Ontario Health

Politique sur les pratiques de l'autorité locale d'enregistrement

Version: 1.8

Identificateur de document : 3543

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	2015-01-22
Comité ConnexionSécurité	2021-03-18

Historique des modifications

NUMÉRO DE VERSION	DATE	RÉSUMÉ DES CHANGEMENTS	AUTEUR DES CHANGEMENTS
1.0	2013-12-23	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	2014-12-05	Révision en fonction des commentaires de membres et du groupe responsable de ONE ID. Ajout de la définition de « mandataire », d'« autorité locale d'enregistrement » et d'« approbateur ». Révision des annexes D et E de manière à y inclure les options d'inscription ou de révocation, de rétablissement ou de suspension de l'accès d'un mandataire ou d'un fournisseur de services électroniques. Suppression de l'obligation de nommer l'équipe de [la solution de DSE] comme autorité d'enregistrement et remplacement par la possibilité de déléguer une personne; modification de la section de la nomination de manière à ce que les responsabilités qui y sont mentionnées reviennent à l'approbateur et non à l'autorité locale d'enregistrement; ajout d'autres processus possibles d'enregistrement à l'annexe D; ajout d'un champ de but de la demande à l'annexe E; ajout du formulaire d'inscription pour les utilisateurs déjà enregistrés (annexe F).	Mark Carter
1.2	2014-12-18	Révision à la suite de la réunion du Comité ConnexionSécurité du 17 décembre. Révision de la section de la nomination de manière à permettre l'accès aux fonctions administratives autorisées de [la solution de DSE].	Mark Carter
1.3	2015-01-22	Ajout d'une mention au point 2.5 exigeant que la	Mark Carter

NUMÉRO DE VERSION	DATE	RÉSUMÉ DES CHANGEMENTS	AUTEUR DES CHANGEMENTS
		personne légalement responsable identifie les personnes ayant le pouvoir d'agir à titre d'approbateur. Reformulation du point 2.7.1 pour le rendre plus clair. Approbation de la politique par le Comité ConnexionSécurité.	
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 processus de décision en matière de dérogation.	Mark Carter
1.5	2017-06-23	Supprime les exigences de validation d'identité. Ceux-ci se trouvent dans le standard de fournisseur d'identité.	Ravi Addepalli
1.7	2021-01-04	Ajouter 1.7	
1.8	2021-01-04	Examen du document avec des modifications mineures, et mise à jour du cycle de révision tous les deux ans	Ana Fukushima

Politique sur les pratiques de l'autorité locale d'enregistrement

Objet

La présente politique a pour but de définir les procédures d'inscription des autorités locales d'enregistrement (ALE) ainsi que des mandataires et des fournisseurs de services électroniques afin de leur accorder l'accès à [la solution de DSE].

Portée

Les procédures décrites ici s'appliquent à tous les dépositaires de renseignements sur la santé (DRS) qui accordent à leurs mandataires et à leurs fournisseurs de services électroniques un accès à [la solution de DSE] au moyen de leur technologie de gestion d'identité ou d'un fournisseur d'identités fédérées.
Elles ne s'appliquent pas aux DRS qui accordent à leurs mandataires et à leurs fournisseurs de services électroniques l'accès à [la solution de DSE] par la solution de gestion de l'identité ONE ID de Santé Ontario.

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 et qui sert donc de dépôt unique de ces renseignements lorsque de tels dépôts n'existent pas à l'échelle provinciale ou régionale, ce qui réduit la charge exercée sur les systèmes sources. Exclut tous les systèmes d'information et les technologies de l'information des dépositaires de renseignements sur la santé participants.

Approbateur : Toute personne ayant le pouvoir d'autoriser l'accès à [la solution de DSE] aux mandataires et aux fournisseurs de services électroniques. Habituellement, les personnes légalement responsables choisissent, en tant qu'approbateurs, des gestionnaires, mais ce peut aussi être une autorité locale d'enregistrement. Il est à noter que la définition d'« approbateur » s'applique précisément au contexte de la présente politique et de [la solution de DSE].

Autorité d'enregistrement : Personne ou entité responsable d'enregistrer des autorités locales d'enregistrement. L'équipe de [la solution de DSE] ou son délégué agira à titre d'autorité d'enregistrement pour tous les DRS dont les mandataires et les fournisseurs de services électroniques recevront un accès à [la solution de DSE] par des processus de contrôle de l'accès, des procédures, des politiques et des systèmes de gestion de l'identité mis en place par les DRS.

Autorité locale d'enregistrement (ALE) : Personne ayant reçu l'autorisation de la personne légalement responsable du dépositaire de renseignements sur la santé de gérer le processus d'enregistrement ou d'inscription des mandataires du dépositaire de renseignements sur la santé et des fournisseurs de services électroniques visant à accéder à [la solution de DSE] par le système de contrôle de l'accès et de gestion de l'identité du dépositaire de renseignements sur la santé. Elle est enregistrée auprès de l'équipe de [la solution de DSE] ou de son délégué et inscrit et enregistre les mandataires et les fournisseurs de services électroniques au nom de l'équipe de [la solution de DSE]. Il est à noter que la définition d'« autorité locale d'enregistrement » s'applique précisément au contexte de la présente politique et de [la solution de DSE].

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 ou entité 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.

Mandataire : Dans le contexte des dépositaires de renseignements sur la santé, personne qui, sous réserve de l'approbation du dépositaire, s'occupe de tout ce qui est lié aux renseignements personnels sur la santé de ce dernier, et ce, dans l'intérêt du dépositaire et non dans son propre intérêt, qu'il ait ou non le pouvoir d'engager le dépositaire, qu'il soit employé ou non par le dépositaire et qu'il soit rémunéré ou non. Par exemple, le mandataire peut être une organisation, un employé ou un entrepreneur qui valide l'identité des utilisateurs du dossier de santé électronique au nom d'un dépositaire de renseignements sur la santé. Un mandataire peut aussi assurer des services de correction de données d'un dépositaire de renseignements sur la santé à partir de son terminal d'envoi de données.

Personne légalement responsable : Personne, souvent un cadre supérieur comme le dirigeant principal de l'information de l'organisation, légalement responsable du processus d'inscription pour son dépositaire de renseignements sur la santé. Elle a pour rôle d'autoriser les approbateurs et les autorités locales d'enregistrement à s'occuper du processus d'inscription au nom du dépositaire de renseignements sur la santé.

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, moteur d'interface HL7, etc.) qui se branche automatiquement à [la solution de DSE] pour rendre les données cliniques accessibles.

Procédures

1. Exigences pour les dépositaires de renseignements sur la santé

1.1. 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.

1.2. 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 :

1.2.1. les professionnels de la santé reconnus qui voient des patients;

1.2.2. les résidents qui prodiguent des soins aux patients;

1.2.3. le personnel administratif qui sort les dossiers pour les médecins;

1.2.4. les commis d'unité qui examinent les résultats pour déceler le trouble du patient pour les médecins.

1.3. 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 :

1.3.1. offrir du soutien pour une fonction prévue pour les titulaires de postes d'administrateurs pour [la solution de DSE] (les agents de protection de la vie privée, les administrateurs de systèmes, les mandataires et les fournisseurs de services électroniques ne doivent par exemple pas recevoir un accès aux fonctions destinées aux professionnels de la santé ou leurs auxiliaires en milieu clinique).

Par exemple, les administrateurs de système peuvent demander un accès à la fonction de gestion des files d'erreurs pour corriger et traiter les messages, les agents de protection de la vie privée peuvent demander l'accès aux rapports sur la vie privée pour produire des rapports d'audit et les spécialistes de mise en correspondance des données peuvent demander un accès aux fonctions de mise en correspondance de la terminologie et des codes. Ces personnes ne doivent pas recevoir un accès aux fonctions destinées aux personnes qui prodiguent des soins ou qui aident ces dernières en milieu clinique, par exemple.

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

1.4.1. planification, évaluation ou surveillance de programmes;

1.4.2. gestion de risques ou d'erreurs;

1.4.3. amélioration de la qualité des soins, des programmes et des services;

1.4.4. formation (à moins que la personne soit étudiante ou résidente et doit y avoir accès pour prodiguer des soins);

1.4.5. traitement de paiements.

1.5. Les approbateurs ne doivent pas accorder l'accès à [la solution de DSE] si l'accès demandé sert aux fins de recherche.

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

1.7. Les approbateurs doivent supprimer les droits dont le mandataire n'a plus besoin, p. ex. le mandataire ne travaille plus pour le DRS.

Dérogations 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 le fournisseur de services électroniques ou la cessation des privilèges d'accès des mandataires, et de demander des mesures correctives.

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 le fournisseur de services électroniques ou la cessation des privilèges d'accès des mandataires, et de demander des mesures correctives.

Références

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)