eHealth Ontario
www.ehealthontario.on.ca

Guide des fournisseurs de soins de santé

Service commun d'imagerie diagnostique

Version : 2.0

Ontario
eHealth Ontario

Généralités

Objet et portée

Le présent guide décrit les fonctions de l'application du service commun d'imagerie diagnostique (ID) et les avantages qu'elle procure à cyberSanté Ontario, ainsi que les procédures et obligations en matière de sécurité et de protection de la vie privée auxquelles les fournisseurs et les organismes de soins de santé doivent se conformer.

Destinataires du document

Les principaux destinataires de ce document sont les fournisseurs et les organismes de soins de santé de l'ensemble de l'Ontario qui utilisent notre application du service commun d'ID pour accéder aux résultats des patients.

Documents connexes

Ce guide sur le service d'ID doit être lu parallèlement aux documents suivants :

- Politique d'utilisation acceptable
- Guide de référence à l'intention des personnes inscrites à ONE ID (en anglais)
- Politique sur la protection des renseignements personnels sur la santé
- Politique de sécurité de l'information
- Politique d'utilisation acceptable des données et des technologies de l'information
- *Loi de 2004 sur la protection des renseignements personnels sur la santé*

De plus, les politiques suivantes sur la protection de la vie privée sont disponibles sur la page http://www.ehealthontario.on.ca/fr/initiatives/resources

- 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
- lisez la Politique de gestion des atteintes à la confidentialité – Dossier de santé électronique
- Politique de conservation – Dossier de santé électronique

Lexique

Terme	Définition
DPC	Déclaration de pratiques de certification
ID	Imagerie diagnostique
d-ID régional	Dépôt d'imagerie diagnostique régional
DSE	Dossier de santé électronique
STIUN	Système de transfert d'images pour les urgences neurochirurgicales
DRS	Dépositaire de renseignements sur la santé
NS	Numéro de (carte) Santé
ESA	Établissements de santé autonomes
ONE® ID	Ensemble de systèmes et de processus pour l'attribution et la gestion des identités électroniques permettant un accès sécurisé aux services de cyberSanté Ontario
RPS	Renseignements personnels sur la santé
LPRPS	*Loi de 2004 sur la protection des renseignements personnels sur la santé*
RP	Renseignements personnels
AE	Autorité d'enregistrement

Description du service

Aperçu

Le service commun d'imagerie diagnostique (ID) est une initiative qui vise le partage et la consultation des résultats des patients par les fournisseurs de soins des établissements hospitaliers et communautaires de l'ensemble de l'Ontario.

Le service commun d'ID présente des renseignements importants qui permettent aux fournisseurs autorisés de prendre des décisions plus éclairées quant au traitement des patients. Avant la mise en place du service commun d'ID, les fournisseurs autorisés ne pouvaient partager des images et des rapports de manière sécuritaire avec d'autres fournisseurs que par l'entremise de leurs dépôts d'imagerie diagnostique régionaux respectifs. La première phase de la mise en place du service commun d'ID rend dès maintenant possible, à l'échelle de la province, le partage des rapports diagnostiques; les prochaines versions permettront le partage d'autres types de renseignements associés à imagerie diagnostique, notamment des images. Les images diagnostiques et les rapports qui s'y rattachent sont stockés dans des dépôts qui en permettent l'extraction en format numérique. Les cliniciens ont donc un accès plus rapide aux renseignements; l'établissement des diagnostics s'en trouve alors accéléré.

Le programme d'ID présente des renseignements importants qui permettent aux fournisseurs autorisés de l'Ontario de prendre des décisions plus éclairées quant au traitement des patients à tout moment et en tout lieu. . Les fournisseurs de soins autorisés peuvent partager des images et des rapports de manière sécuritaire avec d'autres fournisseurs. Les images diagnostiques et les rapports qui s'y rattachent sont stockés dans un dépôt qui en permet l'extraction en format numérique. Les patients doivent donc moins souvent se déplacer pour consulter des spécialistes. Le programme s'appuie sur un certain nombre d'initiatives outre le service commun d'ID, notamment le Dépôt d'imagerie diagnostique des services hospitaliers, l' intégration des établissements de santé autonomes (ESA) et le Système de transfert d'images pour les urgences neurochirurgicales (STIUN).

Le programme d'ID s'inscrit dans l'approche globale de cyberSanté Ontario visant à améliorer l'accès à des soins sécuritaires pour les patients. La mise en place d'une infrastructure technique stable assure aux fournisseurs de soins un accès en temps opportun aux renseignements essentiels aux activités cliniques.

Avantages

Pour vous

- Accès aux rapports diagnostiques pour l'ensemble de l'Ontario
- Accès plus rapide et plus simple aux images[1] et aux rapports, et ce, en tout temps
- L'accès à distance aux rapports d'imagerie diagnostique permettant un service hors des heures d'ouverture
- Collaboration clinique en temps réel, d'où une amélioration de l'accès pour un plus large éventail de spécialistes

Pour vos patients

- Élimination des déplacements inutiles
- Réduction du temps d'attente et de la durée des séjours grâce à l'accélération des processus liés aux rapports d'examen et à la prise de décisions cliniques par les médecins et les spécialistes
- Réduction des examens en double et inutiles
- Élimination des transferts physiques d'images et ou de disques compacts à des spécialistes

[1] La première phase de la mise en place du service commun d'ID rend possible, à l'échelle de la province, le partage des rapports diagnostiques, alors que les prochaines versions y permettront le partage d'autres types de renseignements associés à l'ID.

Protection de la vie privée et sécurité

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.

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) [2]
- Un rapport en particulier (directive sur le consentement visant les dossiers);
- Tous les utilisateurs d'un organisme particulier (directive sur le consentement visant les mandataires – DRS).

[2] 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.

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.

Dérogation à une directive de consentement[3]

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.

[3] 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.

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.

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 possible[4].

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.

[4] 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.

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.

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.

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 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.

Demandes d'accès aux journaux de vérification

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.

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

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.

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 renseignements personnels sur la santé 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.

Conservation

Conseil

Les DRS doivent conserver les dossiers contenant des RPS en respectant certaines durées précises. Tous les renseignements compilés pour répondre aux demandes ou aux plaintes liées à l'accès aux renseignements et à leur rectification, ou aux renseignements en lien avec des directives relatives au consentement, doivent être conservés pour les deux ans qui suivent la

En vertu de la LPRPS, il incombe aux DRS de s'assurer que les dossiers sont conservés en respectant certaines durées précises, et qu'ils sont transférés et éliminés de manière sécuritaire. Il incombe aux DRS de s'assurer que les dossiers sont protégés et éliminés conformément à la *Politique de sécurité de l'information* à l'adressehttp://www.ehealthontario.on.ca/fr/initiatives/resources.

Les DRS conserveront les dossiers contenant les renseignements suivants en respectant les durées correspondantes :

Type de renseignements	**Durée de conservation**
RPS figurant dans le système de DSE	La plus longue des périodes suivantes : • Aussi longtemps que le DRS qui a créé et saisi les RPS dans le DSE conserve ces derniers dans ses systèmes locaux; • Selon la durée indiquée dans le calendrier de conservation établi par le DRS qui a créé et saisi les RPS dans le DSE; • Trente ans après le dernier cas d'utilisation dans le but de fournir des soins de santé, ou 10 ans après le décès du patient et en conformité avec toute ordonnance ou décision judiciaire applicable, ou toute autre exigence prévue par la loi.
Journaux et rapports de vérification contenant des RPS	Trente ans ou lorsque les RPS sont supprimés du DSE, selon la durée la plus longue.
Copies archivées des RPS figurant dans le système de DSE et des journaux et rapports de vérification renfermant des RPS	Conservation n'excédant pas 2 ans.
Renseignements recueillis pour répondre aux demandes des personnes concernant : o leur accès aux renseignements ou la rectification des renseignements en vertu de la LPRPS; o l'émission, la modification ou le retrait d'une directive en matière de consentement en vertu de la LPRPS; o leur demande de renseignements ou leur plainte déposée en vertu de la LPRPS.	Deux ans après le dépôt de la demande. Dans le cas des plaintes, deux après la fermeture, par le DRS, cyberSanté Ontario ou le CIPVP, du dossier de plainte, selon la durée la plus longue.
Renseignements créés au sujet d'une personne dans le cadre d'une enquête sur des violations touchant la protection de la vie privée ou des incidents de sécurité.	Deux après la fermeture, par le DRS, cyberSanté Ontario ou le CIPVP, du dossier lié à la violation touchant la protection de la vie privée, selon la durée la plus longue.
Renseignements utilisés aux fins d'enregistrement du service d'identification renfermant des RP	Sept ans après la dernière utilisation.
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 RPS	Au moins deux ans.

Type de renseignements	Durée de conservation
Modèles ou ressources élaborés par cyberSanté dans le cadre de l'utilisation du DSE	Au moins deux ans.
Documents liés aux assurances	Dix ans.
Documents opérationnels de cyberSanté Ontario	Au moins sept ans.

Les types de RPS en particulier que comprend chaque type de renseignements figurent dans la *Politique de conservation – DSE* à l'adresse http://www.ehealthontario.on.ca/fr/initiatives/resources.

Formation en protection de la vie privée et de la sécurité

Les DRS sont tenus d'offrir de la formation en protection de la vie privée et de la sécurité à leurs agents et fournisseurs de services électroniques avant qu'ils ne puissent accéder au système de DSE. La formation devrait faire en sorte que les agents et fournisseurs de services électroniques soient conscients de leurs obligations conformément à la législation sur la protection des renseignements personnels qui s'applique, notamment la LPRPS, de même qu'aux politiques et procédures sur la protection et la sécurité des renseignements personnels dans le cadre de l'utilisation du système de DSE. La formation devrait être terminée avant la création du compte donnant accès au service commun d'ID. cyberSanté Ontario a mis au point du matériel pour une formation axée sur les rôles afin de faciliter le respect de ces exigences en matière de formation. Pour ne rien oublier dans la formation en protection de la vie privée et de la sécurité, lisez la *Politique sur la formation en protection de la confidentialité et de la sécurité – DSE* qui se trouve à l'adresse http://www.ehealthontario.on.ca/fr/initiatives/resources. Tous les utilisateurs finaux doivent avoir reçu la formation en protection de la vie privée qui s'applique avant de pouvoir accéder au système.

Les DRS sont tenus de s'assurer, par suivi, que les agents, fournisseurs de services électroniques et utilisateurs finaux ont reçu la formation en protection de la vie privée et de la sécurité. La formation initiale ayant été complétée, de la formation doit être offerte annuellement.

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 renseignement personnel sur la santé.

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'organisation;
- la consultation, l'utilisation ou la recherche non autorisée en lien avec les 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 employées, 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.

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 signaler cette atteinte ou cette infraction 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 sur la santé 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.

Directives à l'intention des agents chargés de la protection des renseignements personnels

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 au1 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.

Veuillez 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 maîtriser l'étendue de l'incident, que ce soit par l'agent ou par le fournisseur de services électroniques qui a signalé l'incident, ou par le point de contact.

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.

Résumé des mesures de sécurité en place chez cyberSanté Ontario

Mesures administratives

- le directeur général de la protection de la vie privée et le chef de la sécurité de cyberSanté Ontario sont responsables de la protection de la vie privée et de la sécurité.

- cyberSanté Ontario dispose d'un ensemble complet de politiques sur la sécurité des renseignements qui s'harmonisent avec ses objectifs organisationnels et qui sont régulièrement revues et améliorées. Les membres du personnel et les entrepreneurs sont tenus de se familiariser avec les politiques pertinentes et de signer une attestation confirmant qu'ils ont lu et compris les politiques et qu'ils s'engagent à s'y conformer.

- Tous les employés et les entrepreneurs doivent signer des accords de confidentialité et faire l'objet d'une vérification des antécédents judiciaires avant d'entrer en fonction ou de fournir des services à cyberSanté Ontario cyberSanté Ontario a une politique d'enquête sur la sécurité qui exige que les membres du personnel doivent avoir un niveau approprié d'habilitation de sécurité en fonction de la sensibilité des renseignements auxquels ils peuvent avoir accès.

- cyberSanté Ontario dispose de programmes de sensibilisation et de formation obligatoires en matière de protection de la vie privée et de la sécurité.

- Le personnel et les entrepreneurs de cyberSanté Ontario n'ont généralement pas la capacité ni l'autorisation d'accéder aux RPS. Si l'accès aux RPS est nécessaire dans le cadre de la prestation de services à cyberSanté Ontario, il est interdit aux personnes d'utiliser ou de divulguer de tels renseignements à d'autres fins.

- cyberSanté Ontario veille, grâce à des contrats et à des ententes officielles de niveau de services, à ce que les tiers qu'il embauche pour fournir des services à cyberSanté Ontario ou à des dépositaires de renseignements sur la santé se conforment aux restrictions et aux conditions qui permettent à cyberSanté Ontario de s'acquitter pleinement de ses responsabilités juridiques.

- Le personnel, les consultants, les fournisseurs et les clients de cyberSanté Ontario doivent signaler rapidement à cyberSanté Ontario tout manquement à la protection de la vie privée et toute atteinte à la sécurité aux fins d'enquête. Un programme de gestion interne des incidents touchant la sécurité et la protection de la vie privée (ESPIM) a été établi pour assurer la gestion des incidents et les activités régulières de formation et de sensibilisation des membres du personnel qui participent à la gestion des incidents.

- Les évaluations des menaces et des risques (EMR) à la sécurité sont menées dans le cadre de l'élaboration des produits et des services et lors du déploiement pour les clients. Des activités d'atténuation des risques à la sécurité sont prévues, confiées à une personne responsable, consignées et suivies dans le cadre de chaque évaluation.

- cyberSanté Ontario fournit sur demande aux dépositaires de renseignements sur la santé concernés une copie écrite des résultats des évaluations de l'impact sur la vie privée et des évaluations des menaces et des risques à la sécurité.

- cyberSanté Ontario a établi un programme officiel de gestion des risques, y compris une politique et des lignes directrices. Un forum de gestion spécialisée, le groupe de responsables de la sécurité, fournit une orientation stratégique et assure la surveillance de la gouvernance du programme de sécurité, notamment l'examen périodique des risques et les plans correspondants de traitement des risques.

- Des registres des activités des utilisateurs, des activités des administrateurs de système, des dérogations et des événements touchant la sécurité des renseignements doivent être tenus et conservés en ligne pendant au moins six mois et archivés pendant au moins 18 mois, afin de faciliter la gestion des incidents et des problèmes, les futures enquêtes et la surveillance du contrôle de l'accès.

- cyberSanté Ontario tient un registre électronique de tous les accès aux RPS contenus dans le DSE et l'organisme est en voie d'élaborer des solutions visant à faire en sorte qu'un dossier identifie la personne qui a accédé à des renseignements et enregistre la date.

- Les registres de données qui sont nécessaires en cas de litige doivent être conservés jusqu'à ce que le différend juridique soit réglé.

- Tous les changements au réseau sont sous le contrôle de cyberSanté Ontario et assujettis aux pratiques officielles relatives à la gestion du changement.

Mesures techniques

- Des mots de passe fiables, des jetons sécurisés et d'autres solutions d'authentification sont nécessaires pour accéder aux systèmes sensibles.

- L'accès administratif au matériel de TI et aux applications repose sur le principe d'accès sélectif et est contrôlé à l'aide d'un dispositif d'autorisation approprié et d'une authentification forte à deux facteurs. Toutes les activités d'accès au système et aux applications sont consignées.

- cyberSanté Ontario assure la gestion du trafic sur le réseau à l'aide de mécanismes de sécurité tels que des routeurs, des commutateurs, des pare-feu réseau, et assure la surveillance de ce trafic grâce à des systèmes de détection des intrusions et des programmes antivirus.

- Toutes les données sensibles sont chiffrées lorsqu'elles sont transmises entre des sources externes et les systèmes de cyberSanté Ontario.

- Toutes les données stockées sur les ordinateurs du personnel sont chiffrées. Si un ordinateur portable est perdu ou volé, la confidentialité et l'intégrité des données ne sont menacées.

- Des contrôles de l'intégrité des données sont effectués dans le cadre des activités d'assurance de la qualité des RPS transmis à cyberSanté Ontario par les dépositaires de renseignements sur la santé.

- Des évaluations indépendantes de la vulnérabilité des configurations techniques et des pratiques opérationnelles de sécurité sont effectuées périodiquement.

- Un processus de gestion des correctifs est en place pour veiller à ce que les systèmes d'exploitation, les bases de données et les applications reçoivent les correctifs de sécurité et les mises à jour fonctionnelles à point nommé.

- Lors de la cessation d'un emploi ou de la fin d'un contrat, tous les comptes des anciens membres du personnel ou consultants sont supprimés et l'accès est désactivé.

- Les données et les applications sont sauvegardées régulièrement, et elles peuvent être facilement restaurées en cas d'incidents opérationnels.

- Un plan complet de reprise après catastrophe (RC) et un plan de continuité des activités (PCA) ont été mis en place et sont testés et mis à jour périodiquement.

Mesures physiques

- Les centres de données de cyberSanté Ontario ont été spécialement conçus pour répondre aux besoins de l'organisme. Ils sont dotés de contrôles environnementaux appropriés et sont physiquement protégés contre tout accès non autorisé. Ils sont surveillés par un personnel de sécurité qualifié présent en permanence.

- Des zones de sécurité particulières sont établies afin de séparer et de contrôler l'accès aux zones publiques, de livraison et de chargement, aux bureaux et aux salles d'ordinateurs, avec des contrôles de sécurité physiques de plus en plus rigoureux.

- Les contrôles de sécurité physique des centres de données ont été validés par un tiers indépendant, conformément aux normes du gouvernement fédéral, et à l'aide d'évaluations internes des menaces et des risques.

- L'accès aux bureaux est contrôlé par des laissez-passer et les déplacements dans les bureaux sont enregistrés par des caméras de sécurité.

- L'accès aux bureaux où les activités exigent un accès à des renseignements personnels et à des RPS est physiquement limité aux seuls membres du personnel dont le rôle consiste à traiter les renseignements personnels et les RPS. Les autres membres du personnel n'ont pas accès à ces zones, que ce soit physiquement ou par l'intermédiaire du système informatique.

- Les visiteurs et les fournisseurs externes qui se rendent aux bureaux de cyberSanté Ontario doivent être munis d'un laissez-passer et ils sont escortés en tout temps par des membres du personnel à temps plein. Les laissez-passer sont automatiquement désactivés après 24 heures et ils ne peuvent pas être réutilisés.

- Le matériel mis hors service qui a servi à traiter ou à stocker des renseignements personnels ou des RPS est détruit, selon les procédures approuvées.

- Des procédures et du matériel adaptés sont en place pour l'élimination sécuritaire du papier, des CD ou d'autres médias pouvant contenir des renseignements confidentiels.