO/CEI 27002

Documents liés au dossier de santé électronique de Santé 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 fédérées 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
- Harmonized Privacy Protection Policies (en anglais)

Inforoute Santé du Canada

- Inforoute Santé du Canada, Dossier de santé électronique (DSE) – Exigences en matière de protection de la confidentialité et de sécurité (version 1.1, révisée le 7 février 2005)

Autre référence

- Commissaire à l'information et à la protection de la vie privée de l'Ontario, *Directives concernant la sécurité des transmissions par télécopieur* (janvier 2003)

Annexe A : Demandes de dérogation aux exigences en matière de sécurité de l'information

Étape	Responsabilité	Description
1	Mandataire ou fournisseur de services électroniques de [la solution de DSE] - OU – Dépositaire de renseignements sur la santé, son mandataire ou son fournisseur de services électroniques (« demandeur »)	Remplir la section 1 du *Formulaire de demande de dérogation aux exigences en matière de sécurité de l'information* et envoyer le formulaire à l'Équipe des opérations en matière de protection de la vie privée et de sécurité de Santé Ontario.
2	Équipe des opérations en matière de protection de la vie privée et de sécurité de Santé Ontario	Étudier le contenu du *Formulaire de demande de dérogation aux exigences en matière de sécurité de l'information* et remplir la section 2[1].
3	Organisme de surveillance compétent	Examiner la demande et prendre l'une des mesures suivantes : • Approuver la demande. • Approuver la demande sous certaines conditions. • Rejeter la demande.
4	Équipe des opérations en matière de protection de la vie privée et de sécurité de Santé Ontario	Consigner la décision de l'organisme de surveillance compétent. Informer le demandeur de la décision du Comité directeur et envoyer au dépositaire de renseignements sur la santé une copie du *Formulaire de demande de dérogation aux exigences en matière de sécurité de l'information*. Stocker le *Formulaire de demande de dérogation aux exigences en matière de sécurité de l'information*.

Voici le processus de révision et, s'il y a lieu, de réapprobation des dérogations aux exigences en matière de sécurité de l'information approuvées initialement pour plus de deux ans.

[1] Cette section est remplie en consultation avec le demandeur; il s'agit habituellement d'un processus cyclique. Par exemple, une fois que l'Équipe des opérations en matière de protection de la vie privée et de sécurité de Santé Ontario a consulté le demandeur, ce dernier peut consentir à adopter d'autres mesures de contrôle compensatoires. Le formulaire sera alors mis à jour, et les risques résiduels pourraient être réduits.

Étape	Responsabilité	Description
1	Équipe des opérations en matière de protection de la vie privée et de sécurité de Santé Ontario	Passer en revue le *Formulaire de demande de dérogation aux exigences en matière de sécurité de l'information* approuvé pour déterminer si le niveau de risque établi doit être modifié. S'il n'y a pas de nouveaux risques et que le niveau de risque ne s'est pas accru : • Mettre à jour le registre des demandes de dérogation aux exigences en matière de sécurité de l'information pour signaler qu'un examen a été réalisé, mais qu'il n'y avait pas de nouveaux risques et que le niveau de risque initial n'avait pas augmenté. • Aviser le demandeur du renouvellement de la dérogation. • Consigner le renouvellement. (Le processus se termine ici.) Si de nouveaux risques ont été décelés ou que le niveau de risque initial s'est accru : • L'Équipe des opérations en matière en matière de protection de la vie privée et de sécurité de Santé Ontario met à jour le *Formulaire de demande de dérogation aux exigences en matière de sécurité de l'information* et informe le demandeur de la modification du risque évalué.
2	Demandeur	Examiner le formulaire mis à jour et y inscrire toute mesure de contrôle compensatoire instaurée ou qui le sera pour gérer les risques supplémentaires ou accrus.
3	Équipe des opérations en matière de protection de la vie privée et de sécurité de Santé Ontario	Passer en revue le formulaire mis à jour et ajuster l'évaluation de risques résiduels s'il y a lieu. Envoyer le formulaire à l'organisme de surveillance compétent.
4	Organisme de surveillance compétent	Examiner la demande et prendre l'une des mesures suivantes : o Renouveler la dérogation. o Renouveler la dérogation sous certaines conditions. • Annuler la dérogation.
5	Équipe des opérations en matière de protection de la vie privée et de sécurité de Santé Ontario	Consigner la décision de l'organisme de surveillance compétent. Informer le demandeur de la décision de l'organisme de surveillance compétent et envoyer au dépositaire de renseignements sur la santé une copie du *Formulaire de demande de dérogation aux exigences en matière de sécurité de l'information*. Stocker le *Formulaire de demande de dérogation aux exigences en matière de sécurité de l'information*.

Formulaire de demande de dérogation aux exigences en matière de sécurité de l'information

Remplissez ce formulaire pour demander une dérogation aux exigences en matière de sécurité de l'information. Veuillez prendre contact avec l'Équipe des opérations en matière de protection de la vie privée et de sécurité de Santé Ontario avant de remplir ce formulaire.

Instructions
1. Remplissez tous les champs selon les indications. Les champs obligatoires sont marqués d'un astérisque (*). Le formulaire vous sera retourné s'il n'est pas complet. Indiquez « Ne s'applique pas » ou « S.O. » si un champ ne s'applique pas. 2. Une fois le formulaire dûment rempli, veuillez l'envoyer par courriel à l'Équipe des opérations en matière de protection de la vie privée et de sécurité de Santé Ontario. 3. Si vous avez des questions concernant le présent formulaire, veuillez communiquer avec le coordonnateur de [la solution de DSE] de l'établissement ou l'Équipe des opérations en matière de protection de la vie privée et de sécurité de Santé Ontario. **ASTUCES POUR REMPLIR LE FORMULAIRE : ● À l'ouverture du formulaire, le pointeur se trouvera dans le premier champ. Commencez à entrer les renseignements. ● Servez-vous de la touche de tabulation de votre clavier pour passer au champ suivant. ● Pour revenir au champ précédent, utilisez les touches SHIFT et de tabulation. ● Cliquez sur le bouton gauche de la souris pour cocher des cases.**
SECTION 1 : Demande (à remplir par le demandeur)
Renseignements sur le demandeur

Prénom*		Nom de famille*
Titre* *(p. ex., directeur général, directeur de l'informatique)*	Téléphone au travail* *(indiquer le poste)* ( )	Titre* *(p. ex., directeur général, directeur de l'informatique)*
Nom de l'organisme, de l'établissement ou de l'hôpital *(p. ex., Hôpital ABC)*		
Nom de la politique, de la norme ou du document à l'appui où se trouvent les exigences visées par la demande de dérogation* :		
Numéro de la ou des exigences* :		
Motif(s) du non-respect de ces exigences* :		
Liste des systèmes d'information ou des technologies de l'information qui seront visés par la dérogation* :		
Nature et degré de confidentialité des données concernées* :		

Plan proposé pour la gestion ou l'atténuation des risques associés au non-respect des exigences ou liste des mesures de contrôle compensatoires mises en place* :
Durée prévue de la dérogation* :
Renseignements supplémentaires :
Approbation à l'interne (p. ex., directeur de l'informatique du dépositaire de renseignements sur la santé) :
Veuillez inscrire le nom complet de l'approbateur et son titre (p. ex., John Smith, directeur de l'information) et joindre un courriel de l'approbateur lorsque vous enverrez le formulaire par courriel aux responsables de [la solution de DSE].
SECTION 2 : Évaluation (à remplir par l'Équipe des opérations en matière de protection de la vie privée et de sécurité de Santé Ontario)
Renseignements sur le vérificateur de [la solution de DSE]

Prénom*	Nom de famille*	
Titre* *(p. ex., analyste de la sécurité)*	Numéro au travail* *(indiquer le poste)* ( )	Titre* *(p. ex., analyste de la sécurité)*
Description des risques pour [la solution de DSE] ou la solution de connexion*		**Niveau de risque résiduel*** *(p. ex., élevé, modéré ou faible)*

Recommandation de l'Équipe des opérations en matière de protection de la vie privée et de sécurité de Santé Ontario*
(N. B. : Voici les options possibles : 1) approuver la demande telle quelle, 2) approuver la demande sous certaines conditions (énumérer les conditions), OU 3) rejeter la demande.)
SECTION 3 : Décision (à remplir par l'Équipe des opérations en matière de protection de la vie privée et de sécurité de Santé Ontario)

Décision de l'organisme de surveillance compétent *	**Date d'approbation***
(N. B. : Voici les options possibles : 1) approuver la demande telle quelle, 2) approuver la demande sous certaines conditions (énumérer les conditions), OU 3) rejeter la demande.)	

Preuve de la décision*
(Un courriel du président de l'organisme de surveillance compétent ou une copie du procès-verbal est une preuve acceptable. Veuillez joindre la preuve dans l'espace ci-dessous [p. ex., en insérant un fichier .msg ou PDF dans le document en tant qu'objet]. N. B. Pour ce faire, vous devez d'abord déverrouiller le fichier du formulaire.)