Ontario Health

Norme sur les fournisseurs de services électroniques

Version: 1.8

N° de document : 3538

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	2017-03-26
Comité ConnexionSécurité	2018-03-26
Comité ConnexionSécurité	2021-03-18

Historique des révisions

NUMÉRO DE VERSION	DATE	RÉSUMÉ DES CHANGEMENTS	AUTEUR DES CHANGEMENTS
1.0	2013-12-20	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	2014-10-09	Révision en fonction des commentaires reçus de responsables des programmes ConnexionRGT et Connexion Sud-Ouest de l'Ontario et du groupe de protection des renseignements personnels sur la santé. Modifications mineures aux sections de la portée, des dérogations et de l'application en vue d'une harmonisation avec les politiques du Comité ConnexionConfidentialité; ajout d'une définition officielle de « terminal d'envoi de données » et de « service de gestion d'identité »; ajout de mentions sur les mesures de contrôle pour protéger la vie privée aux points 1.4.10, 1.5, 2.3, 2.4.10 et 2.5; ajout d'une note en bas de page au point 2.6 pour clarifier l'exemple présenté au point 2.7 et montrer que c'est une mesure facultative.	Mark Carter
1.2	2014-11-05	Approbation de la politique à la réunion du 5 novembre 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	Mark Carter

NUMÉRO DE VERSION	DATE	RÉSUMÉ DES CHANGEMENTS	AUTEUR DES CHANGEMENTS
		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.	
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.	Raviteja Addepalli
1.6	2018-03-16	Mise à jour de la norme afin d'inclure l'accès au DSE par les patients.	Geovanny Diaz
1.7	2020-03-16	Mise à jour avec les commentaires des parties prenantes. Mise à jour les références et le modèle.	Ana Fukushima
1.8	2021-01-04	Examen du document avec des modifications mineures, mise à jour du cycle de révision tous les deux ans	Ana Fukushima

Norme sur les fournisseurs de services électroniques

Objet

La présente norme a pour but de définir les exigences de gestion des fournisseurs de services électroniques.

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 fournisseurs de services électroniques qui auront accès aux éléments suivants dans le cas des dépositaires de renseignements sur la santé (DRS) qui utilisent [la solution de DSE] pour voir, traiter ou autrement manipuler 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 fournisseurs de services électroniques qui auront accès aux éléments suivants s'ils le font 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 fournisseurs de services électroniques qui auront accès 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] et qui n'accèdent pas à cette dernière.

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.

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 de la [solution DSE]. Voir la section intitulée Structure de la politique de gouvernance dans le document Politique de sécurité de l'information.

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].

Système d'information : Ensemble autonome de technologies de l'information organisées de manière à recueillir, à traiter, à conserver, à utiliser, à divulguer, à détruire ou à éliminer l'information.

Technologie de l'information : Tout élément (matériel ou électronique) utilisé pour l'acquisition, le stockage, la manipulation, la gestion, le déplacement, le contrôle, l'affichage, l'échange, l'envoi ou la réception automatiques de données ou d'information. Comprend, sans s'y limiter, le matériel informatique, les logiciels, les microprogrammes, le matériel auxiliaire et les ressources connexes.

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) devraient classifier leurs fournisseurs de services électroniques en fonction de leur type (fournisseur de services applicatifs, fournisseur de services de réseau, fournisseur de services de stockage, etc.) et de l'importance des services qu'ils offrent.

1.2. Les DRS doivent évaluer les risques à la sécurité de l'information et à la protection de la vie privée que constituent les nouveaux fournisseurs de services électroniques pour [la solution de DSE] avant de conclure tout contrat avec ces derniers.

1.3. Les DRS doivent définir et consigner tous les systèmes d'information et les services offerts par les fournisseurs de services électroniques au renouvellement des ententes de service. Les ententes de service devraient contenir les renseignements suivants :

1.3.1. les rôles et responsabilités concernant [la solution de DSE] soumis à la LPRPS et aux politiques et procédures en matière de protection de la vie privée et de sécurité de l'information;

1.3.2. les rôles et responsabilités en matière d'implantation, de maintenance et de soutien technique relatifs aux systèmes d'information ou aux services offerts;

1.3.3. le degré d'importance des services;

1.3.4. les dates et heures où les services sont requis;

1.3.5. les exigences de capacité des systèmes et des réseaux;

1.3.6. la durée maximale des interruptions et les objectifs en matière de niveau de service;

1.3.7. les rapports sur le niveau de service et leur fréquence;

1.3.8. les limites de temps à ne pas dépasser (par exemple, la durée de panne de service après laquelle la situation devient inacceptable pour le DRS);

1.3.9. 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;

1.3.10. les mesures de contrôle minimales pour protéger la vie privée et assurer la sécurité de l'information;

1.3.11. les produits livrables attendus;

1.3.12. les représentants de chaque fournisseur de services électroniques.

1.4. Les DRS doivent exiger des nouveaux fournisseurs de services électroniques qu'ils mettent en œuvre des mesures de contrôle pour protéger la vie privée décrites dans la politiques et les normes sur les DSE et assurer la sécurité de l'information avant de leur accorder l'accès à [la solution de DSE].

1.5. Les DRS devraient établir une méthode à respecter pour mettre fin aux relations avec les fournisseurs de services électroniques en y incluant par exemple les étapes suivantes :

1.5.1. la désignation des personnes responsables de mettre fin à la relation;

1.5.2. la révocation des droits d'accès au matériel informatique et aux logiciels de l'organisation;

1.5.3. le retour, le transfert ou la destruction de tous les éléments d'actif (supports de sauvegarde, documents, matériel et dispositifs d'authentification, par exemple).

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

2.1. L'équipe de [la solution de DSE] devrait classifier ses fournisseurs de services électroniques en fonction de leur type (fournisseur de services applicatifs, fournisseur de services de réseau, fournisseur de services de stockage, etc.) et de l'importance des services qu'ils offrent.

2.2. L'équipe de [la solution de DSE] doit évaluer les risques à la sécurité de l'information et à la protection de la vie privée que constituent les nouveaux fournisseurs de services électroniques pour [la solution de DSE] avant de conclure tout contrat avec ces derniers.

2.3. L'équipe de [la solution de DSE] doit définir et consigner tous les systèmes d'information et les services offerts par les fournisseurs de services électroniques au renouvellement ou à la signature des ententes de service. Les ententes de service doivent contenir au minimum les renseignements suivants :

2.3.1. les rôles et responsabilités concernant [la solution de DSE] soumis à la LPRPS et aux politiques et procédures en matière de protection de la vie privée et de sécurité de l'information;

2.3.2. les rôles et responsabilités en matière d'implantation, de maintenance et de soutien technique relatifs aux systèmes d'information ou aux services offerts;

2.3.3. le degré d'importance des services;

2.3.4. les dates et heures où les services sont requis;

2.3.5. les exigences de capacité des systèmes et des réseaux;

2.3.6. la durée maximale des interruptions et les objectifs en matière de niveau de service;

2.3.7. les rapports sur le niveau de service et leur fréquence;

2.3.8. les limites de temps à ne pas dépasser (par exemple, la durée de panne de service après laquelle la situation devient inacceptable pour l'équipe de [la solution de DSE]);

2.3.9. 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;

2.3.10. les mesures de contrôle minimales pour protéger la vie privée et assurer la sécurité de l'information;

2.3.11. les produits livrables attendus;

2.3.12. les représentants de chaque fournisseur de services électroniques.

2.4. L'équipe de [la solution de DSE] doit exiger des 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 accorder l'accès à [la solution de DSE].

2.5. L'équipe de [la solution de DSE] doit veiller à ce que des évaluations des menaces et des risques soient effectuées pour leurs fournisseurs de services électroniques[1].

2.6. L'équipe de [la solution de DSE] doit sérieusement songer à restreindre la location des renseignements, des processus de traitement de l'information et des services des systèmes de l'information contrôlés ou assurés par les fournisseurs de services électroniques (par exemple, une organisation pourrait interdire à un fournisseur de services électroniques de stocker des renseignements sur des serveurs situés à l'extérieur du Canada).

2.7. L'équipe de [la solution de DSE] devrait établir une méthode à respecter pour mettre fin aux relations avec les fournisseurs de services électroniques en y incluant par exemple les étapes suivantes :

2.7.1. la désignation des personnes responsables de mettre fin à la relation;

2.7.2. la révocation des droits d'accès au matériel informatique et aux logiciels de l'organisation;

2.7.3. le retour, le transfert ou la destruction de tous les éléments d'actif (supports de sauvegarde, documents, matériel et dispositifs d'authentification, par exemple).

2.8. L'équipe de [la solution de DSE] doit prévoir des mesures en cas d'imprévu de manière à ce que les processus opérationnels puissent se poursuivre si le fournisseur de services électroniques n'est pas disponible (par exemple en cas de fin de contrat, de catastrophe ou de grève). Ces mesures doivent se baser sur les résultats d'une évaluation des menaces et des risques et peuvent inclure les éléments suivants :

2.8.1. l'utilisation d'autres locaux sûrs pour assurer le maintien des activités;

[1] Voir la *Norme sur la gestion des menaces et des risques* pour obtenir de plus amples renseignements sur les évaluations des menaces et des risques, notamment leur fréquence.

2.8.2. le placement en main tierce des renseignements et des technologies propriétaires (par exemple une entité extérieure digne de confiance telle qu'un avocat qui abrite le code source de l'application et les clés cryptographiques).

2.8.3. des mesures de rétablissement pour assurer le maintien de l'accès aux renseignements stockés chez un fournisseur extérieur ou sur un nuage;

2.8.4. l'adhésion au programme de continuité des activités de l'équipe de [la solution de DSE].

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.

Voir 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 et de normes sur les DSE 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
- 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)