Ontario Health

Norme sur la gestion des menaces et des risques

Version: 1.8

N° de document : 3547

Gestion du document

Fréquence de révision : Une fois par année ou selon la règle établie par le Comité ConnexionSécurité.

Historique des approbations

APPROBATEURS	DATE D'APPROBATION
Comité ConnexionSécurité	2014-09-09
Comité ConnexionSécurité	2017-03-20
Comité ConnexionSécurité	2018-03-26
Comité ConnexionSécurité	2019-07-04
Comité ConnexionSécurité	2021-03-18

Historique des révisions

NUMÉRO DE VERSION	DATE	RÉSUMÉ DES CHANGEMENTS	AUTEUR DES CHANGEMENTS
1.0	2013-11-18	Adoption de la version de novembre 2013 du groupe de travail sur la protection de la vie privée et la sécurité de ConnexionRGT.	Mark Carter
1.1	2014-08-20	Révision en fonction des commentaires reçus des membres du Comité ConnexionSécurité. Ajout d'une référence à la politique d'assurance harmonisée; clarification de la formulation sur les exigences d'EMR des DRS au point 1.1; ajout d'un cas où il est recommandé de faire une EMR (lors d'une modification aux ententes ou aux lois applicables); ajout d'une formulation pour exiger l'approbation des résultats d'EMR par le comité directeur avant leur divulgation aux DRS.	Mark Carter
1.2	2014-09-09	Révision des points 1.5 et 2.7 pour indiquer que les EMR de type « delta » sont facultatives. Approbation de la politique à la réunion du 9 septembre 2014 du Comité ConnexionSécurité.	Mark Carter
1.3	2015-01-21	Harmonisation du nom de la politique sur le contrôle de l'accès en fonction de la décision définitive du Comité ConnexionSécurité à l'issue de la troisième étape du processus de rédaction.	Mark Carter
1.4	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	Mark Carter

NUMÉRO DE VERSION	DATE	RÉSUMÉ DES CHANGEMENTS	AUTEUR DES CHANGEMENTS
		processus de décision en matière de dérogation.	
1.5	2017-03-20	Mise à jour de la norme afin de refléter l'ITSM. Changement du titre du document, qui passe de « Politique » à « Norme ». Mise à jour de la définition de « la solution de DSE ». Révision des contrôles en fonction des commentaires.	Ravi Addepalli
1.6	16 mars 2018	Mise à jour de la norme afin d'inclure l'accès au DSE par les patients.	Geovanny Diaz
1.7	4 juillet 2019	Mise à jour de la norme afin d'inclure les exigences relatives aux normes de sécurité des DSE	Ravi Addepalli
1.8	2021-01-04	Examen du document avec des modifications mineures, mise à jour du modèle et du cycle de révision tous les deux ans. Ajouter une exigence de contrôle pour les DRS pour effectuer une EMR s'il s'agit d'une exigence obligatoire dans le cadre du processus de gouvernance du projet/SDLC.	Ana Fukushima

Norme sur la gestion des menaces et des risques

Objet

La présente norme a pour but de définir la stratégie d'évaluation et de gestion des risques liés à la sécurité pour [la solution de DSE] ou les services de gestion d'identité et les terminaux d'envoi de données des dépositaires de renseignements sur la santé (DRS).

Portée

La présente norme s'applique à [la solution de DSE] et à l'équipe qui en est responsable y compris la totalité des portails et des applications pour les patients.

Elle vise les éléments suivants dans le cas des DRS qui utilisent [la solution de DSE] pour voir des renseignements personnels sur la santé (RPS) à l'aide d'une **technologie de gestion d'identité locale** :

- le système de contrôle de l'accès et de gestion d'identité du DRS (les « services de gestion d'identité ») qui gère les processus d'authentification et d'autorisation donnant accès à [la solution de DSE] (solution de service d'émission de jetons de sécurité de [la solution de DSE], Active Directory Federation Services 2.0 de Microsoft ou autre);

- toute connexion directe au portail du fournisseur de [la solution de DSE] et aux fonctions administratives de cette dernière, ce qui comprend les composants connectés (pare-feu, serveur mandataire, etc.);

- l'intégration du portail du fournisseur de [la solution de DSE] au système d'information local du DRS ou à l'application de gestion des dossiers médicaux électroniques.

Elle vise plutôt les éléments suivants dans le cas des DRS qui utilisent [la solution de DSE] pour voir, traiter ou autrement manipuler des RPS à l'aide du **service ONE ID de Santé Ontario** :

- toute connexion directe aux fonctions administratives de [la solution de DSE], ce qui comprend les composants connectés (pare-feu, serveur mandataire, etc.).

Dans le cas des DRS qui créent et versent des RPS dans le dépôt de données cliniques de [la solution de DSE], la présente norme, en plus de ce qui est prévu pour les sites qui ne font que consulter les données, s'applique aux éléments suivants :

- les terminaux d'envoi de données qui fournissent des RPS au dépôt de données cliniques de [la solution de DSE];

- les technologies de l'information et les processus qui assurent la qualité des données envoyées (la mise en correspondance de la terminologie, par exemple).

La norme ne s'applique pas aux DRS, à leurs mandataires et à leurs fournisseurs de services électroniques qui ne créent pas, ne versent pas et ne consultent pas de données dans [la solution de DSE].

La norme devrait être lue en parallèle avec la politique d'assurance harmonisée et les procédures connexes, ce qui comprend les modifications qui y sont apportées de temps à autre.

Définitions

[la solution de DSE] : Solution utilisée, y compris les systèmes connexes, pour stocker et rendre accessibles les renseignements personnels sur la santé contenus dans les systèmes de renseignements électroniques sur la santé 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.

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.

Comité de protection de la vie privée et de sécurité : Comité composé de mandataires de dépositaires de renseignements sur la santé participants qui font respecter les exigences de protection de la vie privée et de sécurité de l'information.

Devrait/devraient : S'utilisent lorsqu'il y a des raisons, selon les circonstances, de ne pas exécuter ce qui est proposé. La personne doit cependant comprendre les conséquences de ses actes si elle décide de ne pas adhérer à ce qui est écrit et songer à mettre en œuvre des mesures de contrôle en guise de compensation.

Doit/doivent : S'utilisent dans le cas des exigences absolues où il n'y a aucune autre option possible.

Fournisseur de services électroniques : Personne qui fournit des biens ou des services dans le but de permettre à un dépositaire de renseignements sur la santé d'employer des moyens électroniques de recueillir, d'utiliser, de modifier, de diffuser, de conserver ou d'éliminer des renseignements personnels sur la santé et qui comprend un fournisseur de réseau d'information sur la santé.

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

Peut/peuvent : S'utilisent lorsque ce qui est proposé n'est qu'une recommandation ou ne sert que d'exemple qui ne se veut pas exhaustif.

Service de gestion d'identité : Technologies et services, politiques, processus et procédures connexes servant à créer, à conserver, à mettre en sécurité, à valider, à affirmer et à gérer des identités électroniques pour [la solution de DSE].

Terminal d'envoi de données : Technologies et processus connexes qui alimentent le dépôt de données cliniques et font l'objet des recherches de données par l'utilisateur en milieu clinique. Comprend habituellement le système d'information (système d'information hospitalier, système d'information de laboratoire, système d'information clinique, etc.) qui se branche automatiquement à [la solution de DSE] pour rendre les données cliniques accessibles.

Exigences de la norme

1. Exigences pour les dépositaires de renseignements sur la santé

1.1. Les dépositaires de renseignements sur la santé (DRS) sont responsables d'effectuer des évaluations des menaces et des risques (EMR) pour leurs services de gestion d'identité et leurs terminaux d'envoi de données. Les DRS peuvent faire faire une EMR par une autre entité en leur nom pour satisfaire à l'exigence. Les méthodes d'EMR peuvent provenir de l'une ou l'autre des organisations suivantes :

- le Centre de la sécurité des télécommunications Canada (CSTC);
- le National Institute of Standards and Technology (NIST);
- l'Organisation internationale de normalisation (ISO);
- l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA).

1.2. Les DRS devraient demander des sommaires des résultats des EMR effectuées pour [la solution de DSE].

1.3. Lorsqu'un DRS 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 manipulés de manière sécuritaire.

1.4. Les DRS doivent effectuer une EMR, une EMR de type « delta » ou une évaluation de sécurité des DSE dans les cas suivants :

1.4.1. avant la modification des paramètres d'utilisateur des DSE et selon les recommandations correspondantes de Santé Ontario;

1.4.2. avant toute modification importante à l'architecture ou aux fonctions dorsales existantes;

1.4.3. avant toute modification importante à la conception technique ou aux fonctions frontales existantes;

1.4.4. Les DRS doivent effectuer des évaluations des menaces et des risques si ces exigences sont obligatoirs pout la gouvernance du projet.

1.4.5. avant toute modification aux modèles, aux outils, aux processus ou aux personnes du soutien opérationnel;

1.4.6. avant toute modification aux politiques ou aux procédures existantes;

1.4.7. avant d'accorder à un fournisseur de services électroniques l'accès à [la solution de DSE];

1.4.8. avant d'apporter des modifications aux ententes applicables qui pourraient avoir des conséquences sur la vie privée de personnes ou la sécurité de leurs renseignements personnels sur la santé (RPS);

1.4.9. avant d'apporter des changements législatifs à la *Loi de 2004 sur la protection des renseignements personnels sur la santé* (LPRPS) qui pourraient avoir des conséquences sur la vie privée de personnes ou la sécurité de leurs RPS;

1.4.10. à la découverte d'une vulnérabilité qui a entraîné ou qui aurait pu entraîner un incident de sécurité de l'information pour [la solution de DSE];

1.4.11. tous les cinq ans si aucun des points ci-dessus n'a enclenché d'EMR exhaustive.

1.5. Les DRS devraient consigner une méthode de traitement pour tous les risques relevés par EMR. Les méthodes de traitement peuvent inclure l'une ou l'autre des options suivantes ou une combinaison d'entre elles :

1.5.1. l'application d'autres mesures de contrôle de la sécurité de l'information pour réduire davantage le risque;

1.5.2. l'acceptation du risque;

1.5.3. l'élimination du risque en interdisant l'action à son origine.

2. Exigences pour l'équipe de [la solution de DSE]

2.1. L'équipe de [la solution de DSE] est responsable d'effectuer des EMR pour [la solution de DSE].

2.2. L'équipe de [la solution de DSE] doit effectuer toutes les EMR conformément à la *Méthodologie harmonisée d'évaluation des menaces et des risques* du CSTC.

2.3. L'équipe de [la solution de DSE] doit rendre accessibles les sommaires des résultats des EMR et les plans de traitement des risques applicables à la demande des DRS qui ont accès à [la solution de DSE] dans les trois jours suivant l'approbation de l'EMR et du plan d'atténuation des risques par l'organisme de surveillance compétent.

2.4. L'équipe de [la solution de DSE] doit conserver les éléments suivants :

2.4.1. une liste des éléments d'actif relatifs à [la solution de DSE] avec leur catégorie d'importance;

2.4.2. une liste des risques relatifs à [la solution de DSE] avec leur catégorie de vulnérabilité aux menaces.

2.5. Toute modification à apporter aux catégories d'importance ou de vulnérabilité doit être approuvée par l'organisme de surveillance compétent.

2.6. L'équipe de [la solution de DSE] doit traiter les résultats d'EMR effectuées en entier ou en partie et les documents connexes conformément aux exigences de protection de l'information jugée confidentielle.

2.7. L'équipe de [la solution de DSE] doit effectuer une EMR, de type « delta » ou non, pour [la solution de DSE] dans les cas suivants :

2.7.1. avant toute modification importante à l'architecture ou aux fonctions dorsales existantes;

2.7.2. avant toute modification importante à la conception technique ou aux fonctions frontales existantes;

2.7.3. avant toute modification aux modèles, aux outils, aux processus ou aux personnes du soutien opérationnel;

2.7.4. avant toute modification aux politiques ou aux procédures existantes;

2.7.5. avant tout changement de fournisseur de services électroniques;

2.7.6. avant d'apporter des modifications aux ententes applicables qui pourraient avoir des conséquences sur la vie privée de personnes ou la sécurité de leurs RPS;

2.7.7. avant d'apporter des changements législatifs à la LPRPS qui pourraient avoir des conséquences sur la vie privée de personnes ou la sécurité de leurs RPS;

2.7.8. à la découverte d'une vulnérabilité qui a entraîné ou qui aurait pu entraîner un incident de sécurité de l'information si l'organisme de surveillance compétent le juge nécessaire;

2.7.9. au moins tous les deux ans si aucun des points ci-dessus n'a enclenché d'EMR exhaustive.

2.8. L'équipe de [la solution de DSE] doit consigner une méthode de traitement pour tous les risques relevés par EMR. Les méthodes de traitement peuvent inclure l'une ou l'autre des options suivantes ou une combinaison d'entre elles :

2.8.1. l'application d'autres mesures de contrôle de la sécurité de l'information pour réduire davantage le risque;

2.8.2. l'acceptation du risque;

2.8.3. l'élimination du risque en interdisant l'action à son origine.

2.9. Lorsque l'équipe de [la solution de DSE] choisit d'appliquer d'autres mesures de contrôle de la sécurité de l'information, les mesures devraient être mises en œuvre selon les exigences propres à l'EMR.

2.10. L'équipe de [la solution de DSE] doit consigner tous ses risques acceptés dans un registre à cet effet avec le nom des propriétaires, les plans d'action (explication de la méthode de traitement du risque) et l'état des risques pour en faire un suivi. Ce suivi doit se faire chaque trimestre; les méthodes de traitement doivent être actualisées au besoin.

2.11. L'équipe de [la solution de DSE] doit présenter les résultats de ses EMR à Santé Ontario, qui facilitera alors la déclaration au comité ConnexionSécurité et à l'organisme de surveillance compétent.

Lorsqu'il y a des risques résiduels d'importance moyenne ou supérieure, les résultats de l'EMR doivent aussi être approuvés par un cadre supérieur (comme le dirigeant principal de l'information) au sein de l'équipe de [la solution de DSE] avant leur envoi à Santé Ontario.

Dérogations Toute dérogation à la norme doit être approuvée par l'organisme de surveillance compétent, lequel l'autorisera uniquement lorsque la situation le justifie et au degré minimal nécessaire pour la justification apportée.

Consultez à cet effet l'annexe A intitulée *Demandes de dérogation aux exigences en matière de sécurité de l'information* dans la *Politique de sécurité de l'information*.

Application Tous les cas de non-respect seront examinés par l'organisme de surveillance compétent.

L'organisme de surveillance compétent a le pouvoir d'imposer les sanctions appropriées, ce qui peut inclure la cessation des ententes avec le DRS ou les fournisseurs de services électroniques ou la cessation des privilèges d'accès des mandataires, et de demander des mesures correctives.

References

Lois

- LPRPS, art. 12 et 13 et partie V.1
- 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 de politiques sur les DSE de Santé Ontario

- Politique de sécurité de l'information
- Politique d'utilisation acceptable des données et des technologies de l'information
- Politique sur le contrôle de l'accès aux systèmes et les processus de gestion d'identité connexes
- Politique sur les pratiques de l'autorité locale d'enregistrement

- Norme sur la fédération d'identités (en anglais)
- Politique sur la continuité des activités
- Politique sur la cryptographie
- Politique sur les fournisseurs de services électroniques
- Politique sur la gestion des incidents de sécurité de l'information
- Politique sur la gestion de l'information et des éléments d'actif
- Politique sur les réseaux et les opérations
- Politique sur la journalisation de sécurité et la surveillance
- Politique sur le cycle de développement de systèmes
- Politique sur la sécurité matérielle
- Politique sur la gestion des menaces et des risques
- Politiques harmonisées sur la protection de la vie privée (en anglais)

Référence à Inforoute Santé du Canada

- Exigences en matière de protection de la confidentialité et de sécurité d'Inforoute Santé du Canada (version 1.1 révisée le 7 février 2005)

Autre

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