

Guide de soutien de cyberSanté Ontario

Service commun d'imagerie diagnostique

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

Version : 1,0

Propriétaire du document : Service commun d'imagerie diagnostique

Ensemble complet de procédures visant à aider les organismes de soins de santé à assurer la connexion de nouveaux utilisateurs et établissements au service commun d'imagerie diagnostique.

Table des matières

Introduction	4
1. Soutien	4
1.1 Communication avec le service de dépannage	4
1.1.1 Comment communiquer avec le service de dépannage de cyberSanté Ontario	4
1.1.2 Signaler un incident ou créer une demande de service	5
1.1.3 Liste de vérification pour accélérer le processus	6
1.1.4 Incidents, demandes de service et processus de réacheminement technique	6
1.1.5 Avancement de votre ticket d'incident	7
1.1.6 Satisfaction de la clientèle	7
1.2 Processus de soutien	8
1.2.1 Représentation de haut niveau du modèle de soutien lié au service commun d'ID	8
1.2.2 Responsabilités du service de dépannage de l'établissement du client et du groupe de soutien de l'interface de l'application	8
1.2.3 Quand devez-vous communiquer avec le service de dépannage de cyberSanté Ontario?	8
1.2.4 Quand le service de dépannage de cyberSanté Ontario communique-t-il avec vous?	9
1.2.5 Quand le bureau de la protection de la vie privée de cyberSanté Ontario communique-t-il avec vous?	9
1.2.6 Assurance de la qualité des données	9
2. Responsabilités opérationnelles liées aux données du service commun d'ID	10
3. Protection de la vie privée et sécurité	10
3.1 Consentement du patient	10
3.1.1 Gestion du consentement	10
3.1.2 Application des directives de consentement	11
3.1.3 Dérogation à une directive de consentement	12
3.2 Demandes d'accès	13
3.2.1 Demandes d'accès aux données du service commun d'ID présentées par des patients	13
3.2.2 Demandes d'accès aux journaux de vérification adressées aux fournisseurs de soins de santé	14
3.3 Demandes de correction	14
3.4 Demandes de renseignements et plaintes relatives à la protection de la vie privée	15
3.5 Questions posées par les fournisseurs de soins de santé et relatives à la protection de la vie privée	15
3.6 Gestion des atteintes et des infractions à la sécurité	16
3.7 Gestion des violations de la vie privée	16
3.8 Directives à l'intention des fournisseurs de soins de santé	17
3.9 Directives à l'intention des agents de protection de la vie privée	18
4. Soutien et utilisateurs	19
4.1 Inscription des utilisateurs au service	19
Annexe A : Procédure de transfert de fichiers sensibles par courriel	20

Annexe B : Modèle de formulaire de rapport d'incident	25
Annexe C : Lexique	31

Introduction

Ce guide de soutien est un document présentant les différents processus qui ont été créés pour aider les organismes de soins de santé à connecter de nouveaux utilisateurs et établissements au service commun d'imagerie diagnostique (ID). Il contient des renseignements sur le soutien et l'entretien ainsi que sur les procédures et obligations en matière de sécurité et de protection de la vie privée.

1. Soutien

cyberSanté Ontario aidera les organismes de soins de santé de différentes façons :

1.1 Communication avec le service de dépannage

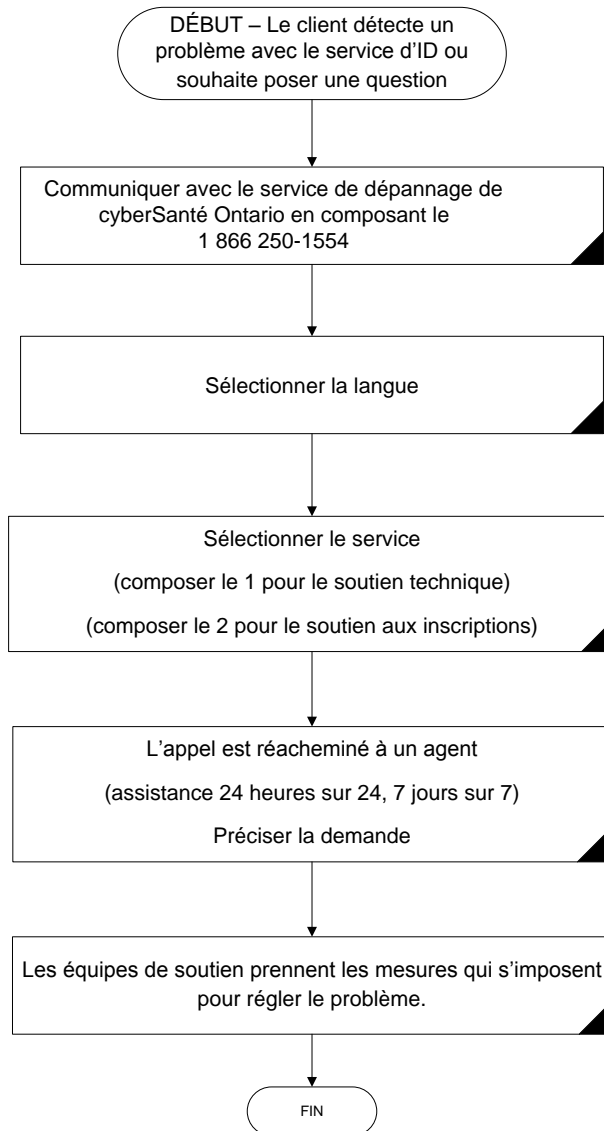
Le service de dépannage de cyberSanté Ontario est le point de contact unique pour ouvrir un ticket en cas de problème lié au service commun d'ID.

1.1.1 Comment communiquer avec le service de dépannage de cyberSanté Ontario

Voici les coordonnées du service de dépannage de cyberSanté Ontario :

<u>Coordonnées</u>	<p>Courriel* : servicedesk@ehealthontario.on.ca Téléphone* : 1 866 250-1554 Télécopieur : 416 586-4040 (Veuillez appeler le service de dépannage de cyberSanté Ontario si vous souhaitez envoyer une télécopie contenant des renseignements relatifs à un incident ou à une demande de service.)</p> <p><i>*Remarque : Le téléphone est le moyen privilégié de communication du service de dépannage de cyberSanté Ontario. À l'heure actuelle, il n'existe aucune entente de niveau de service pour les demandes de service ou les incidents ouverts par courriel.</i></p>
<u>Heures d'ouverture</u>	<p>Le service de dépannage reçoit les appels signalant un incident 24 heures sur 24, 7 jours sur 7, 365 jours par an.</p>

Processus de soutien pour la gestion des incidents



1.1.2 Signaler un incident ou créer une demande de service

Téléphone : Le moyen le plus rapide pour signaler un problème ou un incident présentant un risque élevé (p. ex., la production est interrompue ou l'environnement est gravement détérioré) est de communiquer avec le service de dépannage de cyberSanté Ontario par téléphone pour ouvrir un ticket d'incident ou de demande de service.

1 866 250-1554 – option 1

Courriel : Pour les demandes de service (problèmes présentant un risque faible ou modéré). Toutefois, à l'heure actuelle, il n'existe aucune entente de niveau de service pour les demandes de service ou les incidents ouverts par courriel.

servicedesk@ehealthontario.on.ca

1.1.3 Liste de vérification pour accélérer le processus

Soyez prêt à fournir les renseignements suivants :

- Votre nom;
- Le lieu de votre établissement;
- Vos coordonnées, ainsi que celles de personnes-ressources de remplacement, le cas échéant;
- L'environnement de service de cyberSanté Ontario touché (p. ex., production, essai, etc.);
- La description du problème, notamment la date et l'heure auxquelles il est survenu et le nombre d'utilisateurs touchés (si vous le connaissez);
- Les étapes nécessaires pour reproduire le problème et les mesures de diagnostic et de dépannage qui ont été prises.

1.1.4 Incidents, demandes de service et processus de réacheminement technique

Étape 1	Appelez cyberSanté Ontario au 1 866 250-1554 pour ouvrir un ticket.
Ouverture d'un ticket	Choisissez l'option « service de dépannage ».
Étape 2	Un agent du service de dépannage collabore avec vous pour définir le problème et entame la procédure de dépannage.
Communication avec l'équipe du service de dépannage de première ligne	Un agent du service de dépannage peut, au besoin, communiquer avec un responsable technique de cyberSanté Ontario. L'agent de soutien peut vous demander des renseignements supplémentaires pour faciliter le processus de dépannage. Une fois que toutes les mesures ont été prises, si l'agent du service de dépannage ne peut pas résoudre le problème, la demande est réacheminée à l'équipe de soutien de l'échelon suivant de cyberSanté Ontario.

Étape 3	L'incident est attribué à l'échelon de soutien suivant.
Réacheminement du problème à l'équipe de soutien de l'échelon suivant de cyberSanté Ontario	Un employé de l'échelon de soutien suivant prend contact avec vous. Il étudie l'incident et poursuit les activités de dépannage au besoin. D'autres équipes de soutien peuvent participer à la résolution du problème.

1.1.5 Avancement de votre ticket d'incident

Mises à jour : L'avancement de votre ticket est automatiquement mis à jour. Si vous souhaitez savoir où en est votre ticket d'incident, n'hésitez pas à communiquer avec le service de dépannage.

Priorité de la demande de service : Le niveau de priorité de l'incident est déterminé d'un commun accord entre l'agent de soutien et vous, le client.

Fermeture du ticket d'incident : Votre ticket d'incident sera fermé 15 jours après la résolution de l'incident, une fois que toutes les mesures de dépannage possible ont été prises, ou si vous autorisez l'équipe de soutien de cyberSanté Ontario à fermer le ticket. Si, après avoir tenté de communiquer avec vous par trois fois, le service de dépannage ne reçoit pas de nouvelles de votre part, il fermera le ticket. Vous recevrez trois rappels, et le dernier rappel vous indiquera que le ticket sera fermé le jour suivant.

1.1.6 Satisfaction de la clientèle

Le service de dépannage de cyberSanté Ontario accorde une grande importance à la satisfaction de la clientèle. Vos commentaires sont les bienvenus, et nous vous encourageons à exprimer votre avis de l'une des façons suivantes :

Sondage sur la satisfaction de la clientèle

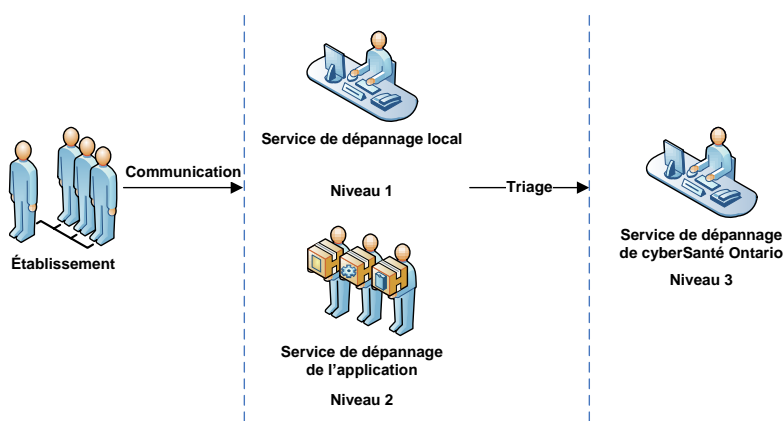
À la fermeture d'un ticket, cyberSanté Ontario sélectionne au hasard des incidents qui feront l'objet d'un sondage. Vous serez peut-être amené à remplir un questionnaire en ligne. En répondant à ce sondage, qui ne vous prendra que cinq minutes, vous contribuerez à améliorer la qualité de notre service, et nous vous en serions très reconnaissants.

Commentaires généraux

Si vous souhaitez nous faire part de vos commentaires ou de vos suggestions, veuillez nous envoyer un courriel à l'adresse servicedesk@ehealthontario.on.ca.

1.2 Processus de soutien

1.2.1 Représentation de haut niveau du modèle de soutien lié au service commun d'ID



1.2.2 Responsabilités du service de dépannage de l'établissement du client et du groupe de soutien de l'interface de l'application

Si un problème est détecté sur le plan de l'interface utilisée pour accéder aux données du service commun d'ID, le service de dépannage de votre établissement et les équipes de soutien de l'interface de l'application de votre établissement tentent de résoudre le problème :

- en menant des activités de dépannage;
- en trouvant une solution, lorsque cela est possible;
- en déterminant les répercussions potentielles du problème;
- en réacheminant le problème aux groupes de soutien concernés ou au service de dépannage de cyberSanté Ontario.

1.2.3 Quand devez-vous communiquer avec le service de dépannage de cyberSanté Ontario?

Communiquez avec le service de dépannage de cyberSanté Ontario si vous avez des questions ou des commentaires liés :

- à une demande d'assistance visant à résoudre un problème lié aux certificats d'infrastructure à clés publiques (ICP) du service commun d'ID;
- à une demande d'assistance visant à résoudre un problème d'interface lié au service;
- au signalement d'une erreur touchant l'application du service commun d'ID;
- au signalement de résultats manquants dans le service commun d'ID;
- au signalement d'un problème lié à la qualité des données du service commun d'ID;

- au signalement d'une violation de la vie privée.

Communiquez avec le service de dépannage de cyberSanté Ontario si vous souhaitez obtenir des renseignements sur le service commun d'ID au sujet :

- de la fonctionnalité du service commun d'ID;
- de la protection et de la sécurité des renseignements personnels sur la santé.

1.2.4 Quand le service de dépannage de cyberSanté Ontario communique-t-il avec vous?

- Pour obtenir des précisions sur un incident que vous avez signalé ou une demande que vous avez présentée;
- Pour vous informer que le site de cyberSanté Ontario fait l'objet d'activités d'entretien et que le service pourrait être touché;
- Pour signaler une défaillance liée à l'application du service commun d'ID;
- Pour vous informer des dates de diffusion et des travaux d'amélioration de l'application.

1.2.5 Quand le bureau de la protection de la vie privée de cyberSanté Ontario communique-t-il avec vous?

- Pour obtenir de plus amples renseignements pour donner suite à une demande d'accès au service commun d'ID;
- Pour faciliter la gestion des incidents.

1.2.6 Assurance de la qualité des données

Les établissements doivent effectuer des contrôles réguliers de la qualité des données pour s'assurer que les données transmises au service commun d'ID sont exactes et exhaustives. cyberSanté Ontario accorde une grande importance à l'exactitude des données figurant dans le service commun d'ID. Si vous vous apercevez qu'il manque des résultats ou que certaines données sont incorrectes, veuillez nous le signaler en communiquant avec le service de dépannage.

Vous devez nous indiquer les renseignements suivants pour faciliter le processus d'enquête :

- Vos coordonnées (numéro de téléphone, adresse de courriel);
- Le nom de votre organisme ou de l'organisme au nom duquel vous signalez le problème (cabinet de médecin, hôpital, service);
- Le nom de l'organisme qui a soumis le résultat;
- Le numéro d'entrée du résultat dans le service commun d'ID;
- L'information manquante (si vous signalez uniquement un résultat manquant);
- Les raisons pour lesquelles vous estimez que le résultat est incorrect, le cas échéant.

2. Responsabilités opérationnelles liées aux données du service commun d'ID

En vertu de la Loi de 2004 sur la protection des renseignements personnels sur la santé (LPRPS), il incombe à cyberSanté Ontario de tenir un registre électronique de tous les accès aux données du service commun d'ID dans un système appartenant à l'organisme ou à un tiers. Pour ce faire, cyberSanté Ontario doit avoir accès aux journaux de vérification. cyberSanté Ontario peut aussi être invité à fournir un rapport de vérification sur ces registres d'accès.

3. Protection de la vie privée et sécurité

3.1 Consentement du patient

Conseil

Dans le système de DSE, les patients, ou leur mandataire spécial, peuvent choisir d'autoriser ou de restreindre l'accès à leurs données. Si un patient souhaite faire émettre une directive de consentement dans le service commun d'ID, il doit remplir le formulaire de consentement qui se trouve à l'adresse <http://www.ehealthontario.on.ca/fr/initiatives/resources> et le transmettre à cyberSanté Ontario. Un fournisseur peut aider le patient à remplir le formulaire et le transmettre à cyberSanté Ontario en son nom.

3.1.1 Gestion du consentement

Le système de dossiers de santé électroniques (DSE) permet aux patients, ou à leur mandataire spécial, d'autoriser ou de restreindre l'accès à leurs données au sein du service commun d'ID. Si un patient restreint l'accès à ses données en appliquant une directive de consentement, les fournisseurs qui utiliseront le service commun d'ID ne seront pas en mesure de consulter les renseignements d'un patient pour lesquels ce dernier aura émis une directive sur le consentement.

On peut rédiger, modifier ou supprimer une directive de consentement qui restreint ou qui autorise l'accès aux données suivantes :

- Tous les dossiers d'un patient (directive globale sur le consentement/directive sur le consentement visant un domaine);¹
- Un rapport en particulier (directive sur le consentement visant les dossiers);
- Tous les dossiers d'un organisme particulier (directive sur le consentement visant les mandataires – DRS).

3.1.2 Application des directives de consentement

Si un patient communique avec un dépositaire de renseignements sur la santé (DRS) pour faire restreindre ou rétablir l'accès à ses renseignements personnels, le DRS doit :

- inscrire l'information relative à la directive de consentement sur le formulaire de consentement relatif aux DSE qui se trouve à l'adresse <http://www.ehealthontario.on.ca/fr/initiatives/resources>;
- transmettre ce formulaire à cyberSanté Ontario par télécopie au 416 586-4397 ou au 1 866 831-0107.

cyberSanté Ontario informera le DRS que la demande a été traitée. Le DRS doit ensuite informer le patient que sa directive de consentement a bien été soumise.

Si un patient souhaite faire émettre une directive de consentement relative à des dossiers sur lesquels a travaillé plus d'un DRS, ou rétablir l'accès à ces dossiers, il doit remplir le formulaire de consentement relatif aux DSE qui se trouve à l'adresse <http://www.ehealthontario.on.ca/fr/initiatives/resources>, ou communiquer directement avec cyberSanté Ontario en appelant le 416 946-4767.

Dans tous les cas, cyberSanté Ontario appliquera les directives de consentement dans un délai de sept jours après avoir vérifié l'identité du patient qui présente la demande. La partie recevant la demande de directive de consentement informe ensuite le patient que sa demande a été traitée. Si vous ne pouvez pas informer le patient, cyberSanté Ontario se chargera de le faire en votre nom et selon vos instructions.

¹ La directive sur le consentement visant un domaine permet à une personne de maintenir ou de retirer son consentement sur l'accès à un dépôt de DSE, mais pas à tous les dépôts de DSE. À l'heure actuelle, il n'existe qu'un seul dépôt de DSE; par conséquent la directive sur le consentement visant un domaine et la directive globale sur le consentement auront le même effet jusqu'à ce que de nouveaux dépôts soient ajoutés.

3.1.3 Dérogation à une directive de consentement²

Conseil

Le service commun d'ID permet à un fournisseur de soins de santé de suspendre provisoirement l'application d'une directive de consentement émise par un patient. Si vous mettez en place une dérogation au consentement, cyberSanté Ontario vous demandera de confirmer l'objectif de cette dérogation, et d'en informer le patient. Une dérogation peut avoir lieu dans deux cas : si le patient a accordé son consentement exprès, ou si la dérogation vise à réduire un risque de lésions corporelles pour le patient ou pour d'autres personnes. Une dérogation à une directive de consentement est en vigueur pour une durée de quatre heures.

Dans des cas exceptionnels, le service commun d'ID permet à un fournisseur de soins de santé de suspendre provisoirement l'application d'une directive de consentement émise par un patient.

Un fournisseur peut obtenir une dérogation à une directive de consentement dans les circonstances suivantes :

- Il obtient l'autorisation expresse du patient ou de son mandataire spécial;
- Il a de bonnes raisons de considérer qu'il est nécessaire de suspendre l'application de la directive pour faire disparaître ou réduire les risques de blessure grave auxquels s'expose le patient concerné et il juge impossible d'obtenir le consentement de ce patient dans un délai raisonnable;
- Il a de bonnes raisons de considérer qu'il est nécessaire de suspendre l'application de la directive pour faire disparaître ou réduire les risques de blessure grave auxquels s'expose une personne autre que le patient concerné ou un groupe de personnes.

La dérogation temporaire et le nom du fournisseur de soins de santé l'ayant créée seront consignés dans le service commun d'ID. Elle sera en vigueur pour une durée maximale de quatre heures.

² Les fournisseurs qui accèdent au service commun d'ID au moyen de l'afficheur ClinicalConnect ne seront pas en mesure de mettre en place une dérogation à une directive de consentement jusqu'à ce que ClinicalConnect soit entièrement intégré à la solution de gestion du consentement.

cyberSanté Ontario en avisera le DRS quand un des agents de ce dernier aura créé une dérogation à une directive de consentement. Une fois informé par cyberSanté Ontario, il incombe au DRS :

1. de vérifier si la dérogation a été mise en place pour l'une des raisons susmentionnées;
2. d'en informer le patient le plus vite possible³.

Si une dérogation à une directive de consentement est appliquée pour faire disparaître ou réduire les risques de blessure grave auxquels s'expose une personne autre que le patient concerné ou un groupe de personnes, le DRS doit en aviser par écrit le Commissaire à l'information et à la protection de la vie privée/Ontario (CIPVP), et ce, dès que possible.

Pour ne rien oublier lorsque vous informez le CIPVP, lisez la *Politique de gestion du consentement – DSE* à l'adresse <http://www.ehealthontario.on.ca/fr/initiatives/resources>.

3.2 Demandes d'accès

Conseil

Si un patient souhaite consulter ou corriger des données qui ont été créées par votre cabinet, suivez vos procédures internes d'autorisation d'accès ou de correction des données. Consignez la demande du patient.

Si un patient souhaite consulter ou corriger des données qui ont été créées par d'autres DRS, invitez-le à communiquer dès que possible avec cyberSanté Ontario par téléphone au 416 946-4767 pour qu'il puisse présenter sa demande.

3.2.1 Demandes d'accès aux données du service commun d'ID présentées par des patients

En vertu de la LPRPS, un patient ou son mandataire spécial a le droit d'accéder aux données détenues par un DRS. Lorsqu'un fournisseur reçoit une demande relative à des dossiers qu'il a compilés, créés ou auxquels il a contribué, il doit se conformer aux dispositions de la partie V de la LPRPS, ainsi qu'à ses politiques, procédures et pratiques internes avant de répondre à la demande.

³ Pour ne rien oublier lorsque vous informez le patient, lisez la *Politique de gestion du consentement – DSE* à l'adresse <http://www.ehealthontario.on.ca/fr/initiatives/resources>. Si vous ne pouvez pas informer le patient, communiquez avec cyberSanté Ontario qui se chargera de le faire en votre nom.

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

- informer la personne que sa demande d'accès concerne des renseignements personnels sur la santé (RPS) qui ne sont pas en sa possession ou de sa responsabilité;
- inviter la personne à communiquer avec cyberSanté Ontario par téléphone au 1 866 250-1554 ou en ligne à l'adresse <http://www.ehealthontario.on.ca/fr/contact>.

En vertu de la *Politique sur l'accès aux renseignements et la rectification des renseignements – DSE* qui se trouve à l'adresse <http://www.ehealthontario.on.ca/fr/initiatives/resources>, cyberSanté Ontario peut demander l'aide du DRS pour répondre directement à une demande d'accès.

3.2.2 Demandes d'accès aux journaux de vérification adressées aux fournisseurs de soins de santé

Lorsqu'une personne adresse directement à un fournisseur de soins une demande d'accès aux journaux de vérification des dossiers stockés dans le service commun d'ID, le DRS doit :

- aviser la personne qu'il se trouve dans l'impossibilité de traiter sa demande d'accès;
- inviter la personne à communiquer avec cyberSanté Ontario par téléphone au 1 866 250-1554 ou en ligne à l'adresse <http://www.ehealthontario.on.ca/fr/contact>.

3.3 Demandes de correction

Lorsqu'une personne adresse directement à un DRS une demande de correction de dossiers médicaux qu'il a à lui seul créés ou auxquels il est le seul à avoir contribué dans le service commun d'ID, le DRS doit se conformer aux dispositions de la partie V de la LPRPS, ainsi qu'à ses politiques, procédures et pratiques internes.

À la demande du patient, lorsqu'une demande de correction est satisfaite, le DRS doit en informer cyberSanté Ontario et demander à obtenir un rapport de vérification d'accès au dossier du patient, dans le cas où ce dernier souhaite informer les autres DRS qui pourraient avoir eu accès à son dossier. Le DRS doit ensuite informer les établissements concernés au sujet de la correction apportée.

Lorsqu'une personne adresse directement à un DRS une demande de correction de dossiers qui ont été créés par un ou plusieurs autres DRS, le DRS doit effectuer ce qui suit dans les deux jours qui suivent la réception de la demande :

- Informer la personne que sa demande d'accès concerne des renseignements personnels sur la santé qui ne sont pas en sa possession ou de sa responsabilité;
- Inviter la personne à communiquer avec cyberSanté Ontario par téléphone au 1 866 250-1554 ou en ligne à l'adresse <http://www.ehealthontario.on.ca/fr/contact>.

cyberSanté Ontario coordonne la réponse à cette demande et, pour ce faire, peut demander l'aide du ou des DRS.

3.4 Demandes de renseignements et plaintes relatives à la protection de la vie privée

Conseil

Lorsqu'une personne soumet une demande de renseignements ou une plainte en lien avec le service commun d'ID, invitez-la à communiquer avec cyberSanté Ontario.

Lorsqu'un DRS reçoit directement une demande de renseignements ou une plainte qui concerne uniquement les dossiers du DRS dans le service commun d'ID, ou ses agents et fournisseurs de service, le DRS est tenu d'y répondre dans le respect de ses propres politiques, procédures et pratiques internes.

Lorsqu'un DRS reçoit directement une demande de renseignements ou une plainte qui concerne uniquement le service commun d'ID ou les agents ou fournisseurs de services électroniques de cyberSanté Ontario, et qu'il se trouve dans l'impossibilité de traiter cette demande ou cette plainte, il doit immédiatement :

- informer la personne que le DRS n'est pas en mesure de répondre à la demande de renseignements ou à la plainte;
- inviter la personne à communiquer avec cyberSanté Ontario par téléphone au 1 866 250-1554 ou en ligne à l'adresse <http://www.ehealthontario.on.ca/fr/contact>.

cyberSanté Ontario peut demander l'aide du ou des DRS pour répondre à une demande de renseignements ou à une plainte qui lui est directement adressée.

3.5 Questions posées par les fournisseurs de soins de santé et relatives à la protection de la vie privée

Pour toute question de la part d'un fournisseur de soins de santé concernant les processus relatifs à la protection de la vie privée mentionnés ci-dessus, y compris la manière de traiter les demandes d'accès des personnes à leurs renseignements, de s'acquitter de ses obligations relatives à l'obtention du consentement ou de gérer les atteintes ou les infractions, celui-ci doit communiquer avec cyberSanté Ontario au 1 866 250-1554.

Lorsque vous envoyez des courriels à cyberSanté Ontario, assurez-vous de ne mentionner aucun renseignement personnel ni aucun RPS.

3.6 Gestion des atteintes et des infractions à la sécurité

La présente section énonce des directives destinées aux DRS lorsqu'ils doivent signaler à cyberSanté Ontario toute atteinte ou infraction à la sécurité (définie ci-dessus).

Une atteinte à la sécurité est une situation indésirable ou inattendue qui entraîne :

- le non-respect des politiques, des procédures, des pratiques ou des exigences en matière de sécurité de l'organisme;
- l'accès, l'utilisation ou la recherche non autorisée de ressources documentaires;
- la communication, la destruction, la modification ou la conservation non autorisée de renseignements;
- une infraction aux accords conclus entre cyberSanté Ontario et votre organisme ou bien les utilisateurs, les employés, les agents ou les fournisseurs de services de votre organisme;
- une tentative d'atteinte à la sécurité soupçonnée ou réelle;
- la dégradation, la fraude, l'abus, le vol, la perte ou la détérioration des ressources.

Le processus de gestion des atteintes et des infractions à la sécurité ne s'applique pas au traitement des incidents internes au DRS ni à tout DRS, à leurs agents ou à leurs fournisseurs de services électroniques qui ne consultent pas les RPS du service commun d'ID et n'y contribuent pas.

3.7 Gestion des violations de la vie privée

Conseil

En cas de violation réelle ou soupçonnée de la vie privée, le DRS doit en référer à cyberSanté Ontario en appelant le service de dépannage ouvert en tout temps au 1 866 250-1554.

La *Politique de gestion des atteintes à la confidentialité – DSE* qui se trouve à l'adresse http://www.ehealthontario.on.ca/fr/initiatives/resources_décrit en détail les étapes à suivre en cas d'incident ou de violation touchant la protection de la vie privée.

En cas de violation réelle ou soupçonnée de la vie privée, le DRS doit en référer à cyberSanté Ontario en appelant le service de dépannage ouvert au 1 866 250-1554 avant la fin du jour ouvrable suivant. Un DRS est tenu d'informer cyberSanté Ontario lorsqu'il a connaissance d'une violation réelle ou soupçonnée de la vie privée causée directement ou indirectement :

- par un autre DRS ou bien par un agent ou un fournisseur de services électroniques d'un autre DRS;
- par plusieurs DRS ou bien par des agents ou des fournisseurs de services électroniques de plusieurs DRS;
- par cyberSanté Ontario ou bien par un agent ou un fournisseur de services électroniques de cyberSanté Ontario;
- par toute autre personne non habilitée qui n'est ni un agent ni un fournisseur de services électroniques de cyberSanté Ontario ou de tout autre DRS.

En cas d'infraction imputable à un DRS qui a créé les renseignements personnels sur la santé dans le service commun d'ID ou qui est le seul à y avoir contribué, le DRS est tenu de respecter ses politiques, procédures et pratiques internes pour en référer dès que possible et conformément à la LPRPS à la personne ou aux personnes concernées par ces renseignements personnels sur la santé et de mettre un terme à cette violation, d'enquêter sur cette violation et d'y remédier.

En cas d'infraction imputable uniquement à un DRS qui n'a pas à lui seul créé les RPS dans le service commun d'ID ou qui n'y a pas contribué à lui seul, le DRS, en collaboration avec les autres DRS qui ont créé les données et cyberSanté Ontario devront nommer les personnes qui seront chargées d'effectuer une enquête. Les rôles spécifiquement attribués à chacune des parties concernées par une violation de ce type figurent dans la Politique de gestion des atteintes à la confidentialité – DSE, à l'adresse <http://www.ehealthontario.on.ca/fr/initiatives/resources>.

3.8 Directives à l'intention des fournisseurs de soins de santé

Si vous avez connaissance d'une atteinte ou d'une infraction réelle ou soupçonnée à la sécurité du service commun d'ID ou à ses données, commise par vous ou par vos employés, agents ou fournisseurs de services, vous devez la signaler immédiatement à votre bureau de la protection de la vie privée. Si vous n'avez pas de bureau de la protection de la vie privée ou que vous n'êtes pas en mesure de communiquer avec lui ou avec votre équipe de soutien pour signaler une infraction, appelez le service de dépannage au 1 866 250-1554 et ouvrez un ticket d'incident de sécurité. Vous êtes tenu de collaborer à toute activité visant à mettre un terme à une atteinte ou à une infraction ou à réaliser une enquête sur une telle atteinte ou infraction.

Pendant l'enquête, vous pourriez être tenu de fournir des renseignements supplémentaires, ce qui pourrait inclure des renseignements personnels ou des RPS pour mettre un terme ou remédier à l'atteinte ou à l'infraction.

Important : Lorsque vous signalez une atteinte ou une infraction à la sécurité au service de dépannage, vous ne devez en aucun cas divulguer de renseignements personnels sur les patients et sur leur santé.

3.9 Directives à l'intention des agents de protection de la vie privée

Si vous avez connaissance d'une atteinte ou d'une infraction réelle ou soupçonnée au service commun d'ID ou à ses données, commise par un membre du personnel de votre organisme, y compris vos employés, vos agents ou vos fournisseurs de services, vous devez la signaler immédiatement au service de dépannage par téléphone au 1 866 250-1554 et ouvrir un ticket d'incident de sécurité.

Important : Lorsque vous signalez une atteinte ou une infraction à la sécurité au service de dépannage, vous ne devez en aucun cas divulguer de renseignements personnels sur les patients et sur leur santé. Vous devez collaborer à toute enquête entreprise par cyberSanté Ontario sur toute atteinte ou infraction à la sécurité des données.

Veillez fournir les renseignements suivants lorsque vous signalez une atteinte à la sécurité soupçonnée ou réelle :

1. L'heure et la date de l'incident en question;
2. Le nom et les coordonnées de l'agent ou du fournisseur de services électroniques qui a signalé l'incident;
3. Des renseignements à propos de l'incident (p. ex., le type d'incident et la manière dont il a été détecté);
4. La ou les conséquences de l'incident;
5. Les mesures prises pour confiner l'incident, que ce soit par l'agent ou par le fournisseur de services électroniques qui a signalé l'incident, ou les services touchés le cas échéant.

Lorsqu'un appel aura été inscrit au service de dépannage, l'équipe chargée de la gestion des incidents sera mobilisée pour régler la situation. Un plan de résolution sera élaboré en collaboration avec le demandeur.

4. Soutien et utilisateurs

4.1 Inscription des utilisateurs au service

Les utilisateurs du service commun d'ID peuvent accéder aux données au moyen de différentes interfaces. Pour certains établissements, l'accès aux interfaces est géré localement, y compris l'attribution d'identifiants de connexion aux utilisateurs. Les utilisateurs de l'afficheur Web doivent disposer d'un identifiant ONE^{MD} ID. Pour obtenir votre identifiant ONE ID, communiquez avec autorité d'enregistrement locale pour remplir un formulaire d'inscription.

Annexe A : Procédure de transfert de fichiers sensibles par courriel

Tour d'horizon

Les politiques de cyberSanté Ontario exigent l'application de mesures de précautions lors du transfert ou de la sauvegarde de documents sensibles au moyen de canaux de communication qui ne sont pas considérés comme sécurisés, tels que les courriels, les CD, les DVD, les clés USB et les cartes mémoire flash.

Le présent document décrit la procédure à suivre pour protéger les fichiers et les rapports sensibles à l'aide de WinZip, une application offerte sur le marché qui peut être utilisée à la fois pour réduire la taille d'un document et pour le protéger.

L'outil de chiffrement décrit dans le présent document est un système de chiffrement à mot de passe. La protection conférée par le chiffrement peut être supprimée si le mot de passe correspondant est compromis. Par conséquent, quiconque utilise cet outil et intervient dans le processus de chiffrement des fichiers est tenu de respecter les lignes directrices relatives à la protection par mot de passe qui figurent dans la section « Communication des mots de passe ».

Utilisations autorisées

Cette procédure peut être utilisée pour chaque transfert de données sensibles par courriel, notamment de documents contenant des renseignements personnels ou des RPS, dans le cadre des processus opérationnels réguliers.

Si l'envoi de renseignements sensibles par courriel non sécurisé constitue un processus opérationnel courant, il faudrait envisager d'automatiser la procédure et d'utiliser un mécanisme d'entreprise pour transférer cette information en toute sécurité.

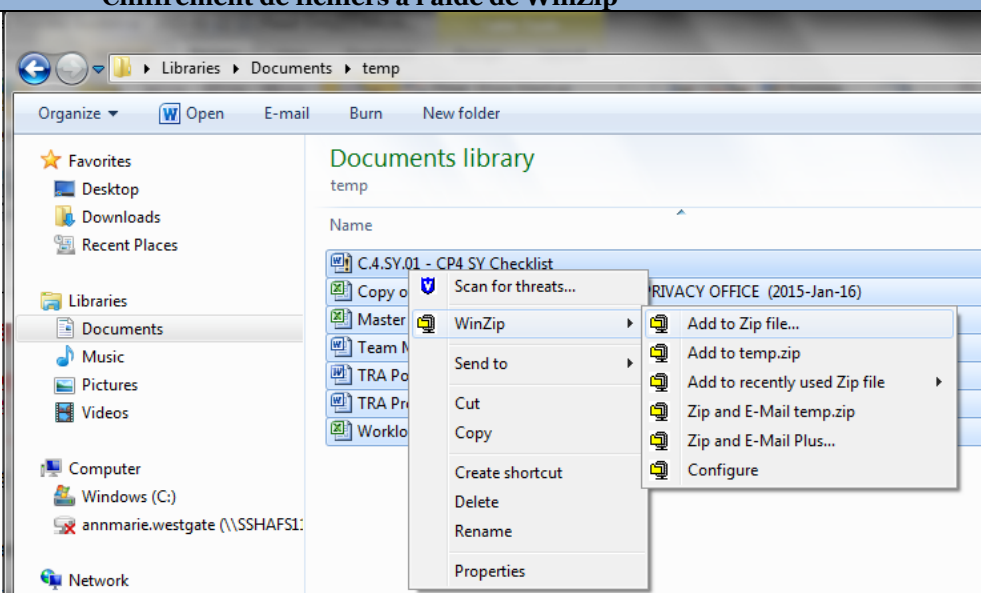
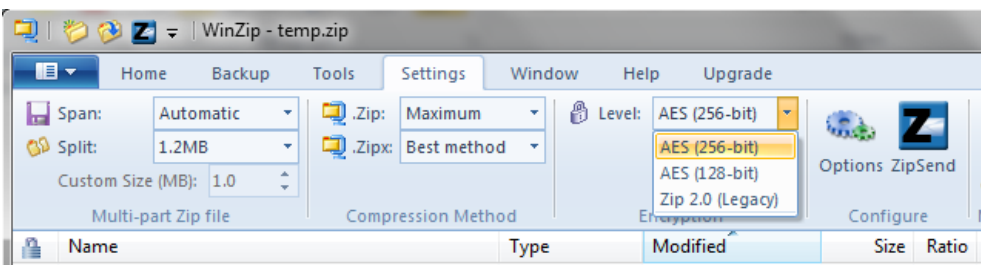
Les pièces jointes transférées par courriel à cyberSanté Ontario ne peuvent dépasser 10 Mo par courriel.

Pour en savoir plus, communiquez avec le service de dépannage de cyberSanté Ontario au 1 866 250-1554.

Instructions pour le chiffrement des fichiers et la création de mots de passe

Utilisation du logiciel de chiffrement WinZip

Comme outil de chiffrement, cyberSanté Ontario recommande les éditions **WinZip 16.0** Standard.

Chiffrement de fichiers à l'aide de WinZip	
<p>Étape 1. Créez une archive : Ouvrez l'emplacement des fichiers.</p> <p>Accédez au dossier où se trouvent les fichiers. À l'aide de la souris, sélectionnez les fichiers que vous souhaitez compresser. Dans la boîte de dialogue qui apparaît, passez votre souris sur WinZip et sélectionnez Ajouter au fichier Zip... (Add to Zip file)</p> <p>Choisissez un nom de fichier.</p>	 <p style="text-align: center;">Étape 1. Ajoutez des fichiers à l'archive</p>
<p>Étape 2. Ouvrez l'archive : Double-cliquez sur le fichier Zip pour ouvrir l'archive.</p> <p>Étape 3. Choisissez un système de chiffrement plus sécurisé Utilisez un chiffrement AES de 256 bits. Dans l'onglet Paramètres (Settings), vérifiez que le niveau de chiffrement sélectionné est AES (256 bits).</p>	 <p style="text-align: center;">Étape 3. Choisissez un système de chiffrement</p>

Chiffrement de fichiers à l'aide de WinZip

Étape 4. Procédez au chiffrement du fichier entier

À partir du menu Outils (Tools), cliquez sur **Chiffrer le fichier Zip** (Encrypt Zip File).



Étape 4. Procédez au chiffrement du fichier entier

Étape 5. Créez un mot de passe fiable

Saisissez un mot de passe et confirmez-le.

Consultez la section **Error! Reference source not found.** ci-dessous pour savoir comment créer un mot de passe fiable.



Étape 5 Créez un mot de passe fiable

Le fichier doit être chiffré et protégé par mot de passe avant que l'expéditeur ne l'envoie au destinataire en pièce jointe d'un courriel.

WinZip, le logiciel décrit dans le présent document, utilise le système de chiffrement symétrique, qui nécessite l'échange d'un mot de passe commun. En d'autres termes, l'expéditeur du fichier chiffré doit communiquer le mot de passe au destinataire du fichier. WinZip ne permet pas de récupérer les fichiers d'une archive chiffrée en cas d'oubli du mot de passe. La création et le partage des mots de passe requièrent donc une attention particulière.

Transfert de fichier et communication du mot de passe

Une fois le fichier chiffré et protégé par mot de passe, il est sauvegardé temporairement sur le partage réseau ou sur le disque dur local. Le mot de passe devrait être communiqué par téléphone au destinataire du fichier ou au moyen d'une méthode « hors bande » (si le document est envoyé par courriel, transmettre le mot de passe par téléphone, télécopie ou courrier). Autrement dit, le mot de passe ne doit pas être transmis en même temps ni de la même façon que le fichier chiffré.

Les exigences suivantes s'appliquent à la gestion des mots de passe :

Création du mot de passe

- Créez un mot de passe fiable pour protéger les fichiers chiffrés.
- Créez et utilisez un mot de passe différent pour chaque archive WinZip.
- Utilisez au moins 8 caractères.
- Le mot de passe doit contenir des caractères appartenant à au moins trois des quatre catégories suivantes : lettres majuscules (A-Z), lettres minuscules (a-z), caractères numériques (0-9) et caractères spéciaux (p. ex. : !, \$, #, _, ~, %, ^).
- Exemple de mauvais choix de mot de passe : *1234Motdepasse!*
- Exemple de bon choix de mot de passe : *iL_fAiT_bEaU22*

Transfert de fichier

Une fois le mot de passe créé, l'expéditeur peut envoyer le fichier par courriel, en prenant soin de ne pas se tromper de destinataire. Lorsque ce dernier reçoit le courriel, il téléphone à l'expéditeur pour connaître le mot de passe.

Communication des mots de passe

La communication de mots de passe entre un DRS et cyberSanté Ontario doit se faire de manière sécurisée.

La procédure est la suivante :

- L'expéditeur détermine qui est le destinataire autorisé de l'information.
- Il met le fichier chiffré à la disposition du destinataire en suivant le processus convenu (SFTP, courriel, etc.).

- Le destinataire appelle l'expéditeur.
- L'expéditeur vérifie oralement l'identité du destinataire :
 - Nom;
 - Titre, unité opérationnelle, organisme;
 - Nom du fichier chiffré reçu ou récupéré.
- L'expéditeur indique à l'oral le mot de passe au destinataire pour qu'il puisse ouvrir le fichier chiffré.
- Le destinataire confirme oralement à l'expéditeur qu'il est parvenu à extraire le(s) fichier(s).
- L'expéditeur détruit de manière sécurisée la copie manuscrite du mot de passe, le cas échéant, et supprime tous les exemplaires du fichier sur les disques locaux ou réseaux.

Récupération des mots de passe

WinZip ne permet pas la récupération des mots de passe. Par conséquent, pour le stockage à long terme des fichiers chiffrés, il faut disposer d'une méthode de récupération des mots de passe. Ainsi, si un employé quitte son emploi et qu'il faut accéder à ses fichiers, cette méthode permettra d'y parvenir.

Pour ce faire, on peut par exemple conserver le mot de passe dans une enveloppe scellée à laquelle seule la haute direction pourra avoir accès, et uniquement dans le but de récupérer le mot de passe.

Suppression des fichiers

Une fois un fichier déchiffré et utilisé, il doit être supprimé par l'expéditeur et par le destinataire.

Annexe B : Modèle de formulaire de rapport d'incident

Rapport d'incident ou d'infraction en lien avec la sécurité ou la vie privée

Partie I : Détermination et signalement de l'incident ou de l'infraction

1. Contexte

Résumé de l'incident ou de l'infraction	
Nom de l'organisme signalant l'incident ou l'infraction	
Point de contact et coordonnées	

2. Précisions sur l'incident ou l'infraction

Date et heure du signalement de l'incident ou de l'infraction	
Date et heure de la découverte de l'incident ou de l'infraction	
Date et heure de l'apparition de l'incident ou de l'infraction	
Lieu de l'incident ou de l'infraction	
Nom et titre de la personne qui a découvert l'incident ou	

l'infraction	
Circonstances de la découverte de l'incident ou de l'infraction	
Organismes et personnes concernés par l'incident ou l'infraction (p. ex., employés, fournisseurs de services)	

3. Type d'infraction en lien avec la vie privée ou la sécurité

Type d'incident ou d'infraction en lien avec la vie privée?	Infraction en lien avec la vie privée <input type="checkbox"/> Oui <input type="checkbox"/> Non Incident en liant avec la vie privée <input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> S.O.
	<input type="checkbox"/> Infraction à une politique <input type="checkbox"/> Infraction à une entente <input type="checkbox"/> Collecte non autorisée <input type="checkbox"/> Utilisation non autorisée <input type="checkbox"/> Divulgateion non autorisée <input type="checkbox"/> Élimination non autorisée <input type="checkbox"/> Autres

4. Ressources d'information concernées

Veuillez indiquer les ressources d'information concernées par l'infraction (serveur, périphérique USB, application de DSE, etc.),	
---	--

ainsi que leur emplacement (service des TI, site distant, etc.).	
--	--

5. Information concernée

Veuillez indiquer le type d'information concerné par l'incident ou l'infraction.	Type de données (p. ex., renseignements personnels, renseignements personnels sur la santé)	Exemple d'éléments de données (p. ex., nom, renseignements de la carte Santé, données diagnostiques)	Format des données
			<input type="checkbox"/> Chiffrées <input type="checkbox"/> Identifiables <input type="checkbox"/> Anonymisées <input type="checkbox"/> Statistiques <input type="checkbox"/> Cumulatives

Partie II : Limitation de l'incident ou de l'infraction

6. Limitation de l'incident ou de l'infraction

Veuillez décrire les mesures qui ont été prises immédiatement pour maîtriser l'étendue de l'incident ou de l'infraction (p. ex., récupération de	Date et heure	Activités

l'information, arrêt du système informatique, changement des serrures).		

Partie III : Communication d'un avis

9. Personnes et organismes avertis

Veuillez indiquer quels sont les personnes et les organismes qui ont été informés de l'incident ou de l'infraction.	Nom de l'organisme	Date et heure	Activités

Communications internes

Veuillez indiquer quels sont les personnes et les services qui ont été informés de l'incident ou de l'infraction en lien avec la sécurité ou la vie privée.	Nom et titre de la personne/Nom du service	Date et heure	Activités

Partie IV : Enquête

11. Enquête au sujet de l'infraction

Résumé de l'enquête	
Résultat de l'enquête	
Cause fondamentale de l'infraction (le cas échéant)	
Estimation du nombre de personnes touchées (p. ex., patients, employés, intervenants externes)	
Risque potentiel pour les personnes et l'organisme (p. ex., risque pour la sécurité, vol d'identité, perte financière, atteinte à la réputation)	
Risque d'exposition continue	

Partie V : Correction et prévention

12. Veuillez indiquer les mesures correctives qui permettraient d'éviter ce type d'incidents à l'avenir.

Mesure corrective proposée	Date prévue	Propriétaire	Avancement	Date d'achèvement
Les mesures proposées figurent dans le document ci-joint.				JJ/MM/AAAA

Production et approbation du rapport

Rapport produit par :	Date 10/07/2013
Rapport révisé par :	Date JJ/MM/AAAA
Rapport approuvé par : Cliquez ici pour saisir du texte.	Date JJ/MM/AAAA

Annexe C : Lexique

Abréviations	Description
ID	Imagerie diagnostique
DRS	Dépositaire de renseignements sur la santé
RPS	Renseignements personnels sur la santé
RP	Renseignements personnels
LPRPS	Loi de 2004 sur la protection des renseignements personnels sur la santé

AVERTISSEMENT

Tous droits réservés. Aucune partie du présent document ne peut être reproduite, entreposée dans un système d'extraction ou transmise, sous n'importe quelle forme ou par n'importe quel moyen (électronique, mécanique, photocopie, enregistrement ou autre), sans la permission écrite préalable de cyberSanté Ontario.

Ni les personnes qui ont participé à la préparation de ce document ni cyberSanté Ontario ne garantissent l'exactitude ou l'actualité du contenu. Il est entendu que le ou les auteurs ou d'autres personnes engagées dans la création de ce document ne peuvent être tenus responsables de l'exactitude ou de l'actualité du contenu ou du résultat de toute mesure prise en fonction des renseignements fournis dans ce document, ou de toute erreur ou omission qu'il pourrait contenir. Aucun participant à la préparation de ce document n'essaie de fournir des conseils juridiques sur la confidentialité ou sur la sécurité ni d'autres conseils professionnels.