cyberSanté Ontario
Travaille pour vous

Guide de soutien de cyberSanté Ontario

Répertoire des données cliniques (RDC)

Guide de référence et obligations et procédures en matière de sécurité et de protection de la vie privée

Le présent guide s'adresse aux établissements qui ont déployé une interface électronique liée à l'un des répertoires de données cliniques (RDC) de cyberSanté Ontario, et qui ont signé ou signeront l'Annexe des services d'interface des dossiers de santé électroniques (DSE). Il fournit aux établissements des renseignements sur les processus liés aux RDC, sur les procédures et obligations en matière de sécurité et de vie privée et sur la façon de communiquer avec cyberSanté Ontario pour obtenir de l'assistance.

Ontario
cyber Santé Ontario

Version 2.2

Avis de droit d'auteur

Tous droits réservés

Marques de commerce

1 Table des matières

2 Généralités

2.1 Objet et portée

Le présent guide de soutien est un document exhaustif présentant les processus relatifs à l'utilisation des répertoires de données cliniques (RDC), notamment :

- l'inscription de nouveaux utilisateurs et établissements et leur connexion à un ou plusieurs RDC;
- les processus de soutien de haut niveau entre les différentes parties en cas d'incident survenant pendant l'utilisation d'un RDC;
- les obligations en matière de protection de la vie privée et de sécurité relatives aux RDC;
- vos responsabilités opérationnelles relatives à l'utilisation des données des RDC.

2.2 Destinataires

Le présent document est destiné aux utilisateurs des visualiseurs cliniques régionaux (p. ex., visualiseur ClinicalConnect de la Hamilton Health Sciences Corporation) qui serviront d'« interface de l'application » assurant la communication entre les RDC de cyberSanté Ontario et les établissements qui consultent des données cliniques dans l'un des RDC.

Le présent document se veut un complément à l'Annexe des services d'interface des DSE que les organisations ont signé ou signeront afin d'afficher des données des RDC dans les visualiseurs cliniques régionaux.

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 normes 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
- Guide des normes d'interaction avec les services

3 Modèle de soutien des RDC

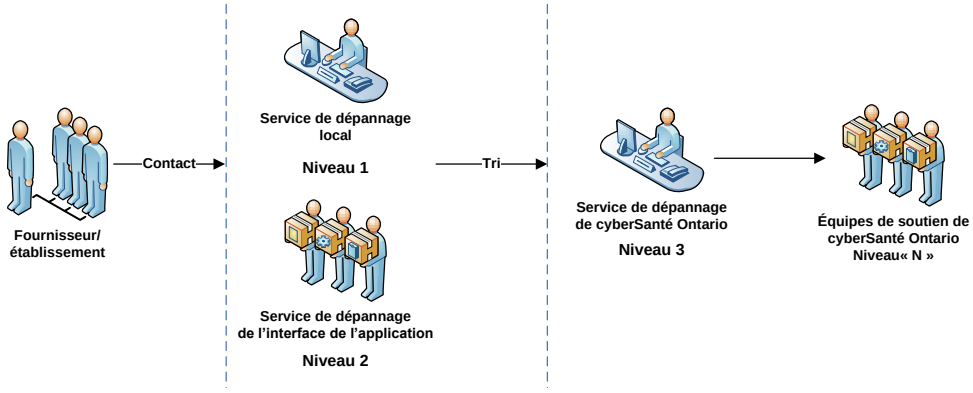


Figure 1 – Modèle de soutien de haut niveau

Comme illustré dans la figure 1 ci-dessus, lorsqu'un fournisseur ou un établissement éprouve des difficultés liées au RDC, il doit suivre le processus ci-dessous. Pour obtenir de plus amples renseignements, veuillez consulter le Guide des normes d'interaction avec les services.

1. **NIVEAU 1 :** Le fournisseur ou l'établissement communique avec le service de dépannage de son organisation, qui recueille les renseignements nécessaires sur le problème. Le service de dépannage local mène ensuite une enquête sur le problème, et le résout, dans la mesure du possible.
    - Veuillez noter que les services de dépannage locaux ont leur propre processus d'enquête. De plus, les établissements ne disposent pas tous d'un service de dépannage.
2. **NIVEAU 2 :** Si le service de dépannage local ne peut résoudre le problème, l'établissement communique avec le service de dépannage de l'interface de l'application et lui fournit les renseignements sur le problème. Le service de dépannage de l'interface de l'application mène ensuite une enquête et le résout le problème, dans la mesure du possible.
    - Veuillez noter que ce processus est régi par un mécanisme de soutien distinct établi entre vous et les établissements locaux que vous gérez.
3. **NIVEAU 3 :** Si le service de dépannage de l'interface de l'application ne peut résoudre le problème, il communique avec le Service de dépannage de cyberSanté Ontario au nom de l'établissement pour lui fournir les renseignements sur le problème. Le Service de dépannage de cyberSanté Ontario mène ensuite une enquête et résout le problème.
4. **NIVEAU « N » :** Si le Service de dépannage de cyberSanté Ontario ne peut résoudre immédiatement le problème, celui-ci sera soumis à différentes équipes de soutien de cyberSanté Ontario, en fonction de la nature du problème : ce sont les équipes de soutien de niveau « N ».

Comme les processus de soutien des services de dépannage des établissements et des services de dépannage de l'interface de l'application sont régis par des ententes distinctes, le présent guide portera sur les processus de soutien des services de dépannage de l'interface de l'application et de cyberSanté Ontario. Cependant, les services de dépannage locaux (niveau 1) et les services de dépannage de l'interface de l'application (niveau 2) sont tenus de faire ce qui suit avant de communiquer avec le Service de dépannage de cyberSanté Ontario :

- Diagnostiquer les problèmes.
- Résoudre les problèmes, dans la mesure du possible.
- Déterminer les effets potentiels des problèmes.
- Transmettre le problème aux groupes de soutien appropriés et/ou au Service de dépannage de cyberSanté Ontario.

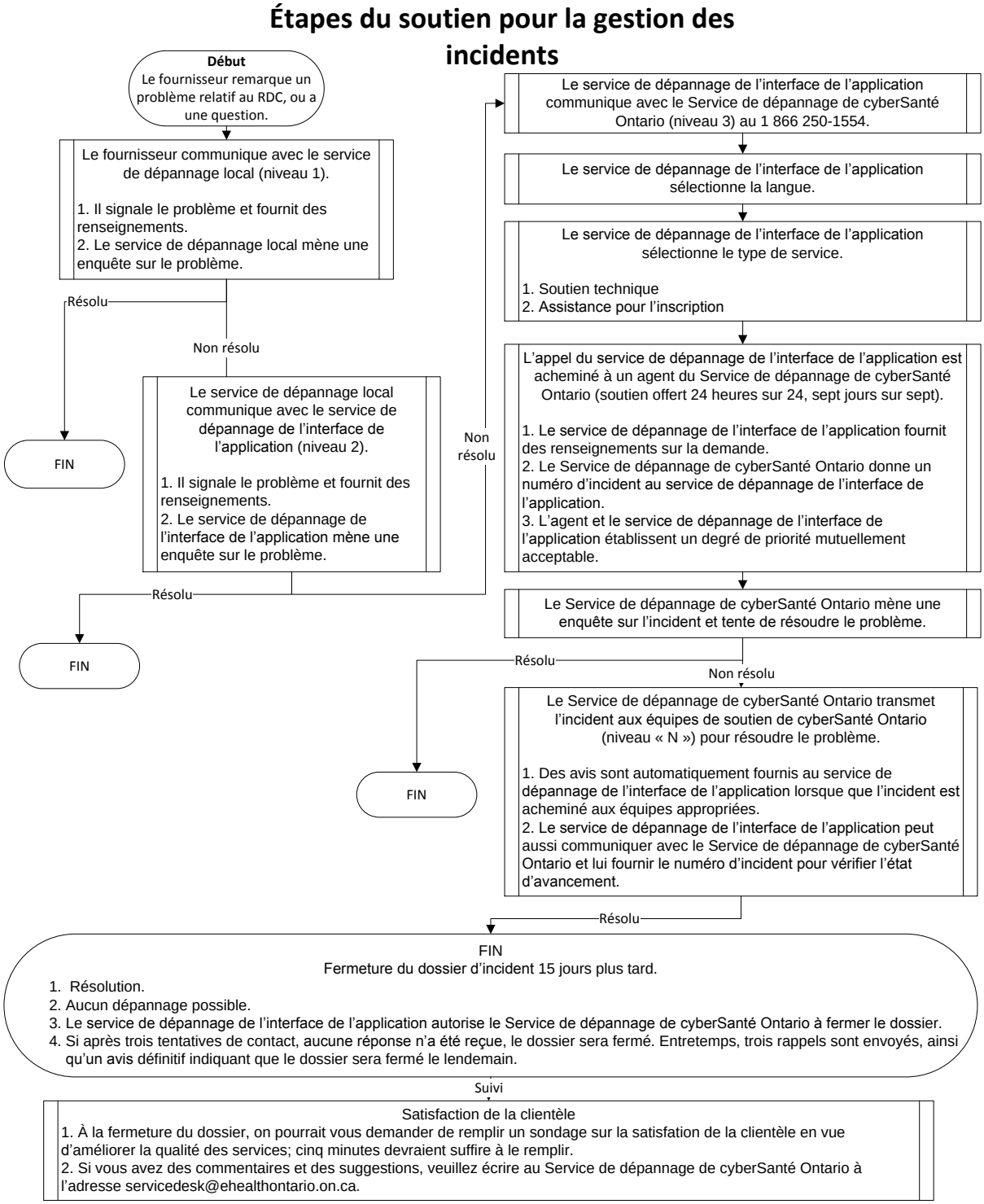


Figure 2 – Étapes du soutien pour la gestion des incidents

3.1 Quand communiquer avec le Service de dépannage de cyberSanté Ontario?

Les services de dépannage de l'interface de l'application doivent communiquer avec le Service de dépannage de cyberSanté Ontario :

1. en cas d'incident affectant le propriétaire de l'interface de l'application;
2. lorsqu'un incident lui ayant été transmis par un établissement et son service de dépannage local n'a pas pu être résolu.

Ces incidents comprennent ce qui suit :

- Résolution de problèmes relatifs aux certificats d'infrastructure à clé publique (ICP) du RDC;
- Résolution des problèmes d'interface en lien avec le service;
- Signalement d'une erreur d'une application des RDC;
- Signalement de résultats manquants dans les RDC;
- Signalement de problèmes relatifs à la qualité des données de l'un des RDC;
- Signalement d'une atteinte à la vie privée réelle ou présumée;
- Demande de renseignements à cyberSanté Ontario sur :
    - les fonctions des RDC;
    - la protection et la sécurité des renseignements personnels sur la santé (RPS).

Le Service de dépannage de cyberSanté Ontario constitue un point de contact unique pour ouvrir des dossiers sur les problèmes en lien avec les RDC.

3.2 Comment communiquer avec le Service de dépannage de cyberSanté Ontario?

Les services de dépannage de l'interface de l'application peuvent communiquer avec cyberSanté Ontario aux coordonnées suivantes :

Courriel* : servicedesk@ehealthontario.on.ca
Téléphone* : 1 866 250-1554
Télécopieur : 416 586-4040
(Lorsque vous télécopiez un document relatif à un incident ou à une demande de service, veuillez en informer le Service de dépannage de cyberSanté Ontario par téléphone.)

*N.B. : Le téléphone est le moyen de communication privilégié du Service de dépannage de cyberSanté Ontario. Il n'existe actuellement aucune entente de niveau de service relative au signalement d'incidents ou à la présentation de demandes de service par courriel.

Le Service de dépannage reçoit les appels 24 heures sur 24, 7 jours sur 7, 365 jours par an.

3.3 Renseignements à fournir au Service de dépannage de cyberSanté Ontario

Lorqu'un membre du service de dépannage de l'interface de l'application communique avec le Service de dépannage de cyberSanté Ontario pour signaler un incident, il doit fournir certains renseignements au préposé, notamment :

- votre nom;
- l'adresse de votre établissement;
- vos coordonnées ainsi que celles d'une personne-ressource secondaire, au besoin;
- les données que l'on tente d'envoyer ou de consulter (p. ex., données sur l'imagerie diagnostique, les soins primaires ou actifs ou les données de laboratoire);
- l'environnement de service de cyberSanté Ontario touché (p. ex., production ou tests);
- la description du problème, notamment la date et l'heure de l'incident, le nombre d'utilisateurs concernés (s'il le connaît);
- les étapes à suivre pour reproduire le problème et les mesures de diagnostic et de dépannage prises.

- Emplacement (nom de l'hôpital ou de l'organisation)
- Coordonnées du point de service
- Identifiant de l'auteur autorisé de l'appel
- Numéro du billet d'incident de l'établissement
- Description du problème
- Effets du problème
- Date et heure de la première occurrence du problème
- Degré de priorité établi par le service de dépannage de l'établissement, ou par l'expert en la matière
- Solution de rechange (le cas échéant)

Lors du signalement de problèmes relatifs à la qualité des données, à des résultats manquants ou à des données inexactes, il faut fournir les renseignements suivants au Service de dépannage de cyberSanté Ontario :

- vos coordonnées (numéro de téléphone et adresse courriel);
- le nom de votre organisation ou de l'organisation au nom de laquelle vous faites le signalement (p. ex., un cabinet médical, un hôpital ou un service);
- le nom de l'organisation qui a présenté le résultat;
- le contenu du message (organisation, nom du patient et numéro de dossier médical);
- l'information manquante (si vous signalez uniquement un résultat manquant);
- les raisons pour lesquelles vous croyez que les données du RDC sont inexactes, le cas échéant.

Ces renseignements doivent être fournis conformément à la Procédure de transfert de fichiers sensibles par courriel de l'annexe A.

Pour recueillir ces renseignements, les services de dépannage de l'interface de l'application pourraient avoir à communiquer avec le fournisseur qui a rencontré le problème, ou avec le service de dépannage de l'établissement.

cyberSanté Ontario recommande aux services de dépannage de l'interface de recueillir ces renseignements auprès des services de dépannage local dès le premier contact, ce qui permettra à cyberSanté Ontario d'accélérer le processus de tri, d'enquête et de résolution si l'incident passe au niveau 3. Si le service de dépannage de l'interface de l'application ou le service de dépannage local doit interrompre le processus pour recueillir ces renseignements, ce sera plus long avant qu'il puisse commencer l'enquête et résoudre le problème.

Pour faire le suivi d'un incident, les services de dépannage de l'interface de l'application doivent indiquer le numéro d'incident fourni par le Service de dépannage de cyberSanté Ontario lors du signalement.

3.4 Quand cyberSanté Ontario communique-t-il avec vous?

Le Service de dépannage de cyberSanté Ontario peut communiquer avec les services de dépannage de l'interface de l'application pour :

- obtenir des précisions sur un incident signalé;
- les informer que le système fait l'objet d'une maintenance qui pourrait avoir des répercussions sur le service de l'établissement;
- signaler une panne dans l'application du RDC;
- les informer des dates de sortie de ses nouvelles versions et des améliorations apportées à l'application;
- lui demander de communiquer avec le service de dépannage local ou avec le fournisseur pour faire un suivi, mener une enquête sur un problème, recueillir des renseignements supplémentaires ou donner des renseignements sur concernant l'incident.

Le Bureau de la protection de la vie privée et le Bureau de la sécurité de cyberSanté Ontario peuvent communiquer avec les services de dépannage de l'interface de l'application pour :

- demander des renseignements supplémentaires afin de donner suite aux demandes d'accès aux renseignements du RDC et aux demandes de correction de ces renseignements;
- soutenir la coordination des incidents en lien avec la protection de la vie privée et la sécurité.

4 Responsabilités opérationnelles liées aux données des RDC

Aux termes de la *Loi de 2004 sur la protection des renseignements personnels sur la santé (LPRPS)*, cyberSanté Ontario est tenue de conserver un registre électronique répertoriant toutes les fois où des données des RDC figurant dans son système ou dans celui d'un tiers ont été consultées.

Afin de répondre à cette exigence, cyberSanté Ontario doit avoir accès à une copie des journaux de vérification tenus par les utilisateurs des visualiseurs cliniques régionaux, qui devraient indiquer :

- les noms des personnes qui ont consulté des renseignements, et les renseignements consultés;
- le moment auquel les renseignements ont été consultés;
- l'endroit d'où la demande a été envoyée.

cyberSanté Ontario pourrait devoir produire des rapports sur ces journaux de vérification dans le cadre d'enquêtes sur des incidents relatifs à la protection de la vie privée afin de répondre aux demandes des patients.

5 Protection de la vie privée et sécurité

5.1 Gestion du consentement

Aide-mémoire

Les RDC permettent aux patients ou à leur mandataire spécial de restreindre ou rétablir l'accès aux données les concernant dans le système. Les patients qui souhaitent donner une directive en matière de consentement dans un 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.

Les RDC donnent 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.

Les RDC permettent 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 les 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 particulier (p. ex., l'hôpital A) n'auraient pas accès aux renseignements personnels sur la santé d'un patient dans le RDC.
- **Mandataires :** 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.

5.1.1 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 d'un patient doivent être déposées par la personne de votre DRS 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.

5.2 Demandes d'accès formulées par les patients

Aide-mémoire
Lorsqu'un patient présente une demande d'accès aux données que votre établissement a saisies, ou une demande de correction de ces données, suivez vos procédures internes pour lui accorder l'accès ou pour apporter les corrections nécessaires. Consignez cette demande.

Lorsqu'un patient présente une demande d'accès aux données que d'autres DSR ont saisies, ou une demande de correction de ces données, invitez le patient à présenter sa demande à cyberSanté Ontario dès que possible au 1 866 250-1554.

5.2.1 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 d'un 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 :

1. 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;
2. 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.

5.2.2 Demandes d'accès aux journaux de vérification

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

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

5.3 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 l'un des 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 l'un des RDC par un ou plusieurs autres DRS, le fournisseur doit répondre dans les deux jours suivant la réception de la demande de rectification pour :

- 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;
- 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 fournit à cyberSanté Ontario les coordonnées d'une personne-ressource de l'organisation qui pourra l'aider à accomplir la tâche.

5.4 Demandes d'information sur la protection de la vie privée

5.4.1 Plaintes et demandes d'information

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

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

- aviser la personne que le DRS n'est pas en mesure de répondre à sa demande ou à sa plainte;
- 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.

5.4.2 Demandes d'information de fournisseurs de soins de santé

Pour toute question relative aux processus de protection de la vie privée décrits ci-dessus, y compris la manière de traiter les demandes d'accès aux renseignements personnels, les obligations relatives au consentement ou les processus de gestion des incidents ou des atteintes à la confidentialité, le fournisseur de soins de santé doit communiquer avec cyberSanté Ontario au 1 866 250-1554 ou à l'adresse info@ehealthontario.on.ca.

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

5.5 Gestion des atteintes à la confidentialité

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

La présente section énonce les directives que les DRS doivent suivre lorsqu'ils signalent à cyberSanté Ontario tout incident de sécurité ou toute atteinte à la confidentialité (voir les définitions ci-dessous).

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 l'organisation, les utilisateurs de l'organisation 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 les RDC.

5.5.2 Gestion des atteintes à la confidentialité

Aide-mémoire
Les DRS doivent signaler toute atteinte à 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 connexe 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). 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 l'un des 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.

5.5.3 Instructions à l'intention des fournisseurs de soins de santé – Incident de sécurité

Si vous avez connaissance ou soupçonnez l'existence d'une atteinte à la confidentialité ou d'un incident de sécurité en lien avec l'un des 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 établissement désignée comme 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 toute enquête. Durant l'enquête, il se peut que l'on vous demande de fournir des renseignements supplémentaires, notamment des renseignements personnels sur la santé ou des renseignements personnels, 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.

5.5.4 Instructions à l'intention de la personne désignée comme responsable de la protection de la vie privée – Incident de sécurité

Si vous avez connaissance ou soupçonnez l'existence d'une atteinte à la confidentialité ou d'un incident de sécurité en lien avec l'un des RDC ou ses données causés par vous-même ou l'un de vos employés, mandataires ou fournisseurs 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'incident de sécurité.

Important : Il est extrêmement important de ne pas divulguer des renseignements personnels du patient, sur la santé ou autres, au Service de dépannage lorsque vous signalez une atteinte à la vie privée ou un incident. 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 prises par le mandataire ou le fournisseur de services électroniques qui a signalé l'incident ou par le point de contact pour en limiter les répercussions.

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.

6 Enregistrement des utilisateurs des services

Les fournisseurs pourront accéder à un RDC dans une interface d'application au moyen de divers systèmes de points de service (p. ex., Internet ou système d'information hospitalier).

Il faut rappeler aux fournisseurs qu'actuellement, ils n'ont pas tous accès aux systèmes de points de service. Les fournisseurs doivent communiquer avec leurs opérateurs d'interface d'application pour savoir quels systèmes de points de service ils peuvent utiliser pour accéder aux données des RDC. De plus, les fournisseurs qui peuvent utiliser une interface d'application n'ont pas nécessairement accès à l'un des RDC; ils doivent communiquer avec leur opérateur d'interface d'application pour le savoir.

Selon les organisations, les fournisseurs utiliseront l'un des différents authentifiants pour accéder aux RDC des interfaces d'application.

1. Authentifiants de ONE ID^{MD} communiqués par cyberSanté Ontario
2. Authentifiants locaux communiqués par l'établissement de soins de santé
3. Authentifiants communiqués par les propriétaires de l'interface d'application

Pour s'enregistrer, les nouveaux utilisateurs doivent communiquer avec l'autorité locale d'enregistrement de leur organisation et remplir le formulaire prévu à cette fin. Les utilisateurs obtiendront des authentifiants pour accéder à l'un des RDC, c'est-à-dire un nom d'utilisateur unique et un mot de passe.

Annexe A : Procédure de transfert de fichiers sensibles par courriel

Présentation

En vertu des politiques de cyberSanté 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, CD, DVD, clé USB, carte mémoire flash, etc.).

Le présent document 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 disponible 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 et/ou des renseignements personnels sur la santé par courriel, conformément à vos processus administratifs habituels.

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

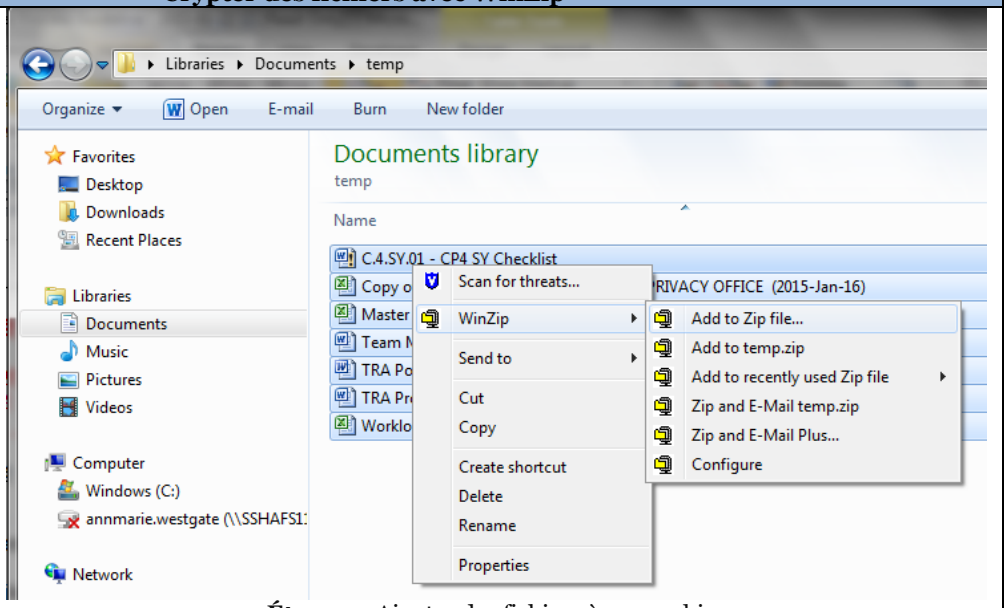
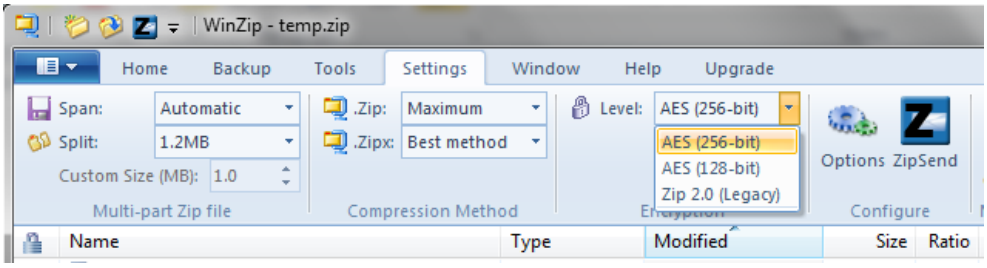
cyberSanté Ontario limite la taille des pièces jointes à 10 Mo par courriel.

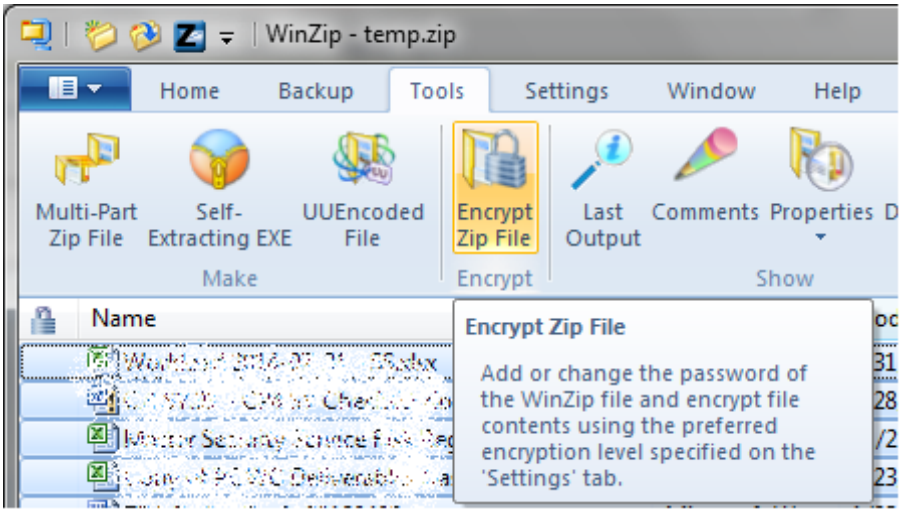
Pour obtenir de l'aide, veuillez appeler le Service de dépannage de cyberSanté Ontario au 1 866 250-1554.

Comment crypter un fichier et créer un mot de passe?

Utiliser le logiciel de cryptage WinZip

cyberSanté Ontario suggère d'utiliser les versions standards de l'outil de cryptage ***WinZip 16.0.***

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 que vous voulez.	 **Étape 1 :** Ajouter des fichiers à une archive
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 3 :** Choisir un niveau de cryptage

Crypter des fichiers avec WinZip	
Étape 4 : Crypter le fichier Dans le menu Outils, cliquez sur **Crypter le fichier Zip.**	 **Étape 4 :** Crypter le fichier Zip
Étape 5 : Entrer un mot de passe difficile à deviner Entrez un mot de passe, puis confirmez-le. Pour savoir comment créer un mot de passe difficile à deviner, consulter la section « **Créer un mot de passe** » ci-après.	 **Figure 4 :** Créer un mot de passe difficile à deviner

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.

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. 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.

Le processus de création du mot de passe doit respecter les exigences ci-dessous.

Créer un mot de passe

- Créer un mot de passe difficile à deviner 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., !, $, #, _, ~, % et ^).
- Exemple d'un mot de passe trop facile : *1234motdepasse!*.
- Exemple d'un mot de passe difficile à deviner : *C_35t_Un3_B3ll3_Journé3*.

Transférer un fichier

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 cyberSanté 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 qui a été 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 le ou les fichiers.
- 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 (par exemple, au cas où des fichiers d'un employé ayant quitté l'organisation devraient être consultés).

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

Supprimer un fichier

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

Annexe B : Exemple de rapport d'incident

Rapport de gestion des atteintes à la confidentialité et des incidents de sécurité

Partie I – Description et signalement

1. Renseignements généraux

Résumé de l'incident ou de l'atteinte	
Nom de l'organisation	
Personne-ressource et coordonnées	

2. Renseignements sur l'incident ou l'atteinte

Date et heure du signalement de l'incident ou de l'atteinte	
Date et heure de la découverte de l'incident ou de l'atteinte	
Date et heure de l'incident ou de l'atteinte	
Lieu de l'incident ou de l'atteinte	
Nom et titre de la personne qui a découvert l'incident ou l'atteinte	
Façon dont l'atteinte ou l'incident ont été découverts	
Organisation(s) ou personne(s) touchées par l'incident ou l'atteinte (p. ex., employés ou fournisseurs de services)	

3. Type d'atteinte à la confidentialité ou d'incident de sécurité

Type d'incident ou d'atteinte à la confidentialité	Atteinte à la confidentialité Incident relatif à la protection de la vie privée	☐ Oui ☐ Non ☐ Oui ☐ Non ☐ S.O.
	☐ Violation d'une politique ☐ Collecte non autorisée ☐ Utilisation non autorisée ☐ Suppression non autorisée ☐ Autres renseignements	☐ Violation d'une entente ☐ Divulgation non autorisée

4. Supports touchés

Veuillez indiquer le support touché par l'atteinte ou l'incident (p. ex., serveur, périphérique USB ou application des DSE) et son emplacement (p. ex., service de TI ou emplacement externe)	

5. Renseignements touchés

Veuillez indiquer le type de renseignements touchés par l'incident ou l'atteinte	Type de données (p. ex., renseignements personnels ou renseignements personnels sur la santé)	Exemple de données (p. ex., nom, renseignements sur la carte Santé, NAS ou renseignements sur un diagnostic)	Format de données
			☐ Données cryptées ☐ Données identificatoires ☐ Données anonymes ☐ Données statistiques ☐ Données regroupées

Partie II – Mesures d'atténuation

6. Mesures d'atténuation de l'incident ou de l'atteinte

Veuillez décrire les mesures prises pour atténuer l'incident ou l'atteinte (p. ex., récupération des renseignements, fermeture du système informatique ou remplacement des dispositifs de verrouillage)	Date et heure	Activités

Partie III – Signalement

7. Personnes et organisations avisées

Veuillez indiquer les personnes et les organisations avisées	Nom de l'organisation	Date et heure	Activités

8. Communications internes

Veuillez indiquer les personnes et services avisés de l'atteinte à la confidentialité ou de l'incident de sécurité	Nom et titre de la personne, ou nom du service	Date et heure	Activités

Partie IV – Enquête

9. Enquête sur l'atteinte

Résumé de l'enquête	
Résultat de l'enquête	
Cause de l'atteinte	
Nombre approximatif de personnes touchées (p. ex., patients, employés et intervenants externes)	
Préjudices potentiels de l'atteinte pour les personnes et l'organisation (p. ex., risques liés à la sécurité, vol d'identité, pertes financières ou atteinte à la réputation)	
Risques que l'atteinte se répète, ou que les renseignements soient davantage exposés	

Partie V – Atténuation et prévention

10. Veuillez indiquer les mesures d'atténuation appliquées pour éviter qu'un tel incident se reproduise.

Mesure d'atténuation	Date	Propriétaire	État d'avancement	Date de fin
Les recommandations et les mesures sont indiquées dans le document en pièce jointe.				AAAA/MM/JJ

Achèvement et approbation du rapport

Rapport préparé par :	Date //
Rapport examiné par :	Date AAAA/MM/JJ
Rapport approuvé par : Cliquer ici pour entrer du texte.	Date AAAA/MM/JJ

Annexe C : Glossaire

Acronyme	Description
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