Santé Ontario

Guide des fournisseurs de soins de santé

Le dossier de santé électronique (DSE)

Version 3.0 (octobre 2020)

Ontario

Table des matières

Renseignements généraux

Objet et portée

Le présent guide décrit les fonctions du dossier de santé électronique (DSE) et les avantages qu'il procure, ainsi que les règles, les rôles et les responsabilités en matière de sécurité, de protection de la vie privée et d'obligations juridiques auxquels les fournisseurs de soins de santé utilisant le DSE et les répertoires de données connexes doivent se conformer.

Les changements qui y sont apportés respectent la partie V.1 de la *Loi de 2004 sur la protection des renseignements personnels sur la santé* (*LPRPS*) et ses règlements d'application adoptés par le gouvernement de l'Ontario le 1er octobre 2020. Le contenu non modifié sera révisé et actualisé ultérieurement. En cas d'incohérence entre le nouveau contenu et l'ancien, c'est le nouveau qui s'applique. À titre informatif, voici où se trouvent les changements importants :

- Directives de consentement – page 13
- Demandes d'accès – page 16
- Demandes de rectification – page 18
- Gestion des incidents et violations touchant la protection de la vie privée – page 24

Destinataires

Le présent document s'adresse aux fournisseurs de soins de santé ontariens, qu'il s'agisse de personnes ou d'organisations, qui ont conclu ou concluront l'entente d'accès requise avec Santé Ontario pour accéder aux données cliniques concernant leurs patients à l'aide du DSE.

Documents connexes

Le présent guide doit être lu en parallèle avec les politiques et normes suivantes, qui se trouvent sur le site du programme de protection de la vie privée de Santé Ontario, à l'adresse www.ehealthontario.on.ca/fr/ :

Protection de la vie privée

- *Politique sur les demandes d'accès aux renseignements personnels sur la santé contenus dans un dossier de santé électronique*
- *Politique sur les demandes de rectification de renseignements personnels sur la santé contenus dans un dossier de santé électronique*
- *Politique de vérification de la conformité – Dossier de santé électronique*
- *Politique sur les directives de consentement et la dérogation à la préséance du consentement pour le dossier de santé électronique*
- *Politique relative aux plaintes et aux demandes de renseignements liées à la protection de la vie privée*
- *Politique sur la journalisation et la surveillance – Dossier de santé électronique*
- *Politique sur les incidents et violations touchant la protection de la vie privée – Dossier de santé électronique*
- *Politique de conservation – Dossier de santé électronique*

Sécurité

- *Politiques et normes – DSE*
- *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 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*
    - *Politique sur les pratiques de l'autorité locale d'enregistrement*
    - *Norme sur la journalisation de sécurité et la surveillance*
    - *Norme sur les réseaux et les opérations*
    - *Norme sur la sécurité matérielle*
    - *Norme sur le cycle de développement de systèmes*
    - *Norme sur la gestion des menaces et des risques*
    - *Politique et norme de Santé Ontario relatives aux fournisseurs de services d'authentification*

Le dossier de santé électronique

Présentation

Le dossier de santé électronique (DSE) est un registre sûr où sont consignés à vie les antécédents médicaux des Ontariens. Il permet aux membres des équipes de soins de santé (médecins de famille, infirmières, urgentologues, spécialistes) d'avoir accès en temps réel aux renseignements médicaux pertinents des patients et des clients afin de leur fournir les meilleurs soins possible. Santé Ontario a mis en place un système provincial qui offre aux fournisseurs de soins de santé dans les hôpitaux, les cliniques de médecine familiale, les foyers de soins de longue durée, les pharmacies et bien d'autres endroits l'accès au DSE du patient qui leur permet de consulter rapidement les résultats d'analyses en laboratoire, les médicaments délivrés couverts par l'assurance-santé, les images numériques (radiographie, imagerie par résonance magnétique), les sommaires de congé, etc.

Il y a plusieurs moyens de consulter les données du DSE, en fonction de la région. Pour en savoir plus, se référer à l'annexe F.

Le dossier de santé électronique d'un patient peut comprendre les renseignements personnels sur la santé (RPS) suivants en lien avec les soins de base, les soins actifs et les soins de santé communautaire :

- Renseignements sur les allergies
- Rapports cardiovasculaires
- Rapports d'imagerie diagnostique (p. ex., radiographie)
- Visites à l'urgence
- Renseignements sur les soins à domicile et les soins de longue durée
- Rapports ou sommaires de congé
- Rapports sur les mesures de contrôle des infections
- Rapports de laboratoire
- Antécédents médicaux
- Renseignements sur les médicaments et les services en pharmacie
- Renseignements sur la santé mentale et les dépendances
- Rapports neurophysiologiques
- Rapports de consultation
- Données démographiques

- Rapports respiratoires
- Renseignements sur les visites et les rencontres

On trouvera en annexe de plus amples renseignements sur les répertoires de données qui contiennent ces renseignements et sur les moyens de les consulter.

Conditions préalables

Conditions techniques

- Avoir un authentifiant ONE ID ou un accès fédéré pour se connecter à un système d'information clinique;
- Avoir la configuration minimale requise (système et navigateur de réseau).

Autres conditions

- Être un dépositaire de renseignements sur la santé (DRS) ou avoir l'autorisation d'un DRS;
- Signer des accords juridiques;
- Répondre aux exigences en matière de protection de la vie privée et de sécurité.

Responsabilités

Responsabilités de Santé Ontario

Il incombe à Santé Ontario :

- de mettre en tout temps à la disposition des fournisseurs de soins de santé inscrits au système les données des DSE et les fonctionnalités de consultation décrites dans le présent document;
- de limiter l'accès aux dossiers contenus dans les répertoires de données dont l'accès a été restreint en vertu d'une ou de plusieurs directives en matière de consentement données par le patient;
- de donner temporairement accès à l'information sur la santé d'un patient se trouvant dans les répertoires de données et qui avait été restreinte en vertu de directives en matière de consentement quand le fournisseur de soins de santé passe outre ces directives avec l'accord du patient ou de son mandataire spécial (MS), ou si les circonstances exigent des soins médicaux pour réduire le risque de lésion corporelle pour le patient ou une autre personne (s'il est permis de le faire);
- de répondre aux questions ou aux préoccupations concernant la protection de la vie privée relativement aux données consultées dans le DSE;
- de mettre à jour les données des répertoires de données des DSE pour accroître et améliorer les fonctions et les sources de données fournies;

- d'évaluer les mesures de sécurité et de protection de la vie privée afin que la collecte, le stockage, l'utilisation et la divulgation des renseignements personnels et des RPS soient conformes à la loi et aux exigences en matière de protection de la vie privée;
- d'offrir son soutien et son expertise pour déterminer les obligations et les exigences de sécurité auxquelles doivent se conformer les fournisseurs de soins de santé et leur donner des recommandations. Les fournisseurs doivent se conformer à certaines exigences en fonction du nombre d'utilisateurs, des méthodes d'accès et du degré d'intégration au DSE;
- d'aider les fournisseurs à s'acquitter de leurs obligations juridiques concernant les demandes d'accès aux renseignements personnels et leur rectification.

Responsabilités des fournisseurs de soins de santé

- Les fournisseurs de soins de santé doivent communiquer avec leur agent de liaison en gestion des comptes afin de déterminer s'ils ont besoin de faire l'évaluation de la sécurité ou si le respect des exigences énumérées plus bas suffit.

Responsabilités des fournisseurs de données

Les fournisseurs de soins de santé qui alimentent les DSE sont tenus de :

- se conformer aux politiques sur la sécurité et la protection de la vie privée lorsqu'ils alimentent le DSE. La liste complète des politiques se trouve à la section Documents connexes;
- remplir l'évaluation de sécurité des DSE pour les organisations fédérées ou fournissant des données et se soumettre à ses exigences.

Responsabilités des fournisseurs de services d'authentification

Les fournisseurs de services d'authentification sont des organisations qui mettent à profit la technologie et tout service de soutien, politique, processus et procédure afférent pour créer, conserver, sécuriser, valider, vérifier et gérer l'identification électronique des dossiers de santé électronique. Ils sont tenus de :

- se conformer aux exigences de la politique et des normes de Santé Ontario relatives aux fournisseurs de services d'authentification;
- se conformer aux politiques sur la sécurité du DSE lorsqu'ils offrent des services de gestion de l'identité. La liste complète des politiques se trouve à la section Documents connexes;
- remplir l'évaluation de sécurité des DSE pour les organisations fédérées ou fournissant des données et se soumettre à ses exigences.

Responsabilités en lien avec le respect de la vie privée lors de la consultation des DSE

Les fournisseurs de soins de santé et le bureau de la protection de la vie privée (le cas échéant) qui consultent les données du DSE sont tenus de respecter les obligations énoncées dans l'entente d'accès correspondante, conclue entre Santé Ontario et eux-mêmes ou leur organisation et :

- d'accepter de se conformer aux politiques de confidentialité sur le DSE mentionnées à la section Documents connexes et d'assurer la protection de la vie privée et de garantir la sécurité dans le cadre de l'utilisation des produits de Santé Ontario, en plus de mettre en place les politiques de confidentialité et de sécurité relatives aux DSE, s'il y a lieu, et d'aider les usagers à s'y conformer;
- d'utiliser les DSE uniquement à des fins cliniques autorisées;
- de toujours indiquer le nom de la personne ou de l'organisation pour le compte duquel l'utilisateur emploie le DSE pour consulter les renseignements sur la santé des patients;
- d'obtenir le consentement du patient ou celui du mandataire spécial, ainsi que son nom et la relation qu'il entretient avec le patient avant de demander une dérogation temporaire des directives en matière de consentement données par le patient pour avoir accès aux renseignements sur sa santé;
- signaler les atteintes à la vie privée et les incidents relatifs à la protection de la vie privée ou à la sécurité (réels ou présumés) et contribuer aux investigations;
- suivre la formation annuelle pour les utilisateurs finaux sur la protection de la vie privée et la sécurité (s'il y a lieu);
- répondre aux questions, aux inquiétudes ou aux demandes des patients en matière de confidentialité (demande d'accès, de rectification, de directives en matière de consentement) ou les diriger vers le groupe ou le secteur approprié;
- vérifier et surveiller l'activité des utilisateurs dans le DSE et préparer des rapports de conformité.

Responsabilités en lien avec la sécurité lors de la consultation des DSE

Ci-dessous se trouvent les exigences minimales des politiques et normes sur la sécurité de la solution de DSE. Tous les fournisseurs de soins de santé qui utilisent le DSE doivent s'y conformer complètement.

Sécurité de l'information

- Les fournisseurs de soins de santé doivent, pour leur organisation, élaborer, mettre en œuvre et tenir à jour une politique de sécurité de l'information et des normes et procédures qui respectent les Politiques et normes – DSE.

Utilisation acceptable des données et des technologies de l'information

- Les mots de passe doivent répondre aux critères suivants :
    - Le mot de passe doit contenir au moins huit caractères et se composer de lettres majuscules et minuscules, de chiffres et de caractères spéciaux (!, $, #, _, ~, %, ^, etc.);
    - Il doit être difficile à deviner et ne doit pas se trouver dans un dictionnaire de la langue courante;

- On ne doit pas y trouver de date d'anniversaire ou d'événement important, de numéro séquentiel ou le nom d'un membre de sa famille ou d'un animal de compagnie;
- Il ne doit jamais comporter trois caractères consécutifs (p. ex., AAA).

- Le mot de passe ne doit jamais être écrit ou communiqué à une autre personne.
- Le mot de passe du compte doit être changé au moins tous les 90 jours.
- Il doit être changé immédiatement si l'utilisateur soupçonne ou découvre que son mot de passe a été divulgué ou compromis; l'utilisateur doit aussi signaler immédiatement l'incident à la personne-ressource à l'interne désignée dans le processus de gestion des incidents en lien avec la sécurité.

Gestion des appareils et des procédures servant à participer à la solution de DSE

- Utiliser uniquement les systèmes, appareils et processus approuvés pour une utilisation à des fins cliniques par les fournisseurs de soins de santé (aucun appareil personnel non approuvé), sur place ou à distance (p. ex., postes de travail pour la pratique, outils d'accès à distance dotés de systèmes de cryptage du disque, de mots de passe, d'antivirus).
- Si des RPS sont sauvegardés sur un appareil mobile sans fil (téléphone, ordinateur portable, tablette), s'assurer que le disque sur lequel sont sauvegardées les données est crypté ou que le système de l'utilisateur effectue un cryptage intégral du disque.
- Les fournisseurs de soins de santé doivent crypter le contenu des courriels sensibles ou utiliser une solution de transfert de fichiers sécuritaire comme ONE Mail®, qui crypte les courriels envoyés aux autres utilisateurs du service.

Les fournisseurs de services électroniques

- Les fournisseurs de soins de santé doivent conserver les documents liés aux contrats de services de soutien, aux ententes et aux délais d'intervention conclus avec chaque fournisseur de services électroniques qui leur permet d'utiliser le DSE.
- Les fournisseurs de soins de santé doivent évaluer les risques potentiels que pose un nouveau fournisseur de services électroniques avant de conclure une entente contractuelle avec lui et définir des mesures d'atténuation pour chacun des risques possibles.

Gestion des incidents de sécurité de l'information

- Les fournisseurs de soins de santé doivent désigner une personne-ressource à l'interne (service de dépannage, chef de bureau, agent d'administration) à qui signaler les incidents réels ou présumés pour qu'il y ait enquête.
- Ils doivent veiller à ce que les utilisateurs, leurs mandataires et les fournisseurs de services électroniques sachent qu'ils doivent signaler sur-le-champ tout incident de sécurité de l'information, réel ou présumé.

- Les utilisateurs doivent immédiatement aviser le service de dépannage informatique ou le responsable de la sécurité de l'organisation s'ils ont des raisons de croire ou qu'ils savent que des authentifiants ont été violés ou compromis ou qu'ils pourraient l'être. Le service de dépannage informatique ou l'administrateur système doit aviser Santé Ontario.
- Santé Ontario peut, à sa discrétion, suspendre ou révoquer l'accès à ses produits, à ses services ou à son infrastructure technologique lorsqu'un utilisateur viole toute politique de sécurité qui fait partie des exigences pour la visualisation de données.
- Les fournisseurs de soins de santé doivent collaborer avec Santé Ontario pour la gestion des violations de politiques (gestion des incidents de sécurité de l'information). Cette responsabilité comprend notamment l'aide à la rédaction et à la diffusion de messages concernant les violations ou les incidents.

Réseau et fonctionnement

- Les fournisseurs de soins de santé doivent mettre en place un contrôle de réseau et le gérer de manière à protéger les ordinateurs internes (le réseau) et à les séparer de l'Internet (réseau de périmètre).
- Par exemple, si votre établissement offre une connexion Internet sans fil « invité » aux patients, il faut faire en sorte que ce réseau « invité » soit séparé du réseau interne des fournisseurs de soins de santé, de manière à éviter que des personnes non autorisées ne puissent y accéder.

Logiciels malveillants

- Les fournisseurs de soins de santé doivent utiliser des logiciels de détection des programmes malveillants dans tous les systèmes et appareils utilisés par les fournisseurs de soins de santé qui se servent de la solution de DSE.
- Les fournisseurs de soins de santé doivent s'assurer que les logiciels de détection des programmes malveillants et leurs correctifs sont à jour, conformément au processus de gestion des incidents de sécurité de l'information.

Sécurité matérielle

- Les fournisseurs de soins de santé doivent s'assurer que leur espace de travail est protégé contre tout accès physique non autorisé. Voici quelques méthodes pouvant être employées pour prévenir l'accès physique :
    - Séparer les espaces publics des espaces de travail;
    - Ranger le matériel et les informations sensibles dans des armoires verrouillées;
    - Installer des serrures ou des verrous aux portes et aux fenêtres vulnérables;
    - Installer un système de surveillance avec téléviseur en circuit fermé;

- Installer des systèmes de détection d'intrus sur les portes extérieures et mettre à l'épreuve les fenêtres accessibles régulièrement;
- Les fournisseurs de soins de santé doivent avoir des procédures en place concernant la destruction des renseignements conformément aux orientations du Commissaire à l'information et à la protection de la vie privée de l'Ontario (CIPVP).

Validation de l'identité et gestion des inscriptions

- La personne légalement responsable (ou déléguée) doit :
  - être au fait des pratiques d'enregistrement et d'inscription et en assurer la supervision;
  - s'assurer qu'un approbateur et une autorité locale d'enregistrement sont choisis pour autoriser l'accès individuel. La personne légalement responsable peut être nommée comme approbateur ou autorité locale d'enregistrement. L'autorité locale d'enregistrement est tenue de :
    - valider l'identité de tous les mandataires des fournisseurs de soins de santé qui ont accès à l'information du DSE en utilisant une combinaison de preuves documentaires et contextuelles, ce qui implique l'examen d'au moins une pièce d'identité avec photo délivrée par le gouvernement;
    - confirmer que la personne est âgée d'au moins 16 ans;
    - garder les dossiers sur l'identité à jour (corriger les erreurs ou supprimer les comptes en double).
  - Les organisations participantes doivent veiller à la protection des justificatifs d'identité permettant d'obtenir directement ou indirectement l'accès aux produits, aux services ou à l'infrastructure technologique.
  - Un examen des comptes annuel est effectué pour garantir un accès approprié et à jour.

Considérations sur la sécurité et la protection de la vie privée

Transfert de fichiers sensibles

Les renseignements personnels et les RPS non cryptés ne doivent pas être transmis par courriel à Santé Ontario. En vertu des politiques sur les DSE, des mesures de protection adéquates doivent être prises chaque fois qu'un document ou un fichier contenant des données sensibles est stocké ou transféré au moyen de canaux de communication qui ne sont pas entièrement sûrs (courriel ordinaire, CD, DVD, clé USB, carte mémoire flash, etc.). Pour en savoir plus, consulter l'annexe G.

Directives de consentement *(Nouveau – Octobre 2020)*

Aperçu

D'après l'article 55.6 de la partie V.1 de la *LPRPS*, un particulier peut à tout moment formuler une directive selon laquelle il refuse ou retire, en tout ou en partie, son consentement à la collecte, à l'utilisation et à la divulgation, par un DRS, de RPS le concernant au moyen du DSE en vue de la fourniture ou d'aide à la fourniture des soins de santé qui lui sont destinés.

Si un DRS cherche à recueillir des RPS visés par une directive de consentement, Santé Ontario l'avise que le particulier a formulé une directive de consentement et veille à ce qu'aucun RPS visé par la directive ne soit fourni au DRS, sauf en cas de dérogation à la préséance du consentement.

D'après la *LPRPS*, Santé Ontario peut fournir des RPS contenus dans le DSE à un coroner pour une investigation menée en application de la *Loi sur les coroners*, que les RPS soient visés ou non par une directive de consentement.

De plus, toujours selon la *LPRPS*, le médecin hygiéniste en chef (MHC) ou un médecin-hygiéniste au sens de la *Loi sur la protection et la promotion de la santé* peut recueillir des RPS au moyen du DSE à des fins liées aux fonctions que lui attribue cette loi ou la *Loi sur l'immunisation des élèves*, que les RPS soient visés ou non par une directive de consentement.

Comment formuler, modifier ou retirer une directive de consentement

Le particulier doit se servir du formulaire de demande de directives de consentement – Dossier de santé électronique pour formuler, modifier ou retirer son consentement à la collecte, à l'utilisation et à la divulgation des RPS le concernant dans le DES par un DRS en vue de la fourniture ou d'aide à la fourniture des soins de santé qui lui sont destinés.

Santé Ontario n'accepte que les formulaires soumis par **le particulier que les RPS concernent, ou son mandataire spécial**. Il déploie des efforts raisonnables pour vérifier si le particulier ayant soumis le formulaire est bien celui que les RPS concernent ou qu'il s'agit du mandataire spécial.

À titre d'organisation prescrite, Santé Ontario est habilité à accepter les demandes de directives de consentement en lien avec les RPS que contiennent le Répertoire des données cliniques (RDC) et le dépôt Service commun d'imagerie diagnostique (SC ID).

Le formulaire de demande de directives de consentement – Dossier de santé électronique **ne peut pas** servir à formuler, à modifier ou à retirer une directive de consentement visant le Système d'information de laboratoire de l'Ontario (SILO) ou le Répertoire numérique des médicaments (RNM). Pour faire une de ces actions, le particulier ou son mandataire spécial doit appeler la ligne INFO de ServiceOntario au 1 800 291-1405 (ATS : 1 800 387-5559).

Si Santé Ontario peut raisonnablement appliquer une directive de consentement uniquement aux RPS que le particulier ou son mandataire spécial a indiqués dans le formulaire de demande de directives de consentement – Dossier de santé électronique et que le demandeur a fourni suffisamment de renseignements, il procède de la sorte dans le DSE. Consultez le formulaire pour connaître les options de consentement actuelles.

Pour en savoir plus sur les directives de consentement dans le DSE, consultez la *Politique sur les directives de consentement et la dérogation à la préséance du consentement pour le dossier de santé électronique*, **qui remplace le document *Consent Management Policy, Electronic Health Record* (version 1.3).**

Dérogation à une directive de consentement

Le DSE permet aux fournisseurs de déroger à la directive de consentement d'un particulier pour recueillir les RPS de ce particulier visés par la directive : c'est ce qu'on appelle une dérogation à la préséance du consentement. La *LPRPS* prévoit trois motifs pour lesquels on peut déroger à la préséance du consentement :

- Le fournisseur obtient l'autorisation expresse du particulier ou de son mandataire spécial;
- Le fournisseur a de bonnes raisons de croire qu'il est nécessaire de déroger à la directive pour éliminer ou réduire un risque important de lésion corporelle grave pour le particulier et qu'il n'est pas raisonnablement possible pour le fournisseur d'obtenir le consentement du particulier à temps;
- Le fournisseur a de bonnes raisons de croire qu'il est nécessaire de déroger à la directive pour éliminer ou réduire un risque important de lésion corporelle grave pour une personne autre que le particulier auquel se rapportent les RPS, ou pour un groupe de personnes.

Par ailleurs, les fournisseurs ne peuvent déroger à la préséance du consentement que lorsque le motif invoqué, comme il est indiqué ci-dessus, est autorisé par le DRS ayant la garde et le contrôle des RPS en question, et pris en charge par la technologie. Veuillez noter qu'un DRS qui recueille des RPS en dérogeant à la préséance du consentement ne peut utiliser ou divulguer ces RPS qu'aux fins auxquelles ils ont été recueillis.

Pour en savoir plus sur les dérogations à la préséance du consentement dans le DSE, consultez la *Politique sur les directives de consentement et la dérogation à la préséance du consentement pour le dossier de santé électronique*, **qui remplace le document *Consent Management Policy, Electronic Health Record* (version 1.3).** De plus, prenez connaissance des précisions qui suivent concernant les dérogations à la préséance du consentement.

Santé Ontario avise de la dérogation à la préséance du consentement le DRS dont le mandataire a procédé à la dérogation. Cet avis présente le motif fourni à Santé Ontario au moment de la dérogation. À la réception de cet avis, pour toutes les dérogations et quel que soit le répertoire du DSE touché, le DRS dont le mandataire a procédé à la dérogation doit :

1. enquêter sur la dérogation pour s'assurer qu'elle a été effectuée pour l'un des motifs susmentionnés, et consigner le bon motif;
2. aviser, à la première occasion raisonnable, le particulier dont les renseignements ont été recueillis en dérogeant à la préséance du consentement;
3. si la dérogation visait à éliminer ou à réduire un risque considérable de blessure grave menaçant une personne (autre que le particulier que les RPS concernent) ou un groupe de personnes, aviser le commissaire à l'information et à la protection de la vie privée de l'Ontario (CIPVP), selon la *LPRPS*.

Signature manuscrite exigée pour le Répertoire numérique des médicaments : Pour les dérogations à la préséance du consentement visant des données du Répertoire numérique des médicaments (RNM) effectuées avec le consentement exprès du particulier ou de son mandataire spécial, le fournisseur de soins de santé doit imprimer et remplir le formulaire *Débloquer ponctuellement l'accès à vos renseignements personnels sur les médicaments et les services de pharmacie reçus*[1]. Il doit obtenir du particulier ou de son mandataire spécial une autorisation à déroger à la préséance du consentement pour le RNM et sa signature manuscrite dans le formulaire, qu'il conservera dans ses dossiers, en lieu sûr, à des fins de vérification.

Exigences relatives aux dérogations à la préséance du consentement pour le Système d'information de laboratoire de l'Ontario : Pour les dérogations à la préséance du consentement qui concernent des données du Système d'information de laboratoire de l'Ontario (SILO) faites avec le consentement exprès du particulier ou de son mandataire spécial, le ministère de la Santé, en tant que dépositaire du SILO, exige que le fournisseur inscrive une note dans le dossier du particulier et qu'il lui explique que même si la dérogation est temporaire en ce qui concerne le SILO, les renseignements que le fournisseur a pu consulter seront conservés dans le système et marqués comme étant sensibles, et qu'ils pourraient être accessibles à d'autres fournisseurs qui participent à ses soins.

---

[1] Ministère de la Santé. *Débloquer ponctuellement l'accès à vos renseignements personnels sur les médicaments et les services de pharmacie reçus* (formulaire nº 5047-87F).

De plus, si le mandataire spécial a autorisé une dérogation à la préséance du consentement, le ministère de la Santé, en tant que dépositaire du SILO, exige du fournisseur qu'il inscrive au dossier du particulier le nom du mandataire spécial et son lien avec le particulier. Si l'application ou le visualiseur sur l'ordinateur n'a pas la fonction requise (un système d'enregistrement électronique), le fournisseur doit inscrire manuellement ces renseignements. Il doit fournir cette information à Santé Ontario sur demande.

Information sur la dérogation à la préséance du consentement avec autorisation expresse pour le visualiseur clinique de ConnexionOntario : Une dérogation à la préséance du consentement faite dans le visualiseur clinique de ConnexionOntario, avec le consentement exprès du particulier (option nº 1 dans la boîte de dialogue « Consent Override ») ou de son mandataire spécial (option nº 2), aura pour effet de démasquer tous les portlets du SILO, du RNM et du RDC qui comportent des données visées par la directive de consentement du particulier. Les données du RNM (dans l'onglet « Dispensed Medications » du visualiseur clinique) ne sont peut-être pas nécessaires pour prodiguer des soins, mais si des données du particulier dans le RNM sont visées par une directive de consentement, puis par une dérogation à la préséance du consentement exprès dans un autre portlet, le système démasquera aussi ces données du RNM. Dans ce cas, vous devrez remplir un formulaire de consentement exprès du RNM en plus de la boîte de dialogue « Consent Override » pour fournir la signature manuscrite exigée, comme il est indiqué plus haut. Si vous sélectionnez l'option nº 3 (risque considérable de blessure grave) dans la boîte de dialogue « Consent Override », le système démasquera uniquement les portlets du RDC sur les soins actifs et communautaires (« Visits/Encounters », « Documents/Notes », « Other Results » et « Community »). Veuillez noter que si vous sélectionnez l'une des trois options susmentionnées pour une dérogation à la préséance du consentement dans le visualiseur clinique de ConnexionOntario, le système ne démasquera pas l'information dans le portlet « Diagnostic Imaging », car le visualiseur clinique ne prend actuellement pas en charge les dérogations à la préséance du consentement visant des données du dépôt Service commun d'imagerie diagnostique.

Demandes d'accès *(Nouveau – Octobre 2020)*

Demandes d'accès faites par des particuliers

La *Loi de 2004 sur la protection des renseignements personnels sur la santé* (*LPRPS*) donne aux particuliers ou à leur mandataire spécial le droit d'accéder aux RPS qu'un DRS conserve au sujet du particulier, et définit une procédure officielle pour les demandes d'accès. Les DRS qui recueillent, utilisent et divulguent des RPS au moyen du DSE doivent continuer de remplir leurs obligations liées aux demandes d'accès conformément à la partie V de la *LPRPS* et de répondre directement au demandeur, ce qui vaut aussi pour les demandes d'accès à l'information tirée du DSE et intégrée au dossier clinique du DRS.

À titre d'organisation prescrite, Santé Ontario continue d'agir comme mandataire au sens de la *LPRPS* en aidant les DRS contributeurs avec le processus administratif associé aux demandes d'accès aux dossiers de RPS accessibles au moyen du DSE dans le respect de toutes les lois applicables et des conditions de la convention des contributeurs de DSE.

Demandes d'accès aux dossiers de RPS ajoutés au DSE par un ou plusieurs DRS

À partir de maintenant, Santé Ontario n'enverra plus les données demandées au demandeur au nom des DRS. La nouvelle version de la *Politique sur les demandes d'accès aux renseignements personnels sur la santé contenus dans un dossier de santé électronique* (2020) apporte des précisions à ce sujet : les DRS sont désormais chargés de soumettre eux-mêmes les données demandées directement au demandeur, conformément à la partie V de la *LPRPS*.

Quand la demande d'accès touche des données ajoutées par un autre DRS ou par plusieurs DRS, le DRS ayant reçu la demande doit :

- aviser le demandeur que sa demande concerne des RPS dont il n'a pas la garde;
- indiquer au demandeur de communiquer avec Santé Ontario au 416 946-4767 ou au 1 888 411-7742, poste 64767;
- dire au demandeur de remplir le formulaire de demande d'accès et de rectification – Dossier de santé électronique et de communiquer directement avec Santé Ontario pour des dossiers liés au Répertoire des données cliniques sur les soins actifs et communautaires (RDC sur les soins actifs communautaires) et au dépôt Service commun d'imagerie diagnostique (SC ID).

N. B. : Les demandeurs doivent acheminer leurs demandes d'accès comme suit :

- Pour le Répertoire numérique des médicaments **(RNM)**, il faut appeler la ligne INFO de ServiceOntario au 1 800 291-1405 (ATS : 1 800 387-5559).

- Pour le Système d'information de laboratoire de l'Ontario **(SILO)**, il faut utiliser les coordonnées suivantes : ministère de la Santé, Bureau de l'accès à l'information et de la protection de la vie privée, 99 Adesso Drive, 1st floor Concord (Ontario) L4K 3C7; 416 327-7040; **ou** generalapo@ontario.ca.

- Pour le Répertoire des données cliniques sur les soins primaires **(RDC sur les soins primaires)**, il faut communiquer avec le bureau du programme ClinicalConnect de la région du Sud-Ouest, par téléphone au 905 577-8270, poste 9, ou par courriel, à privacy@clinicalconnect.ca.

Demandes concernant les registres d'accès

Selon la partie V de la *LPRPS*, à titre d'organisation prescrite, Santé Ontario n'est pas tenu de donner accès aux particuliers aux rapports de vérification portant sur le DSE, notamment les suivants :

- Dossiers répertoriant l'ensemble des consultations, traitements ou autres actions visant l'intégralité ou une partie des RPS par les DRS, ou leurs mandataires et fournisseurs de services électroniques;
- Dossiers répertoriant les formulations, retraits ou modifications d'une directive de consentement par le particulier;
- Dossiers répertoriant les dérogations à la préséance du consentement d'un particulier et les motifs connexes.

Pour en savoir plus sur les demandes d'accès et les registres d'accès, consultez la *Politique sur les demandes d'accès aux renseignements personnels sur la santé contenus dans un dossier de santé électronique*, entrée en

vigueur le 1er octobre 2020 et **remplaçant la *Politique sur l'accès aux renseignements et la rectification des renseignements – Dossier de santé électronique* datée du 17 mars 2016**.

N. B. : Santé Ontario continuera de fournir sur demande des registres d'accès aux DRS concernés à des fins de satisfaction des exigences de vérification et de surveillance prévues à la partie V.1 de la *LPRPS*.

Demandes de rectification *(Nouveau – Octobre 2020)*

Selon la *LPRPS*, si un particulier estime qu'un dossier de RPS n'est pas assez exact ou complet aux fins auxquelles il est destiné, il peut demander par écrit au DRS de le rectifier. C'est au DRS qu'il incombe de s'assurer que les RPS sont complets et exacts. Par conséquent, les DRS qui recueillent, utilisent et divulguent des RPS au moyen du DSE doivent continuer de remplir leurs obligations concernant les demandes de rectification, conformément à la partie V de la *LPRPS*, et de répondre directement au particulier présentant une demande en ce sens.

Demandes de rectification touchant un dossier de RPS dans le DSE auquel un seul DRS a contribué

Quand un DRS reçoit directement du particulier une demande de rectification concernant des RPS ajoutés au DSE créé uniquement par lui, il doit observer la partie V de la *LPRPS* et répondre directement au particulier.

Après la rectification, le particulier peut exiger que le DRS, dans la mesure où il est raisonnablement possible de le faire, avise toutes les personnes à qui les renseignements ont été divulgués, sauf s'il n'y a pas raisonnablement lieu de s'attendre à ce que la rectification puisse avoir des répercussions sur la fourniture continue de soins de santé ou d'autres avantages au particulier.

Demandes de rectification touchant un dossier de RPS dans le DSE auquel plusieurs DRS ont contribué

Quand une demande de rectification touche de l'information ajoutée par un autre DRS ou plusieurs DRS, le DRS ayant reçu la demande doit :

- aviser le demandeur que sa demande concerne des RPS dont il n'a pas la garde;
- indiquer au demandeur de communiquer avec Santé Ontario au 416 946-4767 ou au 1 888 411-7742, poste 64767;
- dire au demandeur de remplir le formulaire de demande d'accès et de rectification – Dossier de santé électronique et de communiquer directement avec Santé Ontario pour les dossiers liés au Répertoire des données cliniques sur les soins actifs et communautaires (RDC sur les soins actifs et communautaires) et au dépôt Service commun d'imagerie diagnostique (SC ID).

À titre d'organisation prescrite, Santé Ontario continuera d'agir comme mandataire au sens de la *LPRPS* en aidant les DRS contributeurs avec le processus administratif associé aux demandes de rectification de dossiers de RPS accessibles au moyen du DSE dans le respect de toutes les lois applicables et des conditions de la convention des contributeurs de DSE.

N. B. : Les demandeurs doivent acheminer leurs demandes de rectification comme suit :

- Pour le Répertoire numérique des médicaments **(RNM)**, il faut écrire au ministère de la Santé, Direction de la mise en œuvre des programmes de médicaments, Division des programmes publics de médicaments de l'Ontario, au 5700, rue Yonge, 3e étage, Toronto (Ontario) M2M 4K5.
- Pour le Système d'information de laboratoire de l'Ontario **(SILO)**, il faut communiquer avec le ministère de la Santé par téléphone au 416 327-7040 ou par courriel à generalapo@ontario.ca.
- Pour le Répertoire des données cliniques sur les soins primaires **(RDC sur les soins primaires)**, il faut communiquer avec le bureau du programme ClinicalConnect de la région du Sud-Ouest par téléphone au 905 577-8270, poste 9, ou par courriel à privacy@clinicalconnect.ca.

Pour en savoir plus sur les demandes de rectification, consultez la nouvelle version de la *Politique sur les demandes de rectification de renseignements personnels sur la santé contenus dans un dossier de santé électronique*, entrée en vigueur le 1er octobre 2020 et **remplaçant la *Politique sur l'accès aux renseignements et la rectification des renseignements – Dossier de santé électronique* datée du 17 mars 2016.**

Formulaire de demande d'accès et de rectification – Dossier de santé électronique (version révisée)

Prenez note qu'une nouvelle version du formulaire de demande d'accès et de rectification – Dossier de santé électronique est maintenant disponible sur notre site Web. Ce formulaire indique les coordonnées des entités auxquelles il faut s'adresser pour les demandes d'accès et de rectification touchant les répertoires de données cliniques suivants :

- Répertoire des données cliniques sur les soins actifs et communautaires (RDC sur les soins actifs et communautaires)
- Répertoire des données cliniques sur les soins primaires (RDC sur les soins primaires)
- Dépôt Service commun d'imagerie diagnostique (SC ID)
- Répertoire numérique des médicaments (RNM)
- Système d'information de laboratoire de l'Ontario (SILO)

Plaintes et demandes d'information sur la protection de la vie privée

Si le DRS reçoit une plainte ou une demande d'information concernant uniquement ses dossiers dans le DSE, ceux de ses mandataires ou de ses fournisseurs de services, il doit suivre ses politiques, ses procédures et ses pratiques internes pour traiter la demande.

Si le DRS reçoit directement une demande d'information ou une plainte concernant exclusivement le DSE ou les mandataires ou fournisseurs de services électroniques de Santé Ontario, et qu'il est incapable de la traiter, il doit :

- aviser la personne que le DRS n'est pas en mesure de répondre à sa demande ou à sa plainte;
- inviter le patient à communiquer avec Santé Ontario au 1 866 250-1554.

Santé Ontario peut demander l'aide du ou des DRS pour répondre directement à la demande ou à la plainte reçue.

N. B. : Comme l'indiquent les formulaires, le patient (ou son mandataire spécial) doit appeler la ligne INFO de ServiceOntario, sans frais, au 1 800 291-1405 (ATS : 1 800 387-5559) pour toute question ou plainte concernant le RNM. Pour toute question ou plainte concernant le SILO, communiquer avec le Bureau de la protection de la vie privée du ministère de la Santé et des Soins de longue durée au 416 327-7040 ou à l'adresse generalapo@ontario.ca.

Conservation de l'information

Aux termes de la *LPRPS*, les DRS doivent veiller à ce que leurs dossiers soient conservés pendant une période donnée, et transférés et éliminés de manière sécuritaire. Ils doivent également s'assurer que leurs dossiers sont protégés et éliminés conformément à la *Norme sur la gestion de l'information et des éléments d'actif*.

Voici la durée de conservation des dossiers des DRS en fonction des renseignements qu'ils contiennent :

Tableau 2 : Durée de conservation des documents

Type d'information	Durée de conservation
Journaux et rapports de vérification contenant des renseignements personnels sur la santé, créés et conservés à des fins de conformité.	Au maximum 30 ans, ou lorsque les renseignements personnels sur la santé sont supprimés du DSE.
Renseignements recueillis pour traiter les demandes des patients : • demandes d'accès ou de rectification en vertu de la *LPRPS*; • demande de formulation, de modification ou de retrait d'une directive en matière de consentement en vertu de la *LPRPS*; • demande d'information ou plainte en vertu de la *LPRPS*.	Deux ans après la demande. Dans le cas d'une plainte, deux ans après la fermeture du dossier par le DRS, Santé Ontario ou le CIPVP, la période la plus longue devant être retenue.
Renseignements sur un patient créés lors d'une enquête sur une atteinte à la vie privée ou un incident de sécurité.	Deux ans après la fermeture, par le DRS, Santé Ontario ou le CIPVP, du dossier relatif à l'atteinte à la vie privée, la période la plus longue devant être retenue.
Renseignements personnels utilisés aux fins d'inscription auprès du fournisseur d'identité.	Sept ans après la dernière utilisation.
Authentifiants de l'utilisateur final si le DRS est un fournisseur d'identité.	Illimitée.
Journaux système, journaux de suivi, rapports et documents connexes servant à l'exécution de tâches liées à la protection de la vie privée et à la sécurité, et ne renfermant pas de renseignements personnels sur la santé.	Au moins deux ans.
Connexions au système si le DRS est un fournisseur d'identité.	60 jours en ligne et 24 mois en tout dans les archives.
Documents liés aux assurances	10 ans.

Les dossiers contenus dans chacun de ces types de renseignements sont détaillés à l'annexe A de la Politique de confidentialité.

Formation en protection de la confidentialité et en sécurité

Les DRS doivent offrir à leurs fournisseurs de soins une formation sur la sécurité et la protection de la vie privée avant que ces derniers n'accèdent au DSE[2]. Cette formation vise à les informer de leurs obligations en vertu des lois applicables sur la vie privée (comme la *LPRPS*) et des politiques et procédures pertinentes sur la sécurité et la vie privée en lien avec le DSE en incorporant le contenu de la *Politique sur la formation en protection de la confidentialité et de la sécurité*. Santé Ontario a mis au point des aides didactiques associées aux différents postes pour faciliter le processus. On peut les trouver dans la boîte à outils sur la confidentialité du DSE et la boîte à outils sur la sécurité du DSE. Les fournisseurs doivent suivre la formation en protection de la confidentialité et en sécurité avant qu'un compte à leur nom ne soit créé dans le DSE. Les utilisateurs finaux doivent obligatoirement avoir reçu la formation pertinente sur la protection de la vie privée avant de pouvoir accéder au système.

Les DRS sont tenus de garder une trace des mandataires, des fournisseurs de services électroniques et des utilisateurs finaux qui ont reçu une formation sur la sécurité et la protection de la vie privée. Une fois la formation initiale terminée, les DRS doivent offrir une formation annuelle sur ce thème.

Questions des établissements de soins de santé sur la protection de la vie privée

Pour toute question relative aux processus de protection de la vie privée décrits ci-dessus, notamment à la façon de répondre aux demandes d'accès des patients, aux obligations de consentement ou aux processus de gestion des atteintes à la vie privée ou des incidents, les fournisseurs de soins de santé peuvent consulter le responsable de la protection de la vie privée de leur établissement comme ressource première. Ils peuvent par la suite consulter le Bureau de la protection de la vie privée de Santé Ontario en appelant au 1 866 250-1554.

Assurez-vous de n'inclure aucun renseignement personnel, sur la santé ou autre, dans vos courriels à Santé Ontario.

[2] Pour l'instant, cette formation ne concerne que ConnexionOntario, le RDC, et le RNM.

Demandes de rapports de vérification en matière de protection de la vie privée

En votre qualité de DRS, il se peut que vous deviez obtenir un rapport de vérification concernant le DSE afin de répondre aux exigences de vérification. S'il vous est impossible de le faire en utilisant les journaux de votre propre système interne, vous pouvez demander à Santé Ontario de vous en fournir un. Voici quelques exemples des rapports que peut fournir Santé Ontario :

Type de rapport	Description
Vérification mensuelle des utilisateurs finaux	Nom des patients dont les dossiers ont été consultés par tous les utilisateurs du DRS sur une période d'un mois.
Vérification trimestrielle des utilisateurs finaux	Nom des patients dont les dossiers ont été consultés par tous les utilisateurs du DRS sur une période de quatre mois.
Rapport d'accès aux RPS par l'utilisateur	Nom des patients dont les dossiers ont été consultés par un utilisateur du DRS en particulier.

Tableau 3 : Types des rapports de vérification

- Rapport de vérification par établissement : Santé Ontario vous fournira un rapport répertoriant tous les utilisateurs de votre établissement ayant consulté des données du DSE pendant la période précisée dans la demande.
- Rapport de vérification par utilisateur : Santé Ontario vous fournira un rapport répertoriant toutes les fois où un utilisateur de votre établissement a consulté des données du DSE pendant la période précisée dans la demande.
- Demande d'accès aux RPS par patient : Santé Ontario vous fournira un rapport répertoriant toutes les fois où les utilisateurs de votre établissement ont consulté des données du DSE concernant un patient en particulier pendant la période précisée dans la demande.
- Dérogation aux directives en matière de consentement obtenues par établissement : Santé Ontario vous fournira une liste de toutes les dérogations aux directives en matière de consentement qui ont été accordées aux utilisateurs de votre établissement pendant la période précisée dans la demande.

- Historique des directives en matière de consentement obtenues par établissement : Santé Ontario vous fournira une liste de tous les changements aux directives en matière de consentement demandées par votre établissement pendant la période précisée dans la demande.

N. B. : Ces demandes doivent être faites par le bureau de la protection de la vie privée de votre établissement. S'il n'y en a pas, vous pouvez communiquer directement avec Santé Ontario.

Pour faire la demande d'un rapport de vérification, appelez le Service de dépannage de Santé Ontario au 1 866 250-1554 et précisez pour quel élément du DSE vous souhaitez avoir un rapport.

Gestion des incidents et des violations touchant la protection de la vie privée *(Nouveau – Octobre 2020)*

Un incident touchant la protection de la vie privée s'entend de ce qui suit :

- une violation des politiques, procédures ou pratiques de protection de la vie privée mises en œuvre par votre établissement ou toute politique applicable de Santé Ontario, lorsque cette violation ne constitue pas un manquement à la législation applicable sur la protection de la vie privée ou un non-respect des obligations et restrictions définies dans l'entente contenue entre Santé Ontario et votre organisation;
- une violation de toute entente conclue entre Santé Ontario et votre établissement, lorsque la violation ne constitue pas un manquement à la législation applicable sur la protection de la vie privée ou un non-respect des obligations et restrictions définies dans l'entente conclue entre Santé Ontario et votre organisation;
- une violation touchant la protection de la vie privée.

Une violation touchant la protection de la vie privée s'entend de ce qui suit :

- la collecte, l'utilisation ou la divulgation de renseignements personnels, sur la santé ou autres, en infraction à la législation applicable sur la protection de la vie privée;
- toute autre situation où des renseignements personnels ou des RPS sont collectés, utilisés, divulgués, copiés, modifiés, conservés ou éliminés sans autorisation, ce qui comprend le vol ou la perte accidentelle des renseignements personnels et des RPS.

Le processus de gestion des violations et des incidents touchant la protection de la vie privée ne s'applique pas à la gestion des incidents ou violations internes aux DRS et ne vise pas les DRS, leurs mandataires ou leurs fournisseurs de services électroniques qui ne créent ou ne consultent pas de RPS dans le DSE ou ne contribuent pas au DSE.

Dans les cas où la violation est causée par un DRS qui est le seul à avoir créé et ajouté les RPS dans le DSE, le DRS doit suivre ses politiques, ses procédures et ses pratiques internes pour aviser, à la première occasion raisonnable, le ou les patients touchés, conformément à la *LPRPS* et pour contenir la violation touchant la protection de la vie

privée, faire enquête et corriger le problème. Une fois qu'un DRS a déterminé qu'une violation touchant la protection de la vie privée a eu lieu, son bureau ou son mandataire responsable de la protection de la vie privée doit la signaler à Santé Ontario.

Instructions à l'intention des fournisseurs de soins de santé

Si vous êtes témoin ou soupçonnez l'existence d'une violation ou d'un incident touchant la protection de la vie privée en lien avec les RPS contenus dans le DSE dont vous-même ou l'un de vos employés, mandataires ou fournisseurs de services êtes à l'origine, vous devez le signaler immédiatement à votre bureau ou mandataire responsable de la protection de la vie privée. Si un tel bureau ou mandataire n'existe pas ou si vous ne parvenez pas à les joindre ou à joindre l'équipe de soutien, communiquez avec le Bureau de la protection de la vie privée de Santé Ontario par téléphone au 416 946-4767 ou par courriel à OH-DS_privacyoperations@ontariohealth.ca et indiquez que vous souhaitez signaler une violation ou un incident touchant la protection de la vie privée.

Il est extrêmement important de ne pas divulguer de renseignements personnels sur le patient ou de RPS à Santé Ontario lorsque vous signalez une violation ou un incident touchant la protection de la vie privée.

Vous devez prêter votre concours à toute enquête menée par Santé Ontario sur la violation ou l'incident en lien avec des RPS contenus dans le DSE. Durant l'enquête, il se peut que l'on vous demande de fournir des renseignements supplémentaires, notamment des renseignements personnels, sur la santé ou autres, pour rectifier le tir et limiter les répercussions. Tout renseignement personnel, sur la santé ou autre, doit être envoyé par courriel dans un document crypté conformément à la *Procédure de transfert de fichiers sensibles par courriel*, qui se trouve à l'annexe G.

Instructions à l'intention des responsables de la protection de la vie privée

Si vous êtes témoin ou soupçonnez l'existence d'une violation ou d'un incident touchant la protection de la vie privée en lien avec les RPS contenus dans le DSE par un membre du personnel de votre établissement, que ce soit un employé, un mandataire ou un fournisseur de services, vous devez le signaler immédiatement[3] au Bureau de la protection de la vie privée de Santé Ontario par téléphone au 416 946-4767 ou par courriel à OH-DS_privacyoperations@ontariohealth.ca et indiquer que vous souhaitez signaler une violation ou un incident touchant la protection de la vie privée.

Dans les cas où la violation touchant la protection de la vie privée est seulement causée par un DRS qui n'est pas le seul à avoir créé et ajouté les renseignements personnels sur la santé dans le DSE, le DRS doit, en collaboration avec les autres DRS ayant ajouté des données et Santé Ontario, désigner la personne qui devra diriger l'enquête.

[3] Si l'atteinte ou l'incident concerne ConnexionOntario, le RDC ou le SC ID, il faut le signaler le plus tôt possible, mais au plus tard à la fin du prochain jour ouvrable, une fois que le DRS a conclu que l'atteinte à la vie privée a bien eu lieu ou s'il a un soupçon raisonnable qu'il y a eu atteinte.

Pour en savoir plus sur la gestion des incidents et violations touchant la protection de la vie privée, consultez la nouvelle version de la *Politique sur les incidents et violations touchant la protection de la vie privée – Dossier de santé électronique*, entrée en vigueur le 1er octobre 2020 et ***remplaçant le document Electronic Health Record Privacy Incidents and Privacy Breaches Policy daté du 6 juillet 2016.***

Gestion des incidents en matière de sécurité

La marche à suivre en cas d'incident lié à la sécurité est décrite en détail dans la *Norme sur la gestion des incidents de sécurité de l'information*.

Constitue un incident lié à la sécurité toute violation ou menace imminente de violation des politiques, normes, procédures ou pratiques de sécurité, ou tout incident qui pourrait compromettre l'utilisation ou menacer la sécurité d'un système d'information ou des processus opérationnels.

Si vous avez connaissance ou soupçonnez l'existence d'une atteinte à la confidentialité ou d'un incident de sécurité en lien avec le DSE ou ses données causés par vous-même ou l'un de vos employés, mandataires ou fournisseurs de services, vous devez le signaler immédiatement à votre bureau de la sécurité. Si vous n'en avez pas, ou que vous n'êtes pas en mesure de communiquer avec lui ou avec l'équipe de soutien pour signaler une infraction, veuillez communiquer avec le service de dépannage de Santé Ontario au 1 866 250-1554 pour demander l'ouverture d'un dossier relatif à une atteinte à la sécurité.

Le DRS doit informer Santé Ontario, avant la fin du prochain jour ouvrable, s'il a connaissance d'un incident lié à la sécurité, réel ou présumé, causé en totalité ou en partie par :

- un autre DRS ou un mandataire ou un fournisseur de services électroniques d'un autre DRS;
- plusieurs DRS ou les mandataires ou fournisseurs de services électroniques de plusieurs autres DRS;
- Santé Ontario ou ses mandataires ou fournisseurs de services électroniques;
- toute autre personne non autorisée qui n'est ni mandataire ni fournisseur de services électroniques de Santé Ontario ou de tout autre DRS.

Important : Lorsque vous signalez une atteinte ou une infraction à la sécurité au Service de dépannage, vous ne devez en aucun cas divulguer des renseignements personnels sur les patients ou sur leur santé. Vous devrez prêter votre concours à toute enquête menée par Santé Ontario sur l'atteinte ou l'incident en lien avec les données.

Vous devrez prendre part aux mesures d'atténuation des incidents ou des atteintes à la confidentialité, ou à l'enquête menée par Santé Ontario. Durant l'enquête de Santé Ontario, il se peut que l'on vous demande de fournir des renseignements supplémentaires, notamment des renseignements personnels, sur la santé ou autres, pour rectifier le tir et limiter les répercussions.

Lorsque vous signalez un incident réel ou présumé, veuillez avoir les renseignements suivants sous la main :

- L'heure et la date de l'incident signalé.
- Le nom et les coordonnées du mandataire ou du fournisseur de services électroniques qui a signalé l'incident.
- Une description de l'incident (p. ex., le type d'incident et la façon dont il a été détecté).
- Les conséquences de l'incident.
- Les mesures prises pour contenir l'incident soit par le mandataire ou le fournisseur de services électroniques qui a signalé l'incident, soit par la personne-ressource.

Une fois le dossier d'incident créé par le Service de dépannage, l'équipe de Santé Ontario en charge de la sécurité s'occupera de la situation. Votre établissement pourrait avoir à gérer les activités de rétablissement.

Instructions pour les responsables de la sécurité

Si vous êtes témoin ou soupçonnez l'existence d'une atteinte à la vie privée ou d'un incident relatif à la protection de la vie privée ou à la sécurité en lien avec les données du DSE par un membre du personnel de votre établissement, que ce soit un employé, un mandataire ou un fournisseur de services, vous devez le signaler immédiatement[4] au service de dépannage de Santé Ontario au 1 866 250-1554 et lui demander de créer un dossier d'atteinte à la vie privée ou d'incident.

Annexe A : Répertoire des données cliniques (RDC)

Présentation

Le RDC est un répertoire de données de Santé Ontario dans lequel les hôpitaux et les fournisseurs de soins de santé en milieu communautaire autorisés peuvent consulter des données cliniques provenant d'établissements de soins actifs et primaires. Les données peuvent comprendre des rapports cliniques (p. ex., rapports de soins à domicile et en milieu communautaire, sommaires de congés, rapports des services d'urgence, visites et rencontres), ainsi que des éléments tirés du profil historique du patient qui se trouve dans le dossier médical électronique (DME). Le RDC met à la disposition des fournisseurs des renseignements importants qui leur permettent de prendre des décisions éclairées lorsqu'ils traitent les patients.

[4] Si l'atteinte ou l'incident concerne ConnexionOntario, le RDC ou le SC ID, il faut le signaler le plus tôt possible, mais au plus tard à la fin du prochain jour ouvrable, une fois que le DRS a conclu que l'atteinte à la vie privée a bien eu lieu ou s'il a un soupçon raisonnable qu'il y a eu atteinte.

Grâce aux technologies de l'information, le RDC recense, recueille et consigne les données prioritaires provenant de bases de données et de répertoires existants comme les systèmes d'information hospitaliers ou les dossiers médicaux électroniques.

Avantages

Avantages pour vous

- Amélioration de la qualité des soins et de l'expérience.
    - Réduction des chevauchements et de la frustration.
    - Amélioration de l'accès à l'information sur le lieu des soins.
    - Amélioration de la transition entre les fournisseurs de soins de santé.
    - Amélioration de la productivité et de la satisfaction.
- Amélioration de l'efficacité de la prise de décision et de la capacité de surveiller les résultats en matière de santé.
    - Accès en ligne à des renseignements intégrés sur les soins de santé.
    - Contribution à l'amélioration des soins interprofessionnels et de la coordination des services.
    - Amélioration de la coordination et des capacités organisationnelles et du système.
- Accélération de l'élaboration et de l'envoi des dossiers de santé électroniques.
    - Réalisation d'importantes économies permettant l'adoption d'une démarche intégrée et durable pour la gestion, la coordination et la planification des soins.
    - Établissement d'éléments fondamentaux de technologie de l'information (TI) qui peuvent servir à d'autres programmes de santé organisationnels, régionaux et provinciaux.

Avantages pour vos patients

- Prestation de soins de santé de meilleure qualité, plus rapide et mieux coordonnée.

Annexe B : Système d'information de laboratoire de l'Ontario (SILO)

Présentation

Le SILO est un répertoire provincial contenant des données de laboratoire qui peuvent être consultées au moyen d'un visualiseur clinique. Peuvent être ajoutées au SILO des données provenant de plusieurs sources : laboratoires de Santé publique Ontario, laboratoires communautaires ou laboratoires d'hôpitaux. L'objectif est de consigner

dans le SILO la totalité des résultats d'analyses en laboratoire effectuées dans la province. Pour consulter la liste à jour des fournisseurs de données actuels et prendre connaissance des dernières nouvelles concernant le SILO, visitez l'adresse https://www.ehealthontario.on.ca/fr/for-healthcare-professionals/digital-health-services/view/olis.

Avantages

Avantages pour vous

- Accès rapide et sécurisé aux renseignements lors de la prise de décisions sur le lieu des soins.
- Facilitation de l'accès à des résultats plus complets et diversifiés d'analyse en laboratoire effectués ailleurs que dans votre établissement.
- Intégration et suivi des analyses en laboratoire pour un patient, suivi de l'évolution du traitement et prise en charge des maladies chroniques grâce à un outil efficace.
- Amélioration de la coordination des soins entre plusieurs praticiens et entre les membres de l'équipe de soins.
- Amélioration du flux de travail et réduction de la dépendance à l'égard des systèmes sur support papier.

Avantages pour vos patients

- Réduction des lacunes dans l'information sur les patients lorsqu'ils reçoivent des soins dans plusieurs endroits différents : hôpitaux, bureaux de praticiens (médecin de famille, spécialiste), soins à domicile et soins de longue durée.
- Réduction des doublons ou des examens inutiles grâce à une plus grande accessibilité et au partage de l'information.
- Meilleure prise de décisions au sein de l'équipe de soins, ce qui améliore les résultats pour la santé.

Étapes d'une recherche par patient

La nouvelle fonction du SILO pourrait avoir l'air différente d'un visualiseur clinique à l'autre. Votre établissement vous offrira une formation propre à votre système. Peu importe le système utilisé, la recherche par patient se fera selon ces étapes :

1. Sélectionnez un patient (p. ex., en consultant son dossier).
2. Filtrez les résultats en fonction d'un renseignement particulier. Il est possible, par exemple, de sélectionner un certain type d'analyse, les analyses effectuées par un fournisseur de soins de santé qui donne une prescription ou un traitement au patient ou qui le prend en charge, ou encore les analyses traitées dans un centre de prélèvement ou un laboratoire en particulier. Vous devez au moins indiquer la période visée pour la recherche.

3. Le SILO cherchera alors tous les résultats d'analyse en laboratoire qui correspondent aux critères sélectionnés.
4. Il est possible de classer les résultats (p. ex., par type d'analyse ou par date).

Considérations sur la sécurité et la protection de la vie privée

Vos obligations en matière de confidentialité

À titre de dépositaires de renseignements sur la santé, les fournisseurs de soins de santé sont tenus de respecter les obligations qui leur incombent en vertu de la *LPRPS* et du Règlement de l'Ontario 329/04 (le « Règlement »).

Santé Ontario, en tant qu'organisme du ministère de la Santé et des Soins de longue durée (MSSLD) – un DRS –, est autorisé, en vertu de la *LPRPS* et de l'article 6.2 du Règl. de l'Ont. 329/04, à exploiter et à administrer le SILO, puisque Santé Ontario reçoit des RPS du MSSLD dans le but de créer et de gérer un ou plusieurs DSE.

En vertu de la *LPRPS*, les fournisseurs de soins de santé ne sont autorisés à recueillir des données du SILO que pour prodiguer ou aider à ce que soient prodigués des soins de santé à leur patient. Une fois que les résultats d'analyse du SILO ont été copiés dans le dossier du fournisseur, peu importe le format (papier ou électronique), ils peuvent être utilisés à n'importe quelle fin autorisée par la *LPRPS* ou toute autre loi applicable.

Chaque fournisseur de soins de santé doit s'assurer de recueillir, utiliser, conserver ou divulguer les données du SILO conformément aux obligations énoncées dans :

- toutes les ententes conclues entre Santé Ontario et lui-même ou l'établissement où il travaille (en tant qu'employé, partenaire, mandataire ou sous-traitant);
- toutes les ententes conclues par lui-même ou l'établissement où il travaille;
- la *LPRPS* et le Règlement de l'Ontario 329/04 (le Règlement);
- toute autre loi ou tout autre règlement applicable;
- tout jugement ou toute décision ou ordonnance rendus par un tribunal, administratif ou autre.

Les fournisseurs de soins de santé doivent s'assurer que leurs employés, leurs mandataires et leurs fournisseurs de services qui gèrent des renseignements personnels sur la santé en leur nom remplissent leurs obligations, décrites plus haut, et qu'ils connaissent et respectent toutes les obligations de la *LPRPS* et du Règlement les concernant.

On trouve une description plus détaillée des responsabilités des fournisseurs en matière de confidentialité dans la *LPRPS* et le Règlement.

Vos obligations en matière de sécurité

Les fournisseurs de soins de santé qui consultent les données du DSE sont tenus de respecter les obligations énoncées dans l'entente d'accès applicable conclue entre Santé Ontario et eux-mêmes ou leur établissement et les exigences décrites dans la section Responsabilités en lien avec la sécurité lors de la consultation des DSE, au minimum.

Directives en matière de consentement

Une restriction d'accès relative au patient ou à l'analyse implique que seuls sont autorisés à consulter les dossiers :

- les fournisseurs de soins de santé qui figurent sur la demande d'analyse de laboratoire (p. ex., le fournisseur qui prescrit l'analyse ou qui est mis en copie conforme);
- le laboratoire qui produit le rapport, le laboratoire où a été effectuée l'analyse et l'établissement qui a fait la demande d'analyse.

Dans les cas où un fournisseur de soins de santé obtient le consentement exprès d'un patient ou de son MS pour déroger à une directive en matière de consentement, le MSSLD, en tant que dépositaire du SILO, exige que le fournisseur inscrive une note dans le dossier du patient et qu'il explique au patient que, même si la dérogation est temporaire en ce qui concerne le SILO, les renseignements que le fournisseur a pu consulter seront conservés dans le système et marqués comme étant sensibles, et qu'ils pourraient être accessibles à d'autres fournisseurs qui participent à ses soins.

De plus, si le MS a donné son autorisation pour une dérogation à une directive en matière de consentement, le MSSLD, en tant que dépositaire du SILO, exige du fournisseur qu'il inscrive au dossier du patient le nom du MS ainsi que sa relation avec le patient. Advenant le cas où l'application ou le visualiseur sur l'ordinateur n'aurait pas la fonction requise (soit un système d'enregistrement électronique), le fournisseur doit inscrire manuellement ces renseignements. Santé Ontario doit pouvoir les consulter sur demande.

Annexe C : Service commun d'imagerie diagnostique (SC ID)

Présentation

Le Service commun d'imagerie diagnostique (SC ID) est une initiative de Santé Ontario qui vise l'amélioration de la prestation des soins aux Ontariens en s'appuyant sur la réussite des répertoires régionaux de résultats d'imagerie diagnostique. Ces répertoires donnent aux fournisseurs de soins de santé l'autorisation d'accéder à l'imagerie diagnostique (ID) et aux rapports connexes des hôpitaux et des établissements de santé autonomes dans leur région. Le Service commun d'imagerie diagnostique offre un accès global aux renseignements sur la santé provenant des répertoires régionaux d'ID afin que ses utilisateurs puissent consulter les rapports et les images de partout dans la province. Il offre un accès complet et sécuritaire aux enregistrements longitudinaux de l'imagerie numérique concernant un patient, et ce, n'importe où, n'importe quand. Les responsables de la mise en œuvre suivent des normes communes de service en matière d'imagerie numérique pour soutenir le partage des rapports d'imagerie numérique et des images.

Avantages

Avantages pour vous

- Accès à l'imagerie diagnostique et aux rapports de partout en Ontario.
- Accès plus rapide et plus facile aux images et aux rapports en tout temps.
- Collaboration interprofessionnelle en temps réel, facilitant l'accès à un plus vaste éventail de spécialistes.
- Élimination de la nécessité de transférer les images en format papier ou sur disque compact.

Avantages pour vos patients

- Élimination des déplacements inutiles.
- Réduction du temps d'attente et de la durée de séjour grâce à l'accélération de la production de rapports d'examen et de la prise de décisions cliniques de la part des médecins et des spécialistes.
- Moins d'examens inutiles ou en double.

Annexe D : Répertoire numérique des médicaments (RNM)

Présentation

Le Répertoire numérique des médicaments (RNM) est le premier pilier de la Stratégie des profils pharmaceutiques complets (SPPC) du ministère de la Santé et des Soins de longue durée, laquelle vise à améliorer la santé et le bien-être des Ontariens ainsi que la qualité des soins qu'ils reçoivent en mettant à la disposition des fournisseurs de soins de santé des données leur permettant d'offrir à leurs patients le meilleur schéma thérapeutique possible (MSTP).

Pour de plus amples renseignements sur les dispositions du Ministère quant à l'accès aux données sur les médicaments financés par l'État, les services en pharmacie et les médicaments contrôlés (indépendamment du payeur), consulter le www.ontario.ca/mesinfosmedicaments.

Contenu du RNM

Les fournisseurs de soins de santé qui dispensent des soins ou qui aident à le faire peuvent accéder aux renseignements suivants d'une personne concernant :

- les médicaments financés par l'État, distribués en Ontario et couverts par le Programme de médicaments de l'Ontario (PMO) ou tout autre programme public de médicaments (p. ex., le Programme de médicaments spéciaux), y compris les médicaments contrôlés pris en charge par ces programmes;
- les médicaments distribués aux ménages ontariens admissibles au Programme de médicaments Trillium;

- les médicaments contrôlés (stupéfiants et substances contrôlées) délivrés en Ontario et couverts par les assurances privées ou payés comptant;
- les services offerts par un pharmacien en Ontario et couverts par le Ministère, notamment :
    - l'examen des médicaments dans le cadre du programme MedsCheck;
    - l'administration des vaccins par les pharmaciens;
    - le dépistage du cancer du côlon à l'aide de la trousse de recherche de sang occulte dans les selles (RSOS) du programme ContrôleCancerColorectal;
    - le Programme d'abandon du tabagisme offert en pharmacie;
    - les trousses de naloxone pour la réduction des méfaits dans le cadre du Programme ontarien de distribution de naloxone en pharmacie;
    - les médicaments distribués pour l'aide médicale à mourir.

En ce qui a trait aux médicaments, les fournisseurs de soins de santé peuvent voir leur date de délivrance, leur nom, la forme galénique, le dosage, la quantité délivrée et l'estimation de la durée du traitement, ainsi que le nom du médecin prescripteur et des renseignements sur la pharmacie. Ils verront également une description des services reçus en pharmacie (et leur date) ainsi que des renseignements sur la pharmacie en question. Dans certains cas, des renseignements sur le prescripteur figureront dans le RNM, par exemple le nom du pharmacien ayant offert le service. La quantité et l'estimation de la durée du traitement sont de 1 par défaut.

Limites du RNM

Le RNM ne contient que :

- les renseignements que le Ministère peut divulguer selon la *LPRPS* et la *Loi de 2010 sur la sécurité et la sensibilisation en matière de stupéfiants*;
- les renseignements consignés dans le système d'évaluation des demandes des programmes publics de médicaments de l'Ontario ou dans le Système de surveillance des stupéfiants et des substances contrôlées jusqu'à présent, concernant les médicaments et les services de pharmacie.

Ces renseignements sont fournis au Ministère par les pharmacies, et il se peut qu'un dossier ne contienne pas la liste exhaustive des médicaments d'un patient pour une période donnée, ou n'indique pas tous les services reçus.

Pour figurer dans le dossier, le médicament doit avoir été inscrit au dossier pharmacologique du patient, lequel doit avoir été transmis au Ministère par la pharmacie. Le fait que le médicament figure dans ce dossier ne signifie pas nécessairement que le patient est allé le chercher et qu'il suit la posologie.

Les fournisseurs de soins de santé n'ont pas accès aux renseignements sur les médicaments qui ne sont pas consignés dans le RNM, soit les médicaments non contrôlés, payés directement par les patients ou les sociétés d'assurances privées, les médicaments sans ordonnance et les produits à base d'herbes médicinales.

Si un patient bloque l'accès à ses renseignements figurant dans le RNM, les fournisseurs de soins ne pourront les consulter qu'avec son consentement exprès ou celui de son mandataire spécial. Les fournisseurs doivent discuter avec leur patient de l'information figurant dans le RNM pour s'assurer que la liste de médicaments est complète et élaborer le meilleur schéma thérapeutique possible.

Les données inscrites dans le RNM sont fournies à titre indicatif et ne visent pas à se substituer au jugement clinique lors de la prestation de services de soins de santé.

Présentation du RNM aux patients

Le MSSLD donne accès aux renseignements sur les médicaments et les services en pharmacie des patients à leurs fournisseurs de soins, par l'intermédiaire du RNM, pour assurer la prestation de soins de santé d'excellente qualité. Il demeure important que les fournisseurs de soins continuent de discuter avec leurs patients pour valider la liste complète de leurs médicaments, et pour les aider à comprendre comment cette information peut servir à élaborer le meilleur schéma thérapeutique possible, et à d'autres fins cliniques.

Vos patients peuvent être mal à l'aise avec l'idée de voir ces renseignements ainsi divulgués, et doivent savoir qu'ils peuvent bloquer l'accès à leurs renseignements. Cependant, nous les encourageons à consulter leurs fournisseurs de soins de santé pour connaître les conséquences qu'une telle action peut avoir sur les soins qu'ils recevront. Vous pouvez expliquer à vos patients qu'il est important pour vous d'avoir accès aux renseignements sur leurs médicaments et les services en pharmacie qu'ils reçoivent, puisque ces données vous aident à prendre des décisions éclairées. Vous pouvez également les rassurer en leur disant que leur fournisseur de soins de santé est tenu par la loi de respecter la confidentialité de leurs renseignements personnels sur la santé.

Il est fort probable que vos patients ne connaissent pas la technologie vous permettant d'accéder à ces renseignements. Bien qu'ils puissent comprendre ce que sont les « dossiers de santé électroniques » en général, la plupart d'entre eux ne sauront pas à quoi vous faites référence lorsque vous parlez du RNM. Par conséquent, le MSSLD recommande de parler de « l'accès des fournisseurs de santé aux renseignements sur les médicaments et les services en pharmacie » plutôt que du système de RNM.

Avantages

Avantages pour vous

- Accès aux données sur les médicaments et les services en pharmacie, pertinentes sur le plan clinique et qui permettent de proposer le meilleur schéma thérapeutique possible (MSTP).
- Intégration améliorée des données pharmaceutiques disponibles grâce aux actifs numériques de santé provinciaux, comme les dossiers médicaux électroniques (DME) et les systèmes d'information hospitaliers, ce qui permet un accès rapide, sécuritaire et efficace aux données dans le but de proposer le meilleur schéma thérapeutique possible.

- Renforcement de la sécurité des patients et de la continuité des soins.
- Amélioration de la collaboration entre les fournisseurs de soins de santé grâce à l'échange de données cliniques sur les patients.

Avantages pour vos patients

- Amélioration de l'expérience des patients ayant recours au système de soins de santé grâce à une prise de décisions éclairée des fournisseurs de soins de santé.
- Amélioration des soins axés sur le patient puisque les fournisseurs de soins de santé bénéficieront d'un accès électronique sécuritaire aux renseignements sur les médicaments et les services en pharmacie de leurs patients et auront plus de temps pour poser un diagnostic, prodiguer un traitement et communiquer avec leurs patients.
- Meilleurs résultats pour les patients et diminution du risque d'effets indésirables.

Considérations sur la sécurité et la protection de la vie privée

Consentement du patient

Le fournisseur de soins de santé doit imprimer et remplir le formulaire intitulé *Débloquer ponctuellement l'accès à vos renseignements personnels sur les médicaments et les services de pharmacie reçus* figurant dans le visualiseur clinique. Si c'est le mandataire spécial du patient qui donne son consentement, le type de relation qui le lie au patient doit être indiqué dans le formulaire. Le fournisseur doit obtenir l'autorisation du patient ou de son mandataire spécial ainsi que sa signature manuscrite sur le formulaire et conserver ce dernier en lieu sûr dans ses dossiers aux fins de vérification.

Annexe E : Les registres provinciaux

Présentation

Les registres provinciaux (le Registre provincial des clients et le Registre provincial des fournisseurs) constituent la base du dossier de santé électronique (DSE). Ils sont une « source fiable » en ce qui concerne les renseignements sur le patient et sur les fournisseurs de soins membres d'un ordre.

Registre provincial des clients (RPC)

Le Registre provincial des clients (RPC) est la ressource qui fait autorité en matière de données démographiques sur les patients ou les clients ou d'identifiants en appui au dossier de santé électronique (DSE) en Ontario. Il fournit une identité pour le patient à l'échelle de la province ainsi qu'un service de résolution pour que les fournisseurs de soins de santé puissent chercher et inscrire un patient et avoir accès à son dossier de santé électronique en regroupant les dossiers de plusieurs lieux de soins.

Le RPC rassemble les données sur l'identité des patients en temps réel depuis la Base de données sur les personnes inscrites (BDPI) du ministère de la Santé et des Soins de longue durée, les hôpitaux et les établissements de soins de santé participants, qui fournissent des données démographiques à jour sur les patients ainsi qu'une liste exhaustive des identifiants des patients.

Registre provincial des fournisseurs (RPF)

Le registre provincial des fournisseurs (RPF) est la ressource qui fait autorité en matière de renseignements sur les fournisseurs de soins de santé et les établissements qui utilisent le DSE en Ontario. Il aide les fournisseurs de soins de santé dans leur flux de travail d'aiguillage en ligne et à tenir à jour leur répertoire des fournisseurs locaux.

Le registre provincial des fournisseurs rassemble les données d'identification des fournisseurs depuis la Base de données centrale sur les fournisseurs de services de santé du ministère de la Santé et des Soins de longue durée et des ordres de réglementation (en vertu de la *Loi de 1991 sur les professions de la santé réglementées*) afin d'offrir un profil complet des fournisseurs de soins. Il permet de recenser les fournisseurs membres d'un ordre et les établissements qui fournissent des soins de santé en Ontario, et comprend des renseignements comme le statut des titulaires de permis, les spécialités et le lieu de pratique.

Avantages

Avantages pour vous

- Partage plus facile des renseignements cliniques par la mise en place d'une identité commune à tous les points de service pour le patient.
- Amélioration de la qualité des données et de l'efficacité du flux de travail clinique.
- Identification formelle des fournisseurs membres d'un ordre.
- Accès à l'information sur les fournisseurs (statut de titulaire de permis, lieu de pratique).

Avantages pour vos patients

- Amélioration de la sécurité pour les patients (liée aux erreurs d'identification).
- Création d'un DSE longitudinal intégré.

- Réduction des efforts manuels liés à la gestion et à la recherche de renseignements sur les fournisseurs.
- Réduction du temps d'attente pour voir un fournisseur (aiguillage, consultation).

Annexe F : Moyens de consulter le DSE

Il y a de nombreuses façons d'accéder aux répertoires de données du DSE. La liste suivante, quoique non exhaustive, en présente quelques-unes. Elle sera alimentée au fur et à mesure que l'information sera disponible.

Visualiseur clinique de ConnexionOntario

Le visualiseur clinique de ConnexionOntario est un portail en ligne sécuritaire qui offre un accès en temps réel aux dossiers de santé électroniques, dans lesquels sont consignés :

- les visites à l'hôpital;
- les résultats des analyses effectuées en laboratoire;
- les médicaments délivrés;
- les images diagnostiques;
- l'information sur les soins à domicile et en milieu communautaire.

À l'aide des technologies de l'information, le visualiseur clinique permet :

- de recenser et de recueillir les données prioritaires : le RDC contient les données de bases et de registres existants;
- d'offrir la possibilité d'échanger des renseignements : les couches d'accès à l'information sur la santé (CAIS) permettent de réunir et de partager en toute sécurité l'information clinique provenant de différentes sources;
- d'avoir accès à l'information : des options d'accès, comme un portail destiné aux fournisseurs et l'intégration directe, permettent aux cliniciens de consulter facilement les renseignements sur les patients en ligne.

Le visualiseur clinique de ConnexionOntario est utilisé par des cliniciens et des fournisseurs de soins de plus de 859 établissements de soins de santé des secteurs suivants :

- Soins actifs
- Services de soutien communautaire
- Soins continus complexes
- Soins de longue durée

- Problèmes de santé mentale et dépendances
- Soins primaires
- Réadaptation
- Pharmacie

ClinicalConnect

ClinicalConnect est un portail en ligne sécurisé qui permet aux fournisseurs de soins de santé d'avoir accès en temps réel aux renseignements médicaux électroniques en provenance des hôpitaux de soins actifs, des réseaux locaux d'intégration des services de santé (RLISS), des services de soins à domicile et en milieu communautaire et des Programmes régionaux de cancérologie dans le Sud-Ouest de l'Ontario, en plus de différents répertoires de données cliniques provinciaux.

Il permet un accès rapide et sécuritaire à des renseignements complets sur les soins de santé du patient, notamment :

1. les visites à l'hôpital;
2. les résultats des analyses effectuées en laboratoire;
3. les médicaments délivrés;
4. les images diagnostiques;
5. les transcriptions de rapports;
6. l'information sur les soins à domicile et en milieu communautaire.

Voici les principaux modules et fonctions de ClinicalConnect :

- Listes de patients (personnalisables)
- Indicateur pour les résultats récents ou anormaux
- Visites des patients (antérieures et futures)
- Transcriptions (congés, salle d'opération, notes de consultation ou d'évolution)
- Rapports de laboratoire (comprend les tendances et des graphiques)
- Rapports de services diagnostiques et radiographies provenant d'hôpitaux
- Ordonnances de certains patients hospitalisés pour les commandes de médicaments et de narcotiques couverts par le PMO à la pharmacie de l'hôpital

- Allergies
- Renseignements sur la santé (caractéristiques démographiques des patients, coordonnées personnelles ou du personnel médical à leurs soins, liste des services, liste de placement, choix ou réservations concernant les foyers de soins de longue durée, ressources de soutien communautaire, diagnostiques, groupes de soins primaires, risques, problèmes liés à la sécurité, etc.)

ClinicalConnect peut être utilisé sur un ordinateur, une tablette ou un appareil mobile. Dans certains RLISS, les médecins ont l'option de télécharger les données de l'hôpital dans leur DME. De plus, les hôpitaux qui utilisent les systèmes fédérés de ONE ID peuvent profiter de l'authentification unique et accéder à ClinicalConnect à partir de leur système d'information hospitalier.

Intégration au dossier médical électronique (DME)

En partenariat avec Santé Ontario, OntarioMD – filiale de l'Association médicale de l'Ontario – maintient une spécification provinciale pour les systèmes de DME. On peut se connecter automatiquement au SILO à partir des produits de DME certifiés de niveau 4 ou plus et recevoir les résultats d'analyse en laboratoire dans le DME.

La recherche par patient permet aux utilisateurs de faire une recherche dans l'historique des analyses de laboratoire pour un patient en particulier, et ce, peu importe qui a ordonné l'analyse. Cela permet :

- de télécharger à l'avance un nouveau dossier pour le patient, qui comprend l'historique de ses résultats d'examens en laboratoire ordonnés par un autre fournisseur de soins;
- de vérifier les résultats antérieurs d'une analyse pour déterminer les tendances;
- de vérifier si un certain type d'analyse a déjà été effectué (pour éviter les doublons).

Rappels importants

- Des filtres de données du DME certifiés par OntarioMD doivent être en place pour que les données du SILO ne soient pas fusionnées avec celles d'un dossier de patient existant de la base de données du DME et qu'elles soient automatiquement marquées pour vérification et approbation dans une liste non assortie.
- Tous les rapports doivent être lus et approuvés par le praticien désigné avant d'être intégrés au dossier du patient dans le DME, et les rapports qui ne correspondent pas à un patient existant doivent être filtrés automatiquement.
- Les praticiens ne devraient avoir accès à l'information qu'au nom d'un DRS qui prodigue ou qui aide à prodiguer des soins de santé à leurs patients dans le contexte d'une requête du praticien dans SILO (requête Z04).

Considérations sur la sécurité et la protection de la vie privée

Il y a des cas particuliers (avec le consentement du patient ou de son mandataire spécial) où un fournisseur peut déroger, à partir du DME, à une directive en matière de consentement d'un patient qui restreint l'accès aux résultats d'une analyse.

Une telle dérogation est enregistrée dans le système de DME, ainsi que l'identité du fournisseur de soins qui la demande et le type de consentement obtenu. De plus, le SILO journalise tous les accès à ses données.

Dans les cas où le fournisseur de soins obtient le consentement exprès du patient pour déroger à la directive qui lui empêche l'accès, il est recommandé que le fournisseur explique au patient que, même si la dérogation est temporaire pour le SILO, l'information que le fournisseur a consultée sera sauvegardée dans le système de DME et marquée comme de l'information sensible, et qu'elle pourrait être accessible à d'autres fournisseurs qui prodiguent des soins au patient.

Départ

Advenant le cas où un fournisseur de soins de santé quitte ses fonctions, vous devez observer ce qui suit :

- Veiller à révoquer l'accès à un utilisateur qui a quitté ses fonctions ou qui n'a plus besoin d'accéder aux données du SILO et de désactiver toute requête automatique (sur un praticien ou un patient) dans le SILO à la première occasion raisonnable, au plus tard cinq jours ouvrables après que l'utilisateur a quitté ses fonctions ou qu'il n'a plus besoin de consulter le SILO;
- Effacez les données en attente d'approbation ou d'élimination dans la boîte de l'utilisateur dans les cinq jours ouvrables suivant le départ du praticien ou après qu'il n'a plus besoin d'accéder au système;
- Si l'établissement a délégué la gestion des comptes utilisateur à son fournisseur agréé de DME, l'établissement doit lui demander de procéder aux tâches ci-haut dans les délais prescrits;
- Retirer l'utilisateur du menu déroulant dans le DME pour qu'il ne puisse pas être sélectionné dans la liste UAO (sous l'autorité de).

Intégration à l'Electronic Child Health Network (eCHN)

Santé Ontario et l'eCHN collaborent afin de rendre l'information du SILO accessible aux utilisateurs autorisés de l'eCHN grâce à la WebChart (fiche médiale en ligne) de ce dernier.

Considérations sur la sécurité et la protection de la vie privée

L'application WebChart permet aux utilisateurs de déroger à une directive en matière de consentement qui concerne les données de l'eCHN quand : a) il y a une urgence ou un besoin clinique; ou b) l'accès a été accordé directement par le patient ou son MS (consentement exprès).

Toutefois, le MSSLD, en tant que dépositaire de renseignements sur la santé du SILO, ne permet pas aux utilisateurs autorisés du SILO de déroger à une directive en matière de consentement appliquée aux données du

SILO sans le consentement exprès du patient (ou de son MS). Les utilisateurs de l'eCHN ne doivent donc pas appliquer de dérogation sans obtenir le consentement exprès, même s'il s'agit d'une urgence clinique.

Par conséquent, l'eCHN a modifié l'interface de la WebChart pour permettre à ses utilisateurs de déroger à une directive du patient en matière de consentement pour les données du SILO, mais seulement avec le consentement exprès du patient ou de son MS, et s'il ne s'agit pas d'une urgence (techniquement, l'option de dérogation pour besoin clinique ou urgence de la WebChart pour les données du SILO a été désactivée dans l'eCHN). La dérogation à une directive du patient pour consulter les données du SILO sans son consentement exprès ou celui de son mandataire constitue une violation de l'entente de l'utilisateur (ou de son établissement) avec Santé Ontario, et entraînera l'application des mesures correctives prévues dans l'entente.

Si vous avez des questions sur la gestion du consentement pour les données du SILO, veuillez contacter le Bureau de la protection de la vie privée de Santé Ontario à l'adresse privacy@ehealthontario.on.ca. Précisez dans le courriel que vous êtes un utilisateur de l'eCHN.

Annexe G : Procédure de transfert de fichiers sensibles

En vertu des politiques de Santé Ontario, des mesures de protection appropriées doivent être prises chaque fois qu'un document ou un fichier contenant des données sensibles est stocké ou transféré au moyen de canaux de communication qui ne sont pas entièrement sûrs (courriel ordinaire, CD, DVD, clé USB, carte mémoire flash, etc.).

Vous devez utiliser ONE Mail lorsque vous devez transmettre des données sensibles à un utilisateur de ONE Mail. Pour les autres utilisateurs toutefois, il est recommandé d'utiliser WinZip ou un autre logiciel similaire.

La présente section explique la procédure à suivre pour appliquer un niveau de protection élevé aux fichiers et aux rapports contenant des données sensibles à l'aide de WinZip, une application offerte sur le marché qui permet de réduire la taille d'un document et de lui appliquer un niveau de protection élevé.

Il est important de garder à l'esprit que l'outil présenté dans ce document est un système de cryptage par mot de passe. Le fichier crypté peut être lu si la sécurité du mot de passe est compromise. Par conséquent, toute personne qui utilise cet outil pour crypter un fichier doit suivre les instructions sur la protection du mot de passe figurant à la section « Communiquer le mot de passe ».

Utilisations autorisées

Vous pouvez suivre cette procédure pour envoyer ponctuellement des données sensibles, notamment des documents contenant des renseignements personnels, sur la santé ou autres, par courriel, conformément à vos processus administratifs habituels.

Si l'envoi de renseignements sensibles par courriel non sécurisé fait partie de vos processus administratifs courants, il est recommandé de songer à automatiser ce processus et à utiliser un mécanisme d'entreprise pour transférer vos données de façon sécuritaire.

Santé Ontario limite la taille des pièces jointes à 10 Mo par courriel.

Pour obtenir de l'aide ou des renseignements qui ne figurent pas dans ce document, veuillez appeler le Service de dépannage de Santé Ontario au 1 866 250-1554.

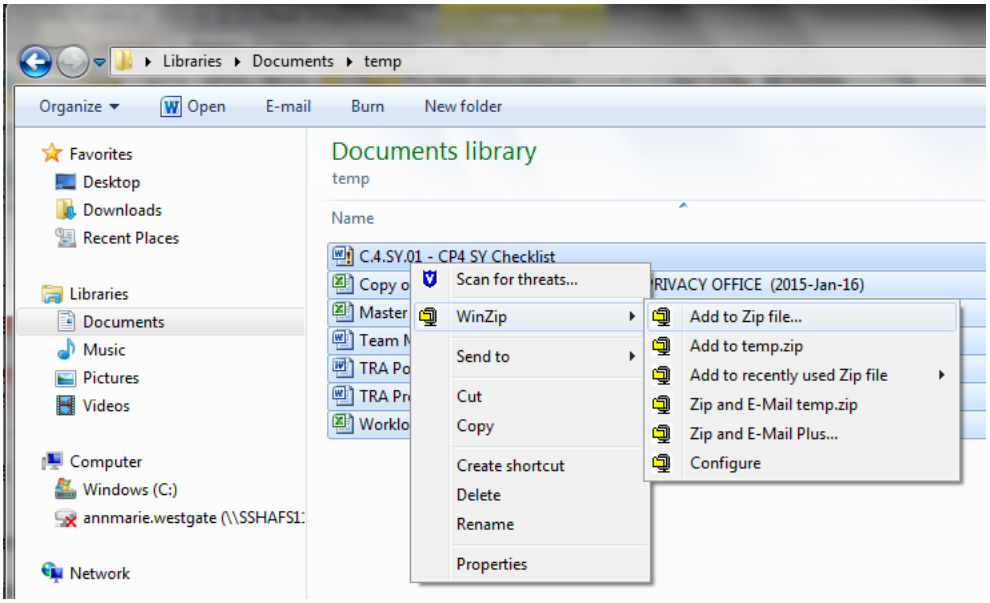
Utiliser le logiciel de cryptage WinZip

Santé Ontario suggère d'utiliser l'outil de cryptage WinZip.

Crypter des fichiers avec WinZip

Étape 1 : Créer une archive

- Ouvrez l'emplacement du fichier.
- Ouvrez le dossier où se trouvent les fichiers. Sélectionnez les fichiers que vous souhaitez compresser. Dans la boîte de dialogue, placez le curseur de la souris sur WinZip et cliquez sur « Ajouter au Zip… ».
- Donnez au fichier le nom de votre choix.

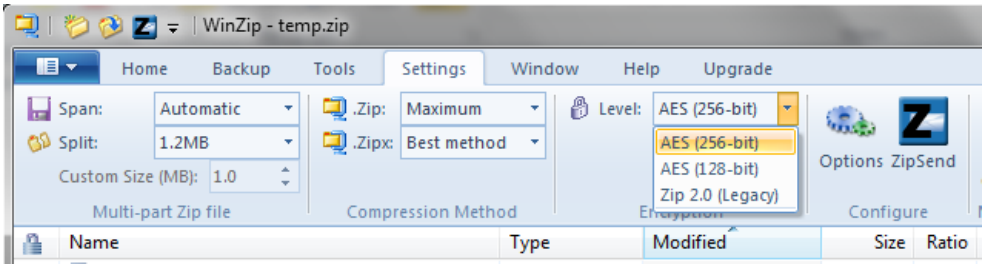


Étape 2 : Ouvrir l'archive

- Double-cliquez sur le fichier Zip pour ouvrir l'archive.

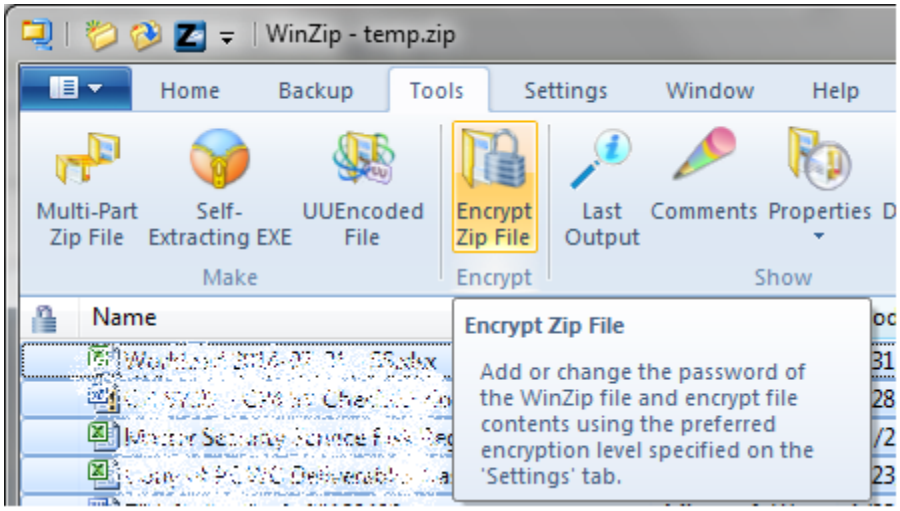
Étape 3 : Choisir un niveau de cryptage élevé

- Utilisez le cryptage AES 256 bits.
- Dans l'onglet « Réglages », assurez-vous que le niveau de cryptage sélectionné est AES (256 bits).



Étape 4 : Crypter le fichier

- Dans le menu « Outils », cliquez sur « Crypter le fichier Zip ».



Étape 5 : Créer un mot de passe fort

- Entrez un mot de passe puis confirmez-le.
- Pour savoir comment créer un mot de passe fort, reportez-vous à la section « Créer un mot de passe » ci-après.

Le fichier doit être crypté et protégé par un mot de passe avant d'être envoyé par courriel sous forme de pièce jointe.

Le logiciel WinZip décrit dans le présent document est un outil de cryptographie symétrique qui nécessite la communication d'un secret (un mot de passe en l'occurrence). En d'autres termes, l'expéditeur du fichier crypté doit communiquer le mot de passe au destinataire prévu du fichier. En cas d'oubli du mot de passe, il sera impossible de récupérer les fichiers se trouvant dans l'archive cryptée. Le processus de création et de communication du mot de passe nécessite donc une attention particulière.

Autres méthodes

Si WinZip n'est pas installé sur votre ordinateur, demandez de l'aide à votre service de dépannage, ou utilisez Microsoft Word ou Excel pour crypter vos fichiers. Voici comment faire :

- Ouvrez le document.
- Cliquez sur l'onglet « Fichier », puis sur « Informations ».
- Cliquez sur « Protéger le document ».
- Dans le menu déroulant, cliquez sur « Chiffrer avec mot de passe ».
- Choissez un mot de passe et confirmez votre choix en cliquant sur « OK ».

Transférer un fichier et communiquer le mot de passe

Une fois le fichier crypté et protégé par un mot de passe, il est temporairement sauvegardé dans le dossier partagé sur le réseau ou dans le lecteur de disque dur local partagé. Il peut alors être joint à un courriel et envoyé au service de dépannage. N'ENVOYEZ PAS de capture d'écran contenant des renseignements personnels, sur la santé ou autre, directement dans le courriel. Vous devez d'abord les crypter et les protéger par mot de passe.

Le mot de passe doit être communiqué au destinataire du fichier par téléphone ou à l'aide d'une méthode « hors bande » (p. ex., si le document est envoyé par courriel, transmettre le mot de passe par téléphone, par télécopieur ou par la poste). En d'autres termes, le mot de passe ne doit pas être envoyé en même temps que le fichier crypté à l'aide de la même méthode.

Créer un mot de passe

- Créer un mot de passe fort pour protéger les fichiers cryptés.
- Créer et utiliser un mot de passe différent pour chaque archive WinZip.
- Utiliser au moins huit caractères.

- Les mots de passe doivent comprendre au moins trois des quatre types de caractères suivants : lettre majuscule (de A à Z); lettre minuscule (de a à z); chiffre (de 0 à 9) et caractère spécial (p. ex., !, $, #, _, ~, % ou ^).
- Exemple d'un mot de passe faible : 1234motdepasse!.
- Exemple d'un mot de passe difficile à deviner : C_35t_Un3_B3ll3_J0urné3.

Une fois qu'il a créé le mot de passe, l'expéditeur envoie le fichier au demandeur par courriel. Il doit s'assurer d'envoyer le courriel au bon destinataire. Lorsque le demandeur reçoit le courriel, il appelle l'expéditeur pour obtenir le mot de passe.

Communiquer le mot de passe

Les DRS doivent communiquer les mots de passe à Santé Ontario de façon sécuritaire. Voici la procédure à suivre :

- Déterminer qui est le destinataire autorisé de l'information.
- Mettre le fichier crypté à la disposition du destinataire selon le processus convenu (p. ex., SFTP, courriel).
- Le demandeur appelle l'expéditeur par téléphone.
- L'expéditeur vérifie oralement l'identité du destinataire :
    - Nom;
    - Titre, division, organisation;
    - Nom du fichier crypté reçu ou récupéré.
- L'expéditeur fournit oralement au destinataire le mot de passe permettant d'ouvrir le fichier crypté.
- Il demande et obtient la confirmation orale que le destinataire a pu extraire les fichiers s'y trouvant.
- Le cas échéant, l'expéditeur détruit de façon sécuritaire la copie écrite du mot de passe ainsi que toute copie du fichier se trouvant sur le réseau ou le disque local.

Récupérer le mot de passe

WinZip ne prévoit aucun mécanisme de récupération du mot de passe. Par conséquent, en cas de stockage à long terme de fichiers cryptés, une méthode de récupération du mot de passe doit être mise en place pour accéder aux fichiers (p. ex., au cas où des fichiers d'un employé ayant quitté l'organisation devraient être consultés).

Par exemple, le mot de passe peut être conservé aux fins de récupération dans une enveloppe scellée accessible uniquement par la haute direction.

Supprimer un fichier

Une fois le fichier décrypté et utilisé, il doit être supprimé par son expéditeur et son destinataire.

Annexe H : Sigles

Sigle	Signification
BDPI	Base de données sur les personnes inscrites
CAIS	couche d'accès à l'information sur la santé
d-ID	dépôt d'imagerie diagnostique
DME	dossier médical électronique
DRS	dépositaire de renseignements sur la santé
DSE	dossier de santé électronique
eCHN	Electronic Child Health Network
ID	imagerie diagnostique
LPRPS	*Loi de 2004 sur la protection des renseignements personnels sur la santé*
MS	mandataire spécial
MSSLD	ministère de la Santé et des Soins de longue durée
MSTP	meilleur schéma thérapeutique possible
PMO	Programme de médicaments de l'Ontario
RDC	Répertoire des données cliniques
RNM	Répertoire numérique des médicaments
RPC	Registre provincial des clients
RPF	Registre provincial des fournisseurs
RPOP	Répertoire principal ontarien des patients

Sigle	Signification
RPS	renseignements personnels sur la santé
RSOS	recherche de sang occulte dans les selles
SC ID	Service commun d'imagerie diagnostique
SILO	Système d'information de laboratoire de l'Ontario
SPPC	Stratégie des profils pharmaceutiques complets

Avis de droit d'auteur

Tous droits réservés

Marques de commerce