cyberSanté Ontario
Travaille pour vous

Guide du fournisseur de soins de santé

Répertoire des données cliniques (RDC)

Ontario
cyber Santé Ontario

Version : 2.2

1 Table des matières

2 Généralités

2.1 Objet et portée

Le présent guide décrit les fonctions du Répertoire des données cliniques (RDC) et les avantages qu'il procure, ainsi que les règles de sécurité et de protection de la vie privée auxquelles les fournisseurs et les établissements de soins de santé utilisant le RDC doivent se conformer.

2.2 Destinataires

Le présent document s'adresse aux fournisseurs de soins de santé ontariens, qu'il s'agisse de personnes ou d'organismes, qui ont conclu ou concluront une ou des ententes d'accès appropriées avec cyberSanté Ontario pour accéder aux données cliniques concernant leurs patients à l'aide du RDC.

2.3 Documents connexes

Le présent guide doit être lu parallèlement aux documents suivants, qui se trouvent sur le site cyberSanteOntario.on.ca :

- Politique sur la protection des renseignements personnels sur la santé de cyberSanté Ontario
- Politique sur l'accès aux renseignements et la rectification des renseignements – Dossier de santé électronique
- Politique de vérification de la conformité – Dossier de santé électronique
- Politique de gestion du consentement – Dossier de santé électronique
- Politique sur les demandes de renseignements et les plaintes – Dossier de santé électronique
- Politique sur la journalisation et la surveillance – Dossier de santé électronique
- Politique sur la formation en protection de la confidentialité et de la sécurité – Dossier de santé électronique
- Politique de gestion des atteintes à la confidentialité – Dossier de santé électronique
- Politique de conservation – Dossier de santé électronique
- Politique et norme de cyberSanté Ontario relatives aux fournisseurs de services d'authentification
- Politiques de sécurité relatives au dossier de santé électronique (DSE)
    - Politique d'utilisation acceptable des données et des technologies de l'information
    - Politique sur le contrôle de l'accès aux systèmes et les processus de gestion d'identité connexes
    - Politique sur la continuité des activités
    - Politique sur la cryptographie
    - Politique sur les fournisseurs de services électroniques
    - Norme sur les fournisseurs d'identités de la fédération d'identité de cyberSanté Ontario
    - Politique sur la gestion des incidents de sécurité de l'information
    - Politique sur la gestion de l'information et des éléments d'actif
    - Politique de sécurité de l'information
    - Politique sur les pratiques de l'autorité locale d'enregistrement
    - Politique sur la journalisation de sécurité et la surveillance
    - Politique sur les réseaux et les opérations
    - Politique sur la sécurité matérielle
    - Politique sur le cycle de développement de systèmes
    - Politique sur la gestion des menaces et des risques

3 Description du service

3.1 Tour d'horizon

Le RDC est un répertoire de données de cyberSanté Ontario dans lequel les fournisseurs de soins de santé autorisés peuvent consulter des données cliniques provenant d'établissements offrant des soins actifs et primaires qui consignent des renseignements dans le répertoire. Les données peuvent comprendre des rapports cliniques (p. ex., rapports de centres d'accès aux soins communautaires [CASC], sommaires de congé, et rapports des services des urgences, les visites et les rencontres), ainsi que des données de dossiers médicaux électroniques (DME). Grâce au RDC, les fournisseurs autorisés ont accès à des renseignements importants qui leur permettent de prendre des décisions éclairées sur le traitement de leurs patients. À l'aide des technologies de l'information, le RDC recense, recueille et conserve des données prioritaires provenant de bases et registres existants (p. ex., systèmes d'information hospitaliers et DME).

3.2 Avantages

3.2.1 Avantages pour vous

1. Amélioration de la qualité des soins et de l'expérience.
   - Réduction des chevauchements et de la frustration.
   - Amélioration de la rapidité de l'accès à l'information sur les patients.
   - Amélioration de la transition entre les fournisseurs de soins de santé.
   - Dossiers plus détaillés sur les patients, et amélioration des données qu'ils contiennent.
2. 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.
3. 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 d'amélioration de la gestion, de la coordination et de 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.

3.2.2 Avantages pour vos patients

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

3.3 Responsabilités

3.3.1 Responsabilités des fournisseurs de services d'authentification

Les établissements de soins de santé sont tenus de :

- se conformer aux exigences de la politique et de la norme de cyberSanté Ontario relatives aux fournisseurs de services d'authentification;
- se conformer aux politiques sur la sécurité du DSE lorsqu'ils offrent des services d'authentification. La liste complète des politiques se trouve à la section Documents connexes.

3.3.2 Responsabilités des personnes qui consultent les données du RDC

Les fournisseurs de soins de santé qui consultent les données du RDC sont tenus de respecter les obligations énoncées dans l'Annexe sur les services d'accès aux DSE ou l'Accord sur l'utilisation des services de DSE par un cabinet médical de cyberSanté Ontario les visant, ou visant leur organisation, et doivent :

- accepter de se conformer aux politiques de sécurité visant les DSE, accessibles à l'adresse http://www.ehealthontario.on.ca/fr/support/;
- prendre connaissance des documents de référence énumérés à la section Documents connexes, et apprendre à assurer la protection de la vie privée et à garantir la sécurité dans le cadre de l'utilisation des produits de cyberSanté Ontario;
- utiliser le RDCuniquement à des fins cliniques autorisées;
- toujours indiquer le nom de la personne ou de l'organisation pour le compte de laquelle l'utilisateur emploie le RDC pour consulter les renseignements sur la santé des patients;
- obtenir le consentement du patient ou du mandataire spécial avant de demander le rétablissement temporaire de l'accès aux renseignements sur la santé qui a été restreint en vertu de directives en matière de consentement;
- instaurer des politiques sur la sécurité et la protection de la vie privée dans le cadre de l'utilisation du DSE, et aider les utilisateurs à s'y conformer, s'il y a lieu.

4 Considérations sur la sécurité et la protection de la vie privée

Aide-mémoire
Le RDC permet aux patients ou à leur mandataire spécial de restreindre ou rétablir l'accès aux données les concernant dans le système. Les restrictions sont appelées des « directives en matière de consentement ». Les patients qui souhaitent donner une directive en matière de consentement dans le RDC doivent remplir le formulaire de consentement relatif à un DSE accessible à l'adresse http://www.ehealthontario.on.ca/fr/support/, puis l'envoyer à cyberSanté Ontario. Les fournisseurs peuvent aider les patients à remplir le formulaire, puis l'envoyer à cyberSanté Ontario pour eux.

4.1 Consentement du patient

4.1.1 Gestion du consentement

Le RDC donne aux patients ou à leur mandataire spécial la possibilité de restreindre l'accès aux données les concernant qui y sont conservées. Si un patient restreint l'accès à ses données, les fournisseurs de soins de santé qui feront une recherche à l'aide de la solution ne seront pas en mesure de consulter les renseignements d'un patient faisant l'objet d'une directive en matière de consentement du patient ou de son mandataire spécial.

Le RDC permet de créer, de modifier ou de supprimer les directives en matière de consentement pour restreindre l'accès aux types de renseignements suivants sur les patients :

- **Renseignements généraux :** Les fournisseurs de soins de santé n'auraient pas accès aux renseignements personnels sur la santé du patient dans le RDC, sauf les données démographiques qui figurent dans les registres des clients et des consentements.
- **Domaine :** Bloquer l'accès de tous les fournisseurs aux dossiers des patients dans le domaine RDC.
- **Mandataires – DRS :** Des fournisseurs de soins de santé particuliers (p. ex., le Dr Tremblay) d'un DRS précis (p. ex., l'hôpital A) n'auraient pas accès aux renseignements personnels sur la santé d'un patient dans le RDC.
- **Mandataire :** Des fournisseurs de soins de santé particuliers (p. ex., le Dr Tremblay) n'auraient pas accès aux renseignements personnels sur la santé d'un patient dans le RDC.

4.1.2 Application des directives en matière de consentement

Si un patient communique avec un DRS pour faire restreindre ou rétablir l'accès à ses renseignements personnels, le DRS doit :

1. inscrire l'information sur la directive en matière de consentement dans le formulaire de consentement relatif à un dossier de santé électronique (accessible sur le site http://www.ehealthontario.on.ca/fr/support);
2. transmettre ce formulaire à cyberSanté Ontario par télécopieur au 416 586-4397 ou au 1 866 831-0107.

cyberSanté Ontario confirmera au DRS qu'on a donné suite à la demande. Le DRS devra alors aviser le patient que la directive en matière de consentement a été appliquée.

Si un patient demande de faire appliquer une directive en matière de consentement ou de rétablir l'accès à des dossiers auxquels ont contribué plus d'un DRS, il doit remplir le formulaire de consentement relatif à un dossier de santé électronique à l'adresse http://www.ehealthontario.on.ca/fr/support, ou communiquer directement avec cyberSanté Ontario au 416 946-4767.

Dans tous les cas, cyberSanté Ontario appliquera la directive en matière de consentement dans les sept jours suivant la vérification de l'identité du patient qui en a fait la demande. Le fournisseur de soins de santé ou l'organisation qui reçoit la demande concernant la directive en matière de consentement envoyée par le patient avise alors ce dernier qu'on a donné suite à sa demande. Si vous ne pouvez pas l'aviser, le DRS informera cyberSanté Ontario afin qu'il s'en charge pour vous.

Veuillez noter que les demandes concernant une directive envoyées à cyberSanté Ontario au nom de votre patient doivent être déposées par la personne de votre organisation désignée comme responsable de la protection de la vie privée; il peut s'agir du directeur de la protection de la vie privée ou de son représentant désigné dans vos ententes avec cyberSanté Ontario.

4.1.3 Dérogation à une directive en matière de consentement

Organisations qui utilisent le visualiseur clinique de ConnexionOntario

Dans des cas exceptionnels, la solution ConnexionOntario permet à un fournisseur de soins de santé de déroger provisoirement à une directive en matière de consentement d'un patient. Les fournisseurs peuvent obtenir une dérogation temporaire à une directive en matière de consentement dans les circonstances suivantes :

- Le fournisseur obtient l'autorisation expresse du patient 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 patient auquel se rapportent les renseignements personnels sur la santé et qu'il n'est pas raisonnablement possible d'obtenir le consentement du patient 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 patient auquel se rapportent les renseignements personnels sur la santé, ou pour un groupe de personnes.

La dérogation temporaire et le nom du fournisseur de soins de santé qui la demande sont consignés dans la solution ConnexionOntario. La dérogation sera en vigueur pour un maximum de 24 heures dans la solution ConnexionOntario. Lorsqu'un agent du DSR déroge à une directive en matière de consentement, cyberSanté Ontario avisera le bureau responsable de la protection de la vie privée du DSR. Ensuite, il incombera au bureau responsable de la protection de la vie privée du DSR :

1. de faire enquête sur la dérogation pour s'assurer qu'elle a été demandée pour une des raisons énoncées ci-dessus;
2. d'aviser le patient de la dérogation dès que possible.

Si la dérogation à la directive en matière de consentement vise à éliminer ou réduire un risque important de lésion corporelle grave pour une personne autre que le patient auquel se rapportent les renseignements personnels sur la santé, ou pour un groupe de personnes, le DSR doit fournir un avis écrit au Commissaire à l'information et à la protection de la vie privée de l'Ontario (CIPVP) dès que possible pour lui indiquer que la dérogation a eu lieu. Pour obtenir de plus amples renseignements sur le contenu de l'avis au CIPVP, voir la Politique de gestion du consentement – Dossier de santé électronique.

Les dérogations aux directives en matière de consentement dans le Système d'information de laboratoire de l'Ontario (SILO) ne peuvent être accordées qu'avec le consentement exprès du patient ou de son mandataire spécial. Pour obtenir de plus amples renseignements, voir le *Guide des fournisseurs de soins de santé – Laboratoires* (SILO).

Organisations qui utilisent le visualiseur clinique de ClinicalConnect

Actuellement, il est impossible de déroger à une directive de consentement sur visant les données du RDC à partir du visualiseur clinique de ClinicalConnect.

4.2 Demandes d'accès formulées par les patients

4.2.1 Demandes d'accès aux données

Aux termes de la *Loi de 2004 sur la protection des renseignements personnels sur la santé* (*LPRPS*), un patient ou son mandataire spécial a un droit d'accès aux renseignements qu'un DRS conserve à son sujet. Lorsqu'un fournisseur de soins de santé reçoit une demande d'accès aux dossiers du RDC qu'il a recueillis ou créés, ou auxquels il a contribué, le fournisseur doit se conformer aux dispositions de la partie V de la *LPRPS,* ainsi qu'à ses propres politiques, méthodes et pratiques internes pour répondre directement à la personne qui a présenté la demande.

Quand la demande d'accès concerne des renseignements fournis par un autre DRS ou par plusieurs DRS, le fournisseur de soins doit :

- informer le patient que sa demande porte sur des renseignements personnels sur la santé qui ne se trouvent pas sous la garde ou le contrôle du DRS auquel la demande a été adressée;
- inviter le patient à communiquer avec cyberSanté Ontario au 1 866 250-1554 ou à l'adresse info@ehealthontario.on.ca.

En vertu de la Politique sur l'accès aux renseignements et la rectification des renseignements – Dossier de santé électronique, cyberSanté Ontario peut demander l'aide du DRS pour répondre directement à une demande d'accès formulée par un patient. Le DRS doit fournit à cyberSanté Ontario les coordonnées d'une personne-ressource de l'organisation qui pourra l'aider à accomplir la tâche.

4.2.2 Demandes d'accès aux journaux de vérification

Les journaux de vérification sont des rapports indiquant qui a consulté les renseignements cliniques vous concernant (à quel moment et à partir de quel endroit, etc.).

Lorsqu'un patient demande à un fournisseur de lui donner accès aux journaux de vérification des dossiers le concernant stockés dans le RDC, le DRS doit :

- aviser le patient qu'il se trouve dans l'impossibilité de traiter sa demande d'accès;
- inviter le patient à communiquer avec cyberSanté Ontario au 1 866 250-1554 ou à l'adresse info@ehealthontario.on.ca.

N.B. : Veuillez noter que les demandes d'accès et les demandes d'accès aux journaux de vérification doivent être présentées par la personne responsable de la protection de la vie privée de votre organisation.

4.3 Demandes de rectification

Lorsqu'un DRS reçoit une demande de rectification directement d'un patient concernant des dossiers de santé qu'il est le seul à avoir créés et versés dans le RDC, il doit respecter la partie V de la *LPRPS* ainsi que ses politiques, procédures et pratiques internes pour répondre à la demande de rectification du patient.

- À la demande du patient, lorsqu'une rectification est effectuée, le DRS doit informer cyberSanté Ontario de la rectification et demander un rapport de vérification des personnes ayant accédé au dossier, au cas où le patient souhaite informer d'autres DRS ayant consulté son dossier. Le DRS doit ensuite aviser les établissements ayant consulté le dossier du patient qu'une rectification a été apportée.

Si un DRS reçoit une demande de rectification directement d'un patient concernant des dossiers de santé créés et versés dans le RDC par un ou plusieurs autres DRS, il doit répondre dans les deux jours suivant la réception de la demande de rectification pour :

1. informer le patient que la demande de rectification concerne des renseignements personnels sur la santé qui ne sont pas sous sa garde ou son contrôle;
2. indiquer au patient qu'il doit communiquer avec cyberSanté Ontario au 1 866 250-1554 ou à l'adresse info@ehealthontario.on.ca.

cyberSanté Ontario coordonnera le traitement de cette demande; il est possible qu'il demande l'aide du ou des DRS pour répondre au patient. Le DRS doit fournir à cyberSanté Ontario les coordonnées d'une personne-ressource de l'organisation qui pourra l'aider à accomplir la tâche.

N.B. : Les demandes de rectification doivent être faites par la personne responsable de la protection de la vie privée de votre organisation.

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

Aide-mémoire
Si une personne dépose une plainte ou demande de l'information concernant le RDC, invitez-la à communiquer avec cyberSanté Ontario.

Si le DRS reçoit une plainte ou une demande d'information concernant uniquement ses dossiers dans le RDC, 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 RDC ou les mandataires ou fournisseurs de services électroniques de cyberSanté Ontario, et qu'il est incapable de la traiter, il doit :

1. aviser la personne que le DRS n'est pas en mesure de répondre à sa demande ou à sa plainte;
2. indiquer au patient qu'il doit communiquer avec cyberSanté Ontario au 1 866 250-1554 ou à l'adresse info@ehealthontario.on.ca.

cyberSanté Ontario peut demander l'aide du ou des DRS pour répondre directement à la demande ou à la plainte qu'il a reçue.

4.5 Conservation de l'information

Aide-mémoire
Les DRS doivent conserver les dossiers de renseignements personnels sur la santé durant une période donnée. Tout renseignement recueilli pour traiter les demandes d'accès, de rectification et d'information et les plaintes, ainsi que les renseignements en lien avec les directives en matière de consentement doivent être conservés durant deux ans après la réception d'une demande.

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

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

Type de renseignements	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 : o demandes d'accès ou de rectification en vertu de la *LPRPS*; o demande de formulation, de modification ou de retrait d'une directive en matière de consentement en vertu de la *LPRPS*; o 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, cyberSanté 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, cyberSanté 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.
Ressources ou modèles élaborés par cyberSanté Ontario concernant le DSE.	Au moins deux ans.
Documents liés aux assurances.	10 ans.

Les types de renseignements personnels sur la santé contenus dans chacun de ces types de renseignements sont détaillés dans la Politique de conservation – Dossier de santé électronique.

4.6 Formation sur la sécurité et la protection de la vie privée

Les DRS doivent offrir à leurs mandataires et à leurs fournisseurs de services électroniques une formation sur la sécurité et la protection de la vie privée avant que ces derniers n'accèdent au RDC. Cette formation vise à les informer de leurs obligations en vertu des lois applicables sur la protection de la vie privée (p. ex., la *LPRPS*) et des politiques et procédures pertinentes sur la sécurité et la protection de la vie privée en lien avec le RDC. Les utilisateurs finaux doivent suivre la formation :

1. avant qu'un compte à leur nom ne soit créé dans le RDC;
2. avant d'avoir accès au RDC;
3. chaque année.

Cette formation fait partie du processus de déploiement du RDC dans votre établissement.

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 dans le cadre du processus de déploiement, et annuellement par la suite.

Pour faciliter le processus, cyberSanté Ontario a mis au point des aides didactiques associées aux différents postes. Pour obtenir de plus amples renseignements sur le contenu de la formation, consultez la Politique sur la formation en protection de la confidentialité et de la sécurité – Dossier de santé électronique et la trousse de protection de la vie privée (EHR Privacy Toolkit, en anglais seulement).

4.7 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 appeler cyberSanté Ontario au 1 866 250-1554, ou écrire à l'adresse info@ehealthontario.on.ca.

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

4.8 Gestion des atteintes à la confidentialité

Aide-mémoire
Les DRS doivent signaler toute atteinte à la confidentialité réelle ou présumée en appelant dans les plus brefs délais le Service de dépannage de cybersanté Ontario au 1 866 250-1554 (ouvert 24 heures sur 24, 7 jours sur 7).

La marche à suivre en cas d'atteinte à la confidentialité ou d'incident réel ou présumé est décrite en détail dans la Politique de gestion des atteintes à la confidentialité – Dossier de santé électronique.

Les DRS doivent signaler toute atteinte à la confidentialité réelle ou présumée à cyberSanté Ontario en appelant dans les plus brefs délais – ou au plus tard avant la fin du jour ouvrable suivant – le Service de dépannage au 1 866 250-1554 (ouvert 24 heures sur 24, 7 jours sur 7). Aux termes de la Politique de gestion des atteintes à la confidentialité – Dossier de santé électronique, les DRS doivent aviser cyberSanté Ontario s'ils ont connaissance d'un tel incident, 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;
- cyberSanté 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 cyberSanté Ontario ou de tout autre DRS.

Dans les cas où l'atteinte à la confidentialité est causée par un DRS qui est le seul à avoir créé et ajouté les données dans le RDC, 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 l'atteinte à la confidentialité, faire enquête et corriger le problème.

Dans les cas où l'atteinte à la confidentialité 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 RDC, le DRS doit, en collaboration avec les autres DRS ayant ajouté des données et cyberSanté Ontario, trouver la personne en question pour faire enquête. Les rôles de chacune des parties prenantes sont inscrits dans la Politique de gestion des atteintes à la confidentialité – Dossier de santé électronique.

4.9 Gestion des atteintes à la confidentialité et des incidents de sécurité

Voici les directives à l'intention des DRS pour le signalement à cyberSanté Ontario des incidents de sécurité ou des atteintes à la confidentialité (voir définitions ci-dessous) liés au RDC.

Un incident de sécurité s'entend d'une situation non désirée ou imprévue entraînant :

- un manquement aux politiques, aux procédures, aux pratiques ou aux exigences de sécurité de l'établissement;
- la consultation, l'utilisation ou l'étude non autorisée de renseignements;
- la divulgation, la destruction, la modification ou la rétention non autorisée de données;
- une violation des ententes conclues entre cyberSanté Ontario et votre établissement, les utilisateurs de votre établissement ou ses employés, mandataires ou fournisseurs de services;
- une tentative d'atteinte ou une atteinte réelle ou présumée à la sécurité;
- la suppression, la fraude, l'abus, le vol, la perte ou des dommages en lien avec des ressources.

Le processus de gestion des atteintes à la confidentialité et des incidents de sécurité ne s'applique pas à la gestion des incidents survenant au sein des DRS et ne vise pas les DRS, leurs mandataires ou leurs fournisseurs de services électroniques qui ne créent et ne consultent pas de renseignements personnels sur la santé dans le RDC.

4.9.1 Instructions à l'intention des fournisseurs de soins de santé

Si vous avez connaissance ou soupçonnez l'existence d'une atteinte à la confidentialité ou d'un incident de sécurité en lien avec le RDC ou ses données causés par vous-même ou l'un de vos employés, mandataires ou fournisseurs de services, vous devez le signaler immédiatement à la personne de votre organisation désignée responsable de la protection de la vie privée. Si vous ne parvenez pas à la joindre ou à joindre l'équipe de soutien, veuillez appeler le Service de dépannage de cyberSanté Ontario au 1 866 250-1554 et demandez à ce que soit créé un dossier d'incident de sécurité.

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

Important : Il est extrêmement important de ne pas divulguer de renseignements personnels du patient, sur la santé ou autres, au Service de dépannage lorsque vous signalez une atteinte à la confidentialité ou un incident de sécurité.

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

Il est possible que votre établissement, selon sa nature et sa taille, n'ait pas de bureau de protection de la vie privée ou de responsable de la protection de la vie privée. Dans ce cas, une personne a été désignée responsable de la protection de la vie privée dans le cadre de votre entente avec cyberSanté Ontario.

Si vous avez connaissance ou soupçonnez l'existence d'une atteinte à la confidentialité ou d'un incident de sécurité en lien avec le RDC ou ses données causés par un membre du personnel de votre établissement, comme un employé, un mandataire ou un fournisseur de services, vous devez le signaler immédiatement au Service de dépannage de cyberSanté Ontario au 1 866 250-1554 et demander à ce que soit créé un dossier d'atteinte à la confidentialité ou d'incident de sécurité.

Important : Il est extrêmement important de ne pas divulguer de renseignements personnels du patient, sur la santé ou autres, au Service de dépannage lorsque vous signalez une atteinte à la confidentialité ou un incident de sécurité. Vous devrez prêter votre concours à toute enquête menée par cyberSanté Ontario sur l'atteinte ou l'incident en lien avec les données.

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

1. L'heure et la date de l'incident signalé;
2. Le nom et les coordonnées du mandataire ou du fournisseur de services électroniques qui a signalé l'incident;
3. Une description de l'incident (p. ex., le type d'incident et la façon dont il a été détecté);
4. Les conséquences de l'incident;
5. Les mesures adoptées 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, le responsable ou l'équipe responsable des interventions en cas d'incident est chargé de gérer la situation. Un plan d'atténuation des risques est alors élaboré de concert avec le demandeur.

5 Liste des mesures de protection mises en place par cyberSanté Ontario

5.1 Mesures de protection administratives

- cyberSanté Ontario a un directeur général de la protection de la vie privée et un directeur général de la sécurité de l'information; ceux-ci sont responsables de la protection des renseignements sur la santé et de la sécurité.
- Le Comité de protection de la vie privée et de sécurité (composé des établissements de soins de santé utilisant le RDC) supervise les programmes de confidentialité et de sécurité.
- Les établissements de soins de santé doivent veiller à ce que leurs fournisseurs de soins de santé connaissent leurs responsabilités.
- Les ententes, les politiques et les procédures définissent les rôles des établissements pour la protection des RP et des renseignements personnels sur la santé, de même que les rôles de toute personne travaillant pour l'établissement et de tout fournisseur de services qu'il emploie. Les employés et les sous-traitants de l'établissement doivent lire les politiques pertinentes et signer une attestation confirmant qu'ils les ont lues et comprises, et qu'ils s'engagent à s'y conformer.
- Lorsque le Comité de protection de la vie privée et de sécurité juge qu'un changement suffisamment important a été apporté au RDC ou au système d'information, des évaluations de la confidentialité et de la sécurité sont menées pour évaluer les nouveaux risques.
- cyberSanté Ontario informe les établissements de soins de santé de tout accès non autorisé aux renseignements personnels ou aux renseignements personnels sur la santé qu'ils ont versés dans le RDC.
- Le personnel, les consultants, les fournisseurs et les utilisateurs du RDC doivent signaler rapidement toute atteinte à la vie privée ou à la sécurité afin qu'une enquête soit menée. Un programme de gestion des incidents de sécurité et des atteintes à la confidentialité a été mis sur pied pour gérer les incidents et les activités régulières de formation et de sensibilisation des employés qui assurent la gestion des incidents.

5.2 Mesures de protection techniques

- Seuls les fournisseurs de soins de santé autorisés et leur personnel de soutien autorisé peuvent consulter les renseignements se trouvant dans le RDC.
- Les utilisateurs doivent entrer leurs authentifiants chaque fois qu'ils accèdent au système.
- Lorsqu'une personne consulte des renseignements personnels ou des renseignements personnels sur la santé, cette information est enregistrée électroniquement.
- Les renseignements personnels et les renseignements personnels sur la santé envoyés par les établissements et ceux qu'ils reçoivent sont toujours cryptés.
- Les réseaux sont protégés par des dispositifs (pare-feu et routeurs) qui limitent l'accès aux systèmes.
- Toutes les activités liées au système d'information sont journalisées afin que les responsables de la protection de la vie privée et les établissements de soins de santé puissent surveiller les fournisseurs de soins de santé et les employés qui consultent les renseignements personnels et les renseignements personnels sur la santé stockés dans le système d'information et mener des vérifications à leur égard.
- Des dispositifs de sécurité sont installés sur chaque système pour protéger le RDC des logiciels malveillants et pour détecter les intrusions.

- La vulnérabilité des configurations techniques et des pratiques opérationnelles de sécurité est évaluée régulièrement.

5.3 Mesures de protection physiques

- Les renseignements personnels et les renseignements personnels sur la santé sont stockés dans un centre de données à accès restreint doté de caméras, de systèmes d'alarme et d'un service de sécurité 24 heures sur 24, 7 jours sur 7.
- Lorsque des serveurs ne sont plus requis, les disques durs contenant les renseignements personnels et les renseignements personnels sur la santé sont physiquement détruits ou effacés de manière permanente.
- Les renseignements ne sortent jamais physiquement du centre de données.

Glossaire

Sigle	Terme
CASC	Centre d'accès aux soins communautaires
CIPVP	Commissaire à l'information et à la protection de la vie privée
DME	Dossier médical électronique
DRS	Dépositaire de renseignements sur la santé
DSE	Dossier de santé électronique
LPRPS	*Loi de 2004 sur la protection des renseignements personnels sur la santé*
RDC	Répertoire des données cliniques
TI	Technologie de l'information