

cyberSanté Ontario

Politique sur la protection des renseignements personnels sur la santé

Identificateur du document : 2478

Version : 4.0

Table des matières

1	Introduction	1
1.1	But/Objectif	1
1.2	Portée	1
1.3	Application	2
1.4	Autres politiques	2
2	Aperçu de la LPRPS	2
2.1	Généralités	2
2.2	Dépositaire de renseignements sur la santé	3
2.3	Gestionnaire de l'information	3
2.4	Fournisseur d'un réseau d'information sur la santé	3
2.5	Fournisseur de services électroniques	4
2.6	Mandataire	4
3	Politique sur la protection des renseignements personnels sur la santé	5
4	Premier principe : Responsabilité	5
4.1	Responsabilité de cyberSanté Ontario	5
4.2	Accords	6
4.3	Gestion de l'information	8
4.4	Surveillance de la conformité	9
4.5	Gestion des incidents touchant la protection de la vie privée	9
4.6	Formation et sensibilisation	9
4.7	Norme de conduite	10
4.8	Responsabilité à l'égard du public et transparence	11
5	Deuxième principe : Détermination des fins de la collecte de renseignements	
6	Troisième principe : Consentement	11
6.1	Rôle de cyberSanté Ontario dans la gestion du consentement	12
7	Quatrième principe : Limitation de la collecte	12
8	Cinquième principe : Limitation de l'utilisation, de la communication et de la conservation	13
8.1	Utilisation des RPS par cyberSanté Ontario	13
8.2	Divulgaration des RPS par cyberSanté Ontario	13
8.3	Conservation des RPS par cyberSanté Ontario	14
8.4	Contrôle d'accès	14
8.4.1	Accès par les membres du personnel de cyberSanté Ontario	14
8.4.2	Consignation de accès	15
8.4.3	Accès par les utilisateurs finaux	16
8.4.4	Accès par les fournisseurs de service	16
9	Sixième principe : Exactitude	17
10	Septième principe : Mesures de sécurité	17
10.1	Mécanismes de sécurité	17
10.2	Surveillance de la conformité	18
10.3	Évaluations de l'impact sur la protection de la vie privée	19
11	Principe 8 : Transparence	20
12	Principe 9 : Accès aux renseignements personnels	20
13	Principe 10 : Possibilité de porter plainte contre le non-respect des principes	21
13.1	Plaintes relatives à cyberSanté Ontario	21
13.2	Plaintes relatives aux DRS	22
13.3	Plaintes au CIPVP	22

14	Approbation et examen des politiques	23
15	Glossaire.....	23
16	Références et documents connexes	25

Contrôle du document

La version électronique de ce document est reconnue comme la seule version valide.

Emplacement du document :	http://www.ehealthontario.on.ca/privacy
Fréquence de révision :	Annuellement ou plus souvent, à la discrétion du chef de la protection des renseignements personnels
Initiateur du document *	Anne Motwani Analyste principale, protection des renseignements personnels

*Les demandes de renseignements sur ce document doivent être adressées à l'initiateur du document.

Historique de l'approbation

Approbateur(s)	Date d'approbation
John Moore, premier vice-président aux services généraux	2011-10-18
Patrick Lo, directeur de la protection des renseignements personnels	2011-10-17
Kathy Callfas, gestionnaire des services d'assurance de la protection des renseignements personnels	2011-10-17
Groupe de direction de la protection des renseignements personnels	2011-09-19

Historique des révisions

Numéro de la version	Date de la version	Résumé du changement	Auteur
4	2011-10-13	Version définitive	Anne Motwani
3.1	2011-08-31	Révisions afin d'assurer la conformité à l'article 6.2 de la LPRPS de l'Ontario, <i>Règl. 329/04</i> , modifié par le <i>Règl. de l'Ont. 331/11</i>	Anne Motwani
3	2009-08-12	Révision effectuée par le chef de la protection des renseignements personnels et de la sécurité	Patrick Lo
2	2008-09-26	Révision effectuée par le vice-président, protection des renseignements personnels et sécurité. Révisions définitives complétées.	Angelique Hamilton
1	2007-09-28	Version définitive	Sharan Dosanjh

1 Introduction

1.1 But/Objectif

La présente politique sur la protection des renseignements personnels a pour but d'établir les exigences et les responsabilités obligatoires pour la protection des renseignements personnels sur la santé (RPS) reçus ou envoyés par cyberSanté Ontario.

Les RPS désignent généralement les renseignements sur une personne, sous forme orale ou écrite, qui ont trait à sa santé physique ou mentale. À titre d'exemple, les antécédents familiaux en matière de santé, le numéro de carte santé et tout renseignement qui identifie une personne et la relie à un fournisseur de soins de santé.

cyberSanté Ontario s'engage à être un chef de file en matière de protection de renseignements personnels et à encourager la confiance de ses clients et du public. Par conséquent, les exigences énoncées dans la présente politique sont supérieures à celles énoncées dans la loi et le règlement et reflètent les pratiques exemplaires en matière de gestion de l'information pour la protection des RPS.

1.2 Portée

La présente politique s'applique à tous les employés permanents et au personnel temporaire de cyberSanté Ontario (sous l'appellation collective « personnel ») et aux tiers fournisseurs de services choisis pour appuyer ses activités et la prestation de ses services.

Elle s'applique :

- à la *Loi de 2004 sur la protection des renseignements personnels sur la santé* (LPRPS), chap. 3, et plus particulièrement :
 - art. 10
 - art. 17
- au *Règlement de l'Ontario 329/04* adopté en vertu de la LPRPS, et plus particulièrement :
 - art. 6
 - art. 6.1
 - art.6.2
- au *Règlement de l'Ontario 43/02* adopté en vertu de la *Loi sur les sociétés de développement*, L.R.O. 1990, chapitre D. 10.

L'article 6.2 de la LPRPS, *Règl. de l'Ont. 329/4*, telle que modifiée par le *Règl. de l'Ont. 331/33* en juin 2011, précise le rôle de cyberSanté Ontario en matière de création et de tenue d'un ou de plusieurs dossiers de santé électronique (DSE) et précise les responsabilités et les obligations de cyberSanté Ontario à cet égard. En vertu de l'article 6.2 du Règlement, cyberSanté Ontario n'est pas considérée comme rassemblant ou diffusant des RPS en créant ou en tenant des DSE. Cette

modification s'applique à cyberSanté Ontario jusqu'au 31 décembre 2013, lors de l'expiration de l'article du règlement modifié et/ou jusqu'à ce qu'il en soit déterminé autrement.

Consulter la section 2 ci-dessous pour connaître les rôles en vertu de la LPRPS que cyberSanté Ontario pourrait jouer éventuellement ainsi que les obligations qui découlent de ces rôles aux termes de la *Loi*.

1.3 Application

La présente politique s'applique à tout le personnel à plein temps, à temps partiel et temporaire de cyberSanté Ontario, aux employés contractuels, aux tiers fournisseurs de services ou aux mandataires retenus (sous l'appellation collective « personnel »). Elle s'applique à tous les services et activités de l'entreprise susceptibles d'avoir une incidence sur la confidentialité des RPS confiés à cyberSanté Ontario. Les dispositions applicables de cette politique seront abordées dans les accords de cyberSanté Ontario avec les tiers fournisseurs de services et les usagers finaux des services de cyberSanté Ontario.

1.4 Autres politiques

La présente politique doit être consultée de concert avec la *Politique sur la protection de la vie privée et des données* de cyberSanté Ontario. Elle est appuyée par d'autres politiques, normes, procédures et lignes directrices de cyberSanté Ontario qui font partie d'un programme global pour la protection des RPS. Ces politiques incluent, sans en exclure d'autres :

- Health Ontario Privacy Impact Assessment Policy (Politique d'évaluation de l'impact sur la protection de la vie privée de cyberSanté Ontario)
- eHealth Ontario Privacy Incident Management Policy (Politique de gestion des incidents touchant la vie privée)
- *Procédure des plaintes et des enquêtes en matière de vie privée* de cyberSanté Ontario
- eHealth Ontario Privacy Policy on the Responsibilities of Third Party Service Providers (Politique sur la protection des renseignements personnels relative aux responsabilités des tiers fournisseurs de services de cyberSanté Ontario)

2 Aperçu de la LPRPS

2.1 Généralités

La LPRPS est une loi provinciale sur la protection des renseignements personnels sur la santé. Elle établit les règles de gestion des RPS et de la protection de la confidentialité de ces renseignements, tout en facilitant la prestation efficace de services de soins de santé.

En élaborant, fournissant et maintenant des solutions et des services, cyberSanté Ontario doit se conformer aux exigences particulières aux rôles décrits dans la LPRPS et son Règlement. La série

d'exigences qui s'appliquent à cyberSanté Ontario dépend de la nature de la relation d'affaires entre cyberSanté Ontario et ses clients ainsi que de la nature des services qu'elle leur fournit.

cyberSanté Ontario peut agir dans un certain nombre de capacités prévues à la LPRPS et à son Règlement : en vertu de l'article 6.2 du Règlement de l'Ontario 329/04, comme fournisseur d'un réseau d'information sur la santé (FRIS), mandataire d'un dépositaire de renseignements sur la santé, fournisseur de services électroniques ou fournisseur de services à un réseau d'information sur la santé. Chaque rôle est axé sur la relation que cyberSanté Ontario entretient avec un ou plusieurs dépositaires de renseignements sur la santé (DRS).

2.2 Dépositaire de renseignements sur la santé

Un dépositaire de renseignements sur la santé est une personne qui fournit des services de soins de santé. Les médecins, les hôpitaux, les pharmacies, les laboratoires, les centres d'accès aux soins communautaires ainsi que le ministère de la Santé et des Soins de longue durée sont de dépositaires de renseignements sur la santé. cyberSanté Ontario n'en est pas un.

Un DRS a la garde et le contrôle des RPS en raison du travail qu'il accomplit. Il a le droit de traiter avec les RPS et de créer des dossiers, de même que la responsabilité de maintenir la confidentialité et la sécurité des RPS. Bien qu'il soit le propriétaire des documents et des systèmes dans lesquels les renseignements sont inscrits (p. ex. les papiers graphiques, les ordinateurs ou les systèmes de technologie de l'information), les patients sont les propriétaires de leurs RPS.

2.3 Gestionnaire de l'information

L'article 6.2 du *Règl. de l'Ont. 329/04* de la LPRPS a été modifié en juin 2011 afin de clarifier le rôle de cyberSanté en matière de création et de tenue d'un ou de plusieurs DSE en tant que service à l'intention des DRS. En vertu de la modification de l'article 6.2 du Règlement de la LPRPS, cyberSanté Ontario a l'autorisation de créer des dossiers de RPS en format électronique afin de permettre aux dépositaires de renseignements sur la santé d'utiliser des moyens électroniques pour divulguer des RPS entre eux dans le but de fournir ou d'aider à fournir des soins de santé à la personne dont les RPS sont contenus dans le dossier.

cyberSanté Ontario peut avoir des RPS dans ses systèmes pendant la prestation de services. Cependant, le DRS doit rendre compte au patient des pratiques de protection des renseignements personnels relatives aux RPS.

2.4 Fournisseur d'un réseau d'information sur la santé

En qualité de FRIS, cyberSanté Ontario fournit des services à deux ou à plusieurs DRS principalement afin de leur permettre d'utiliser des moyens électroniques pour divulguer des RPS entre eux. cyberSanté Ontario agit en cette qualité dans un certain nombre de ses relations d'affaires.

À titre d'exemple, cyberSanté Ontario est un FRIS lorsqu'il fournit les services de réseau ONE[®] Network à des milliers de DRS afin de leur permettre d'échanger des RPS sur ce réseau en toute sécurité.

En qualité de FRIS, cyberSanté Ontario peut avoir des RPS dans ses systèmes pendant qu'elle fournit des services. Cependant, le DRS doit rendre compte au patient des pratiques de confidentialité relatives aux RPS.

2.5 Fournisseur de services électroniques

En qualité de fournisseur de services électroniques (FSE), cyberSanté Ontario fournit des services afin de permettre à un DRS d'utiliser des moyens électroniques pour recueillir, utiliser, modifier, divulguer, conserver ou éliminer des RPS. À titre d'exemple, cyberSanté Ontario peut héberger un service de gestion clinique utilisé par les médecins.

Lorsque cyberSanté Ontario agit à titre de FSE, ses obligations en matière de protection de la vie privée sont définies par un accord entre cyberSanté Ontario et le DRS. En vertu de cette autorité, cyberSanté Ontario ne joue aucun rôle indépendant de décideur relativement aux RPS et ne détient aucun intérêt à leur égard, mais agit conformément aux directives du DRS qu'il sert, dans les limites prévues à la LPRPS.

2.6 Mandataire

En qualité de mandataire d'un DRS, cyberSanté Ontario agit pour ou au nom du DRS en matière de collecte, utilisation ou divulgation des RPS, pour les besoins du DRS, et non pour ses propres besoins. À titre d'exemple, le MSSLD peut désigner cyberSanté Ontario comme mandataire pour gérer un répertoire électronique de patients en Ontario.

Un DRS peut permettre à cyberSanté Ontario d'accéder aux RPS, de les utiliser, de les divulguer ou d'en disposer en son nom seulement dans les limites déjà imposées au DRS à cet égard, avec l'autorisation expresse du DRS.

En qualité de mandataire d'un DRS, cyberSanté Ontario ne prend aucune décision indépendante en matière de traitement des RPS, mais agit uniquement conformément aux conditions de cet accord avec le DRS et conformément à la LPRPS.

3 Politique sur la protection des renseignements personnels sur la santé

Cette politique est structurée autour de dix principes relatifs à l'équité du traitement du *Code type sur la protection des renseignements personnels* de l'Association canadienne de normalisation (*Code type de la CSA*)¹. Le *Code type de la CSA* a été reconnu comme norme nationale pour la protection de la vie privée en 1996 et est utilisé dans tout le Canada comme fondement de la législation sur la protection des renseignements personnels sur la santé, notamment pour la LPRPS.

4 Premier principe : Responsabilité

Le principe de responsabilité signifie qu'un organisme est responsable des RPS qu'il gère et qu'il a désigné une ou plusieurs personnes qui sont responsables de la conformité de l'organisme aux principes de protection des renseignements personnels.

4.1 Responsabilité de cyberSanté Ontario

Le Conseil d'administration de cyberSanté Ontario doit rendre compte aux DRS et aux patients de la protection et de la confidentialité des RPS qu'on lui a confiés. cyberSanté Ontario s'est engagée à observer la norme la plus élevée de soin et de protection des renseignements personnels dans les services et les technologies qu'elle gère.

Le Conseil d'administration délègue au président et chef de la direction l'autorité de mettre en œuvre des mesures de protection des renseignements personnels et des données chez cyberSanté Ontario. Il peut déléguer une personne qui agira en son nom et nomme le chef de la protection des renseignements personnels à ce titre.

Le chef de la protection des renseignements personnels est chargé de surveiller le Bureau de la protection de la vie privée de cyberSanté Ontario. Il délègue la responsabilité de mettre en œuvre les politiques et les programmes de protection de la vie privée de cyberSanté Ontario à l'échelle de l'organisme au directeur, Protection de la vie privée.

Les éléments clés du programme de protection de la vie privée de cyberSanté Ontario incluent :

- une série de politiques et de procédures sur la protection de la vie privée qui appuient la gestion et l'opérationnalisation efficaces de la protection de la vie privée par cyberSanté Ontario;
- un programme de formation et de sensibilisation des employés complet et axé sur leur rôle;

¹ Association canadienne de normalisation, CAN/CSA – Q830-96, *Code type sur la protection des renseignements personnels*, mars 1996.

- des évaluations à jour et exactes sur la protection de la vie privée des systèmes et des services de cyberSanté Ontario qui comportent des RPS;
- des activités de gestion des risques en matière de protection de la vie privée dans tout le cycle de vie des systèmes et des services qui comportent des RPS;
- un réseau de personnes dans tout l'organisme ayant des responsabilités définies en matière de protection de la vie privée.

Les responsabilités du chef de la protection des renseignements personnels consistent à :

- veiller à ce que le directeur, Protection de la vie privée, soit informé des nouveaux services ou activités de l'organisation qui concernent des RPS;
- veiller à ce que les parties responsables accordent suffisamment de temps et de fonds dans leurs plans de projets pour mener des évaluations du seuil de protection de la vie privée et/ou des évaluations de l'impact sur la protection de la vie privée, conformément à la politique d'évaluation de l'impact sur la protection de la vie privée;
- veiller à la disponibilité et à la collaboration d'un personnel suffisant pour faciliter la collecte et la documentation de renseignements relatifs au service soumis à une analyse de protection de la vie privée;
- mettre en œuvre les recommandations des évaluations du seuil de protection de la vie privée et/ou des évaluations de l'impact sur la protection de la vie privée.

Le directeur principal, Approvisionnement stratégique et gestion des fournisseurs est chargé d'aider à veiller à ce que les exigences en matière de protection de la vie privée établies par le chef de la protection des renseignements personnels soient respectées dans les accords avec les tiers fournisseurs de services qui demandent l'accès aux renseignements, aux sites, aux produits d'information ou aux systèmes d'information de cyberSanté Ontario (incluant l'accès à distance) ou qui traitent des RPS au nom de cyberSanté Ontario.

Le personnel de cyberSanté Ontario doit respecter toutes les politiques sur la protection de la vie privée de cyberSanté Ontario, dans la mesure où celles-ci s'appliquent à leurs activités.

Le Bureau de protection de la vie privée de cyberSanté Ontario est chargé de définir et de surveiller les activités quotidiennes de l'organisme qui visent à protéger les RPS et la vie privée. Ce bureau, en collaboration avec les unités fonctionnelles de cyberSanté Ontario pertinentes, maintiendra les protocoles de protection de la vie privée établis par cyberSanté dans ses politiques, procédures et autres éléments de régulation sur la protection de la vie privée.

cyberSanté Ontario peut imposer des sanctions à son personnel et/ou à ses tiers fournisseurs de services agissant en son nom qui enfreignent cette politique selon les politiques et procédures disciplinaires et d'approvisionnement de l'organisme, et peut se prévaloir de mesures jusques et y compris le licenciement ou la résiliation de contrat.

4.2 Accords

Les accords ont pour objet d'établir officiellement les rôles et responsabilités liés à la gestion et à protection des RPS. cyberSanté Ontario conclut des accords avec toutes les personnes et entités :

- auxquelles cyberSanté Ontario fournit des services, avant de les fournir, incluant les utilisateurs finaux, les DRS et les FRIS;
- qui fournissent des services à cyberSanté Ontario, avant de les offrir, incluant les employés et les tiers fournisseurs de services de cyberSanté Ontario.

Les accords doivent porter, s'il y a lieu, sur les domaines suivants :

- les responsabilités et obligations législatives pertinentes;
- les rôles et responsabilités mutuels, les processus et les mesures de protection pour les RPS;
- le traitement des RPS;
- les conditions selon lesquelles les parties peuvent accéder aux RPS et la portée des RPS auxquels chaque partie peut accéder;
- les rôles et responsabilités pour la gestion des incidents liés à la protection des renseignements personnels;
- les rôles et responsabilités relatifs au service fourni;
- les processus et les obligations mutuelles relativement à la surveillance et à la conformité;
- les pénalités pour les violations de l'accord;
- un plan de protection des renseignements personnels (à l'intention des tiers fournisseurs de services, s'il y a lieu).

En vertu de la LPRPS, lorsque cyberSanté Ontario agit aux termes de l'article 6.2 de la LPRPS, Règl. de l'Ont. 329/04 aux fins de créer et de tenir un ou plusieurs DSE, l'organisme n'est pas tenu de conclure des accords avec ces DRS. Cependant, cyberSanté Ontario s'engage à mettre en œuvre des pratiques exemplaires en sus de ses obligations en vertu de la LPRPS et à instaurer une confiance à l'intérieur et à l'extérieur du secteur de la santé. Par conséquent, cyberSanté Ontario s'engage à conclure des accords avec toutes les entités et personnes qui traitent des RPS (incluant les DRS, les mandataires, les FRIS, les utilisateurs finals, le ministère de la Santé et des Soins de longue durée et les tiers qui aident à fournir des services), dans une mesure raisonnable, afin de s'assurer que les RPS sont protégés et que la protection de la vie privée est respectée.

cyber Santé Ontario conserve et gère les accords par le biais d'une fonction centrale intégrée.

cyberSanté Ontario maintient des outils et des procédures afin de s'assurer que les accords sont surveillés et mis à jour au besoin.

Tout accord conclu par cyberSanté Ontario avec des tiers pour appuyer sa prestation de services aux DRS et aux FRIS doit prévoir que le tiers accepte de se conformer à toutes les lois, restrictions, conditions et exigences applicables auxquelles cyberSanté Ontario est également liée.

4.3 Gestion de l'information

Les politiques et procédures de cyberSanté Ontario pour la protection des RPS et de la vie privée des patients sont des éléments essentiels de l'approche de gestion de l'information de l'organisme. Cette approche place tous les dépôts de RPS de cyberSanté Ontario dans une matrice de rôles et de responsabilités, de processus administratifs et opérationnels de haut niveau, ainsi que de protections et de contrôles.

cyberSanté Ontario protège les RPS qui lui sont confiés pendant tout leur cycle de vie, à partir du moment où ils leur parviennent jusqu'à ce qu'ils soient détruits, conformément au calendrier de conservation de ses dossiers.

La gestion de l'information inclut des procédures et des processus de conservation et de destruction des RPS. La politique sur la gestion du cycle de vie des RPS est détaillée à la section 8.

cyberSanté Ontario attribue à chaque dépôt des RPS une personne (appelée *responsable des données*) chargée de la gestion et de la surveillance du dépôt de données. Le mandat des responsables des données est maintenu par le Bureau de la protection de la vie privée de cyberSanté Ontario.

L'approche de gestion de l'information de cyberSanté Ontario définit les rôles pour toutes ses unités administratives qui jouent un rôle dans la protection des RPS, surtout la sécurité de l'information, mais aussi le service de l'approvisionnement, des éléments juridiques, de la gestion des risques et des opérations. Ces rôles sont définis selon une matrice de gestion de l'information de haut niveau RACI (responsabilité, approbation, consultation et information). Le Bureau de la protection de la vie privée de cyberSanté Ontario gère la définition de tous les rôles pertinents.

Le Bureau de la protection de la vie privée de cyberSanté Ontario garde une liste de magasins de données pour tous les dépôts de données, qu'on peut trouver sur le site Web de cyberSanté Ontario. La liste est revue périodiquement de sorte qu'elle soit exacte et complète.

cyberSanté Ontario doit s'assurer que :

- la confidentialité des données de la liste des magasins de données est protégée adéquatement;
- l'accès est limité aux membres du personnel dont les rôles exigent un tel accès;
- l'accès est consigné, incluant le nom de la personne qui a accédé à l'information, l'objet de cet accès ainsi que la date et l'heure de celui-ci;
- les consignations d'accès sont examinées périodiquement afin de s'assurer que tout accès aux RPS est encore pertinent aux fins indiquées;
- les dépôts des données sont conservés uniquement le temps nécessaire pour satisfaire aux besoins pour lesquels elles ont été recueillies.

4.4 Surveillance de la conformité

cyberSanté Ontario surveille activement la conformité à ses politiques et procédures qui comprennent les mesures de protection et de contrôle qu'elle a mises sur pied pour protéger les RPS dans ses systèmes.

La conformité du personnel de cyberSanté Ontario et de ses tiers fournisseurs de services avec lesquels elle a conclu des accords (particulièrement les DRS et les fournisseurs tiers ayant accès aux RPS) est surveillée constamment d'une façon qui permet à l'organisme de mesurer et d'évaluer la conformité à ses politiques et à ses normes et d'en rendre compte. Le chef de la protection des renseignements personnels présente régulièrement un compte rendu des résultats de la surveillance à la conformité au comité exécutif de cyberSanté Ontario et, s'il y a lieu, à son Conseil d'administration.

cyberSanté Ontario aide les DRS qui utilisent ses services à respecter leurs propres obligations de surveillance de la conformité à ces services.

En tant qu'élément clé de la protection des RPS, la surveillance de la conformité est abordée de façon plus détaillée à la section 9.

4.5 Gestion des incidents touchant la protection de la vie privée

cyberSanté Ontario prend toutes les mesures nécessaires afin d'aborder toute collecte, conservation, utilisation ou divulgation des RPS dans ses systèmes qui ne sont pas conformes à la loi pertinente, particulièrement la LPRPS, ou aux politiques et procédures de cyberSanté Ontario.

La *Privacy Incident Management Policy* (Politique de gestion des incidents touchant la protection de la vie privée) de cyberSanté Ontario décrit l'approche de l'organisme de la gestion de tels incidents. Le processus selon lequel un incident est confiné, examiné et corrigé est défini par le programme de gestion interne des incidents touchant la sécurité et la protection de la vie privée (ESPIM).

Conformément à la *Privacy Incident Management Policy* (Politique de gestion des incidents touchant la protection de la vie privée) et à ESPIM, cyberSanté Ontario doit confiner les effets de l'incident en déterminant sa nature et sa portée et émettre tous les avis nécessaires par le biais d'un processus clair de communication et de signalisation progressive, le premier avis étant envoyé au DRS ou aux DRS qui ont la garde réelle des RPS qui ont fait l'objet de l'incident.

4.6 Formation et sensibilisation

cyberSanté Ontario est dédiée à encourager une culture solide de sensibilisation à la protection de la vie privée au sein de son personnel. Par conséquent, elle possède un programme complet de formation et de sensibilisation à la protection de la vie privée et à la sécurité qui offre aux membres de son personnel :

- un aperçu de la LPPS et des obligations de cyberSanté Ontario en vertu de la législation relative à la protection de la vie privée;
- une description de leurs responsabilités en matière de protection de la vie privée;
- des responsabilités à ce chapitre fondées sur leur rôle pour ceux qui sont susceptibles d'exiger un accès aux RPS, le cas échéant, en se fondant sur les responsabilités du poste de la personne ou du travailleur contractuel;
- des renseignements sur les mesures de protection physique, technique et administrative en vigueur chez cyberSanté Ontario pour protéger les RPS;
- le processus servant au repérage et au compte rendu d'incidents potentiels ou réels en matière de protection des renseignements personnels et de sécurité.

Le contenu de la formation doit être révisé annuellement ou plus souvent, à la discrétion du chef de la protection des renseignements personnels. Ce contenu sera mis à jour pour aborder tous les changements importants aux exigences de la loi, des règlements et des politiques de cyberSanté Ontario et toute autre question que le chef de la protection des renseignements personnels juge appropriée.

Tous les membres du personnel de cyberSanté Ontario doivent suivre la formation en matière de protection de la vie personnelle et de sécurité à l'échelle de l'entreprise dans les 30 jours qui suivent leur entrée en fonction au sein de l'organisme, puis annuellement par la suite.

cyberSanté Ontario doit élaborer et donner une formation en matière protection de la vie privée et de sécurité axée sur les rôles à l'intention des membres de son personnel susceptibles de devoir accéder aux RPS pour accomplir les tâches qui leur sont attribuées.

Les membres de cyberSanté Ontario qui peuvent avoir accès aux RPS dans le cadre de leurs tâches doivent suivre une formation en matière de protection de la vie privée et de sécurité avant d'obtenir l'accès à des RPS.

Les DRS et les tiers fournisseurs de services sont chargés de donner une formation en matière de protection de la vie privée et de sécurité à leur personnel et à leurs représentants. cyberSanté Ontario appuie les DRS et les tiers fournisseurs de services à ce chapitre relativement aux services qu'elle offre (p. ex. politiques relatives à la gestion des incidents touchant la protection de la vie privée).

cyberSanté Ontario maintient des procédures et d'autres mécanismes de soutien nécessaires afin de lui permettre de vérifier si la formation a été donnée et d'assurer la conformité aux exigences en matière de formation.

4.7 Norme de conduite

Tous les membres du personnel de cyberSanté Ontario doivent signer un formulaire indiquant qu'ils reconnaissent et acceptent la *Norme de conduite* avant le début de leur emploi à l'organisme.

cyberSanté Ontario fournit une *Norme de conduite* aux membres de son personnel et à ses tiers fournisseurs de services détaillant leurs responsabilités et obligations en matière de protection de la vie privée et de la sécurité.

4.8 Responsabilité à l'égard du public et transparence

cyberSanté tient à rendre son programme de protection de la vie privée et les mesures qu'elle prend pour protéger les RPS aussi clairs et accessibles que possible. cyberSanté Ontario décrit en langage clair ses services et ses mesures de protection en la matière et, dans la présente politique et, des discussions claires sur la législation et les règlements pertinents, particulièrement la LPRPS et la LPRPS, Règl. de l'Ont. 329/04.

De plus, cyberSanté Ontario fournit des comptes rendus sur les listes de contrôle, au besoin, offre des résumés en langage simple de ses évaluations de l'impact sur la protection de la vie privée et fournit un processus clair afin de gérer les plaintes et les demandes de renseignements liées à la protection de la vie privée. Des détails sur ces mesures figurent dans cette politique, aux sections 9,10,11 et 12.

5 Deuxième principe : Détermination des fins de la collecte de renseignements

Le principe de détermination des fins de la collecte de renseignements signifie que les fins pour lesquelles les RPS sont recueillis doivent être déterminées par l'organisme avant ou au moment de la collecte.

La collecte des RPS incombe au DRS afin d'informer le patient des fins pour lesquelles les RPS seront recueillis, utilisés et divulgués.

Les fins pour lesquelles on permet à cyberSanté Ontario d'utiliser les RPS sont énumérées à la section 8 de la présente politique. La liste des magasins de données de cyberSanté Ontario figurant sur son site Web comprend un énoncé de but pour chaque dépôt de données. cyberSanté Ontario devra respecter cet énoncé en ce qui a trait à l'échange, la collecte, l'utilisation et la divulgation de données, au besoin, dans chaque dépôt qu'elle gère.

6. Troisième principe : Consentement

Le principe de consentement signifie que la personne doit être informée et consentir à la collecte, l'utilisation et la divulgation des RPS, sauf lorsque cela est inopportun.

Le consentement est la permission que donne un patient au DRS pour la collecte, l'utilisation et la divulgation de ses RPS. Il doit être bien informé, transparent et significatif et avoir rapport aux renseignements recueillis, utilisés ou divulgués par le DRS à une fin particulière et doit être obtenu sans tromperie ou coercition.

Une personne a le droit d'établir une directive de consentement sur ses RPS. Une telle directive est une instruction expresse d'une personne à son DRS relativement à l'utilisation ou la divulgation de ses RPS. Les directives de consentement incluent :

- le retrait de consentement de partager ou d'utiliser des RPS à des fins de soins de santé (ce qui entraîne le blocage du dossier du patient);
- le rétablissement de consentement pour partager des RPS afin de fournir ou d'aider à fournir des soins de santé et un traitement (qui entraîne le déblocage du dossier du patient).

Les DRS peuvent généralement compter sur un consentement implicite (présumant que le patient est bien informé) afin de recueillir, utiliser et divulguer des RPS dans le but de fournir des soins de santé ou d'aider à les fournir. Un DRS doit obtenir le consentement exprès (consentement qui est explicitement et directement accordé par le patient sous forme orale ou écrite) lorsqu'il utilise ou divulgue des RPS pour une autre raison que celle pour laquelle ils ont été recueillis.

6.1 Rôle de cyberSanté Ontario dans la gestion du consentement

cyberSanté Ontario doit aider les DRS à respecter leurs obligations en vertu de la LPRPS en matière de consentement en offrant dans ses services aux DRS les mécanismes nécessaires afin d'enregistrer le consentement du patient et de gérer les directives relatives à ce consentement, particulièrement la création et la révocation des directives de consentement, l'annulation des directives ainsi que l'enregistrement des annulations et l'alerte connexe.

cyberSanté Ontario doit maintenir des exigences à jour pour la conception et la mise en œuvre des processus de gestion du consentement dans ses services et systèmes. Les directives de consentement doivent être documentées de façon constante, dans une mesure raisonnable et pratique, et conservées dans un environnement sécurisé.

cyberSanté Ontario n'accédera pas aux RPS qui ont été bloqués en raison d'une directive de consentement, à moins que ce soit absolument nécessaire de le faire, conformément à la LPRPS. S'il faut accéder aux RPS, cet accès sera enregistré et restreint, conformément aux exigences en matière de sécurité de l'information de cyberSanté Ontario sur le contrôle d'accès aux systèmes et à celles prévues à la présente politique.

7 Quatrième principe : Limitation de la collecte

Le principe de limitation de la collecte signifie que la collecte des RPS doit se restreindre à ce qui est nécessaire aux fins déterminées par l'organisme. Les RPS doivent être recueillis par des moyens équitables et licites.

cyberSanté Ontario ne « recueille » pas les RPS, selon la définition de ce terme dans la LPRPS pour ses propres fins. cyberSanté Ontario recueille les RPS seulement à la demande des DRS auxquels elle fournit des services lorsqu'elle agit à titre de mandataire aux termes de la LPRPS.

Lorsque cyberSanté Ontario crée ou tient un ou plusieurs DSE, elle ne *recueille* pas de RPS selon la définition du terme dans la LPRPS.

Les DRS déterminent quels RPS, tirés des renseignements recueillis auprès des patients, sont fournis à cyberSanté Ontario et à quelles fins. cyberSanté Ontario a la permission de ne recevoir que les renseignements que les DRS ont en commun.

8 Cinquième principe : Limitation de l'utilisation, de la communication et de la conservation

Le principe de limitation de l'utilisation, de la communication et de la conservation signifie que les RPS ne doivent pas être utilisés ou communiqués à des fins autres que celles pour lesquelles ils ont été recueillis, à moins que la personne concernée n'y consente ou que la loi ne l'exige. cyberSanté Ontario n'utilise ni ne divulgue les RPS, selon la définition de ces termes dans la LPRPS, à ses propres fins. On ne doit conserver les RPS qu'aussi longtemps que nécessaire pour la réalisation des finalités déterminées.

8.1 Utilisation des RPS par cyberSanté Ontario

cyberSanté Ontario n'utilise les RPS que sous la direction des DRS auxquels elle fournit des services lorsqu'elle agit en tant que mandataire aux termes de la LPRPS.

Les activités qui suivent sont considérées comme étant des utilisations permises et nécessaires des RPS par cyberSanté Ontario :

- le traitement des RPS dans le but de créer et de tenir des DSE;
- le traitement des RPS afin de vérifier la préproduction;
- l'accès imprévu aux RPS aux fins de fournir des services incluant l'entretien, le soutien, les enquêtes sur les incidents et la surveillance (voir la section 8.4).

Les utilisations permises et nécessaires des RPS doivent être établies à l'aide d'accords entre cyberSanté Ontario et les DRS et guidées en tout temps par des exigences pertinentes de la LPRPS.

8.2 Divulgence des RPS par cyberSanté Ontario

cyberSanté Ontario ne doit divulguer les RPS qu'à la demande des DRS auxquels elle fournit des services lorsqu'elle agit à titre de mandataire aux termes de la LPRPS, ou lorsque celle-ci le permet ou l'exige.

Selon la LPRPS et son règlement, lorsque les RPS sont fournis à cyberSanté Ontario par un DRS aux fins de créer et de tenir un ou plusieurs DSE, on ne considère pas que le DRS *divulgue* les RPS à cyberSanté Ontario, ni que cette dernière *recueille* les RPS, selon la définition de ces termes dans la LPRPS.

cyberSanté Ontario ne *divulgue* pas de RPS aux DRS lorsqu'elle crée ou tient un ou plusieurs DSE. cyberSanté Ontario reçoit des RPS des DRS et en envoie aux DRS autorisés à des fins de prestation ou d'aide à la prestation des services de soins de santé.

8.3 Conservation des RPS par cyberSanté Ontario

cyberSanté Ontario ne doit conserver les RPS qu'à la demande des DRS auxquels elle fournit des services lorsqu'elle agit à titre de mandataire aux termes de la LPRPS.

cyberSanté Ontario conserve les RPS pendant le temps exigé par les DRS, selon les exigences réglementaires et des politiques des DRS dans une mesure raisonnable et pratique. Les exigences relatives à la conservation des RPS sont stipulées dans les accords conclus entre cyberSanté Ontario et les DRS et dans la *Politique sur la conservation des données* de cyberSanté Ontario.

8.4 Contrôle d'accès

Les contrôles d'accès servent à empêcher l'accès non autorisé ou inapproprié aux RPS, à assurer la protection des services de cyberSanté Ontario, à prévenir l'accès non autorisé aux ordinateurs, à détecter les activités non autorisées ou inappropriées et à assurer la sécurité de l'information.

cyberSanté Ontario n'autorise l'accès aux RPS qu'à des personnes autorisées en se fondant sur le principe de droit d'accès minimal, ce qui signifie que seuls les membres du personnel qui doivent accéder aux RPS y ont accès et qu'ils n'obtiennent ce droit d'accès qu'aux RPS dont ils ont besoin pour satisfaire aux exigences de leur travail.

cyberSanté Ontario doit s'assurer que le contrôle d'accès est fondé sur les rôles et responsabilités. Elle doit maintenir une matrice de contrôle d'accès qui illustre les rôles pour les types d'accès aux RPS. Les privilèges d'accès pour chaque rôle doivent inclure les détails sur l'information ou le service auquel on peut accéder ainsi que le type de l'accès permis (p. ex. lecture seulement, lecture et mise à jour).

cyberSanté Ontario doit établir les raisons de l'accès et les méthodes d'accès aux RPS dans les accords conclus avec les DRS et les tiers fournisseurs de services.

8.4.1 Accès par les membres du personnel de cyberSanté Ontario

La plupart des membres du personnel de cyberSanté Ontario n'ont jamais accès aux RPS que fournissent les DRS lorsqu'ils utilisent les services de cyberSanté Ontario. Cependant, dans tout milieu de technologie de l'information, un nombre limité de membres du personnel spécialisé peut devoir accéder ou obtenir un accès fortuit à de l'information sensible telle que les RPS, afin de fournir des services techniques ou de soutien à des clients. À titre d'exemple, les membres du personnel de cyberSanté Ontario peuvent avoir un accès fortuit aux RPS lorsqu'ils recherchent la cause d'une panne du système d'un client.

cyberSanté Ontario n'accorde l'accès aux RPS par son personnel autorisé que pour des utilisations permises et autorisées des RPS, telles que décrites dans la section 8 de la présente politique. Il est interdit au personnel de cyberSanté Ontario d'accéder aux RPS à d'autres fins.

cyberSanté Ontario veille à la mise en œuvre de la séparation des tâches relatives à la technologie de l'information afin de gérer le conflit d'intérêts, l'apparence de conflit d'intérêts et la fraude.

L'équipe des Opérations de sécurité de cyberSanté Ontario tient une liste des rôles à attribuer au personnel aux fins de contrôler l'accès aux dépôts des sources d'information.

cyberSanté Ontario maintient des procédures afin de s'assurer de ce qui suit :

- après avoir eu une entrevue, avoir été embauché ou avoir obtenu un travail contractuel, les membres du personnel sont au courant de la nécessité de maintenir la confidentialité et la sécurité de l'information grâce à une référence explicite dans les descriptions de travail et les contrats;
- à l'embauche ou à l'attribution d'un contrat, le personnel se voit attribuer uniquement les privilèges d'accès nécessaires afin d'accomplir leurs fonctions professionnelles;
- dans le cadre de leur emploi ou de leur contrat, les privilèges d'accès accordés au personnel sont examinés périodiquement afin de s'assurer qu'ils sont toujours exigés;
- immédiatement après un changement d'emploi ou de contrat, les privilèges d'accès accordés sont examinés afin d'en établir la pertinence;
- immédiatement après la cessation d'emploi ou de contrat, l'accès à tous les dépôts d'information est rapidement annulé.

Le personnel de cyberSanté Ontario qui exige l'accès au fonds de renseignements d'une région éloignée doit obtenir l'approbation du Bureau de protection de la vie privée et de l'équipe de la sécurité de l'information et remplir une *Remote Access Privacy Checklist* (liste de vérification d'accès à distance aux renseignements personnels) avant de se voir accorder un accès à distance.

8.4.2 Consignation de l'accès

cyberSanté Ontario conserve un dossier électronique des accès à l'ensemble ou à une partie des RPS contenus dans un DSE et s'assure que le dossier précise le nom de la personne qui a accédé à l'information, ainsi que la date, l'heure et l'endroit de l'accès.

cyberSanté Ontario rend disponibles à un DRS, sur demande, les rapports de consignation relatifs à l'accès aux RPS dont il a la garde et/ou le contrôle.

Une personne autorisée est celle qui demande l'accès aux RPS dans le cadre de ses tâches et qui possède un niveau approprié d'autorité, de formation et de filtrage de sécurité pour justifier l'accès.

Les personnes autorisées auxquelles on a accordé l'accès aux RPS sont responsables de la protection de la confidentialité de ces renseignements et de la vie privée des personnes qui en font l'objet. Elles doivent également utiliser ces renseignements de façon responsable, conformément aux lois, règlements, politiques et accords contractuels qui s'appliquent afin de garantir la sécurité et l'intégrité des RPS.

Les membres du personnel de cyberSanté Ontario qui peuvent avoir accès aux RPS dans le cadre de leurs tâches doivent avoir obtenu une formation sur la protection de la vie privée et la sécurité fondée sur leur rôle avant d'obtenir l'accès à des systèmes contenant des RPS.

8.4.3 Accès par les utilisateurs finaux

Un utilisateur final est un DRS ou une personne qui est autorisée par un DRS à utiliser un service de cyberSanté Ontario. Cette dernière maintient un processus d'enregistrement des utilisateurs finaux qui est observé pour chacun d'eux avant d'obtenir un compte et un accès aux RPS. Les exigences en matière de vérification de l'identité des utilisateurs finals comprennent :

- la saisie exacte de l'identité de l'utilisateur final (p. ex. nom, date de naissance, adresse actuelle, identificateur des professionnels de la santé);
- la vérification de l'identité à l'aide d'un mécanisme fiable;
- la saisie exacte, après vérification, des titres de compétence professionnelle durables (p. ex. spécialité médicale et/ou appellation d'emploi);
- l'attribution d'un identificateur d'utilisateur formel.

cyberSanté Ontario gère et ferme les comptes des utilisateurs finaux conformément aux lignes directrices établies par la sécurité de l'information. cyberSanté Ontario veille à ce qu'une authentification stricte soit exigée pour l'accès des utilisateurs finaux aux RPS. Une authentification à deux facteurs signifie que, pour accéder au système de cyberSanté Ontario, l'utilisateur final doit avoir un mot de passe et un autre mécanisme d'authentification, tel qu'un jeton d'accès.

8.4.4 Accès par les fournisseurs de services

cyberSanté Ontario définit l'accès autorisé aux RPS pour les fournisseurs de services par le biais de ses accords avec ceux-ci. Les tiers fournisseurs de services ayant accès aux RPS seront assujettis aux mêmes conditions et contraintes, le cas échéant, que le personnel de cyberSanté Ontario relativement au traitement des RPS. Ces conditions incluent la signature d'accords de confidentialité, la participation à une formation en matière de sensibilisation à la protection des renseignements personnels et à la sécurité, une approbation explicite de l'accès à distance, etc.

cyberSanté Ontario attribue des identifiants d'accès uniques à chaque fournisseur de services ayant accès aux RPS dans ses systèmes. Les fournisseurs de services n'ont pas la permission de communiquer ces identifiants.

9 Sixième principe : Exactitude

Le principe d'exactitude signifie que les RPS doivent être aussi exacts, complets et à jour que nécessaire aux fins de leur utilisation.

Le DRS qui recueille les RPS est responsable de leur exactitude. Toutes les corrections ou les changements aux RPS doivent être effectués uniquement par le DRS qui en a la garde et/ou le contrôle.

cyberSanté Ontario, dans la mesure du possible, fournit des mécanismes aux DRS pour appuyer l'entrée exacte des RPS dans ses systèmes (comme le contrôle de la validation des données d'entrée). cyberSanté Ontario maintient, à l'aide de ses pratiques de sécurité de l'information, des mécanismes pour protéger l'intégrité des RPS (voir la section 10 ci-après).

cyberSanté Ontario veille à ce que l'intégrité des RPS qui lui sont envoyés par les DRS soit maintenue et protégée sur place et en transit. L'intégrité signifie que les RPS n'ont pas été modifiés par inadvertance ou autrement, et qu'on peut s'y fier aux fins pour lesquelles ils ont été recueillis.

cyberSanté Ontario fournit un mécanisme aux DRS afin qu'ils inscrivent un avis de désaccord dans le DSE relativement à l'exactitude des RPS du DSE.

10 Septième principe : Mesures de sécurité

Le principe des mesures de sécurité signifie que les RPS doivent être protégés par des mesures de sécurité convenant à la sensibilité des renseignements.

10.1 Mécanismes de sécurité

Des procédures et des contrôles de la sécurité de l'information sont essentiels à la protection de la confidentialité des RPS, tout en permettant aux professionnels de la santé d'accéder à l'information dont ils ont besoin pour prendre des décisions relatives aux soins aux patients. cyberSanté Ontario dispose d'une Politique sur la sécurité de l'information très importante qui fournit un cadre stratégique élaboré pour la protection de tous les renseignements sur la santé, particulièrement les RPS.

Les politiques et les procédures sur la sécurité de l'information de cyberSanté Ontario précisent la façon dont elle protège les RPS. Cette protection comprend des mécanismes de sécurité administratifs, techniques et physiques appropriés au niveau de sensibilité de l'information, incluant :

- le cryptage obligatoire des RPS en transit ou sur des appareils mobiles;
- des évaluations de la menace et des risques (EMR);
- l'enregistrement des vérifications;

- la surveillance;
- le contrôle de l'accès et les rapports de connexions;
- la formation en matière de sécurité;
- la destruction sécuritaire des dossiers.

cyberSanté Ontario met en œuvre des mesures pour protéger les RPS d'un accès, d'une divulgation, de copies, d'une utilisation, de modifications, de perte ou de destruction non autorisés, peu importe le format ou le support dans lequel ils sont stockés.

Les exigences de cyberSanté Ontario relativement aux mécanismes de sécurité administratifs, techniques et physiques pour protéger les RPS sont détaillées dans sa *Politique sur la sécurité de l'information* affichée sur son site Web.

cyberSanté Ontario donne aux DRS et au public une description générale de ses services et des mesures de sécurité qu'elle a instaurées pour protéger l'intégrité, la sécurité et la confidentialité des RPS. On peut trouver ces renseignements sur le site Web de cyberSanté Ontario.

10.2 Surveillance de la conformité

cyberSanté Ontario veille à ce que les personnes ayant accès aux RPS par l'entremise de ses services se conforment à la LPRPS, à son Règlement, ainsi qu'aux politiques et procédures de cyberSanté Ontario.

Plus particulièrement, cyberSanté Ontario surveille la conformité :

- du personnel aux politiques et procédures internes de cyberSanté Ontario;
- des fournisseurs de services aux obligations contractuelles établies dans les accords.

cyberSanté Ontario fournit des mécanismes et des services aux DRS pour les aider à respecter leurs obligations en matière de surveillance de la conformité (p. ex. les rapports sur les listes de contrôle relativement à tous les RPS sous la garde du DRS).

cyberSanté Ontario mène des examens sur la conformité à la protection des renseignements personnels selon le calendrier proposé par le chef de la protection des renseignements personnels et acceptés ou dirigés par le Comité de vérification du Conseil d'administration de cyberSanté Ontario.

cyberSanté Ontario peut imposer des sanctions aux membres de son personnel ou à des tiers agissant au nom de cyberSanté Ontario qui ont enfreint cette politique, conformément aux politiques et procédures disciplinaires et d'approvisionnement de l'organisme, jusques et y compris une sanction civile, des sanctions pénales ainsi que le congédiement ou la résiliation de contrat.

cyberSanté Ontario offre aux membres de son personnel un moyen de signaler leurs préoccupations en matière de protection des renseignements personnels à titre confidentiel et de

s'assurer que des mesures sont prises de façon à ce qu'ils ne fassent pas l'objet de représailles (voir la *Procédure des plaintes et des enquêtes* de cyberSanté Ontario) pour obtenir plus de détails.

cyberSanté Ontario emploie des processus automatisés et manuels qui, s'il y a lieu, visent à *prévenir* plutôt qu'à *exposer* les incidents de non-conformité.

cyberSanté Ontario doit exécuter une série de processus de surveillance systématiques et transparents, y compris mais de façon non limitative :

- un programme de consignation des vérifications afin de repérer les principales dimensions du traitement des RPS, incluant :
 - l'accès aux RPS par tous les rôles;
 - les transferts des RPS d'un DRS à un DRS;
 - les changements et les dérogations aux directives relatives au consentement;
- la surveillance des processus administratifs, incluant les autoévaluations, les visites informelles au hasard, les vérifications des processus (p. ex. des processus de gestion des incidents et des processus de traitement des plaintes);
- la gestion des contrats, incluant l'exercice opportun des clauses de vérification et de surveillance;
- l'exécution de la formation et de la sensibilisation en matière de respect de la vie privée;
- le renouvellement des accords et des énoncés de confidentialité d'utilisation acceptable;
- l'examen régulier des seuils de déclaration des listes de contrôle.

cyberSanté Ontario ne restreindra pas le compte rendu de la surveillance de la conformité seulement aux données techniques, mais aussi aux processus administratifs, à l'aide de paramètres tels que le temps pendant lequel les incidents sont confinés ou la fréquence de perfectionnement de la formation en matière de protection de la vie privée.

10.3 Évaluations de l'impact sur la protection de la vie privée

cyberSanté Ontario effectue des évaluations de l'impact sur la protection de la vie privée pour chacun de ses services qui comporte des RPS, conformément à sa *Politique d'évaluation de l'impact sur la protection de la vie privée*.

cyberSanté Ontario aborde tous les risques et toutes les questions établis dans ses évaluations de la façon la plus opportune possible, soit à l'aide de recommandations faisant partie des évaluations ou de plans de traitement des risques relatifs à la protection de la vie privée élaborés par cyberSanté Ontario en réponse aux conclusions des évaluations.

Les détails sur l'approche de cyberSanté Ontario relativement à l'exécution des évaluations de l'impact sur la protection de la vie privée et aux réponses à celles-ci figurent dans la *Politique d'évaluation de l'impact sur la protection de la vie privée*.

11 Principe 8 : Transparence

Le principe de transparence signifie qu'un organisme doit mettre à la disposition des personnes des renseignements précis sur ses politiques et pratiques de gestion des RPS.

Les RPS qui sont gérés par cyberSanté Ontario appartiennent à la personne qui fait l'objet de ces renseignements. cyberSanté Ontario a la responsabilité de faire preuve d'ouverture et de transparence sur la façon dont elle gère et protège les RPS et d'informer les personnes de leurs droits à la protection de la vie privée.

cyberSanté Ontario met à la disposition des DRS et du public :

- une approche en langage clair sur la LPRPS et ses règlements qui s'applique à cyberSanté Ontario;
- les rôles et les obligations de cyberSanté Ontario en vertu de la LPRPS et ses règlements;
- les droits des personnes en vertu de la LPRPS dans le contexte des politiques et procédures de cyberSanté Ontario (p. ex. l'accès aux renseignements personnels, la correction, les plaintes, les directives relatives au consentement);
- les politiques et procédures de cyberSanté Ontario relatives aux RPS (sans fournir des renseignements qui pourraient compromettre la sécurité des services de cyberSanté Ontario ou la confidentialité des RPS);
- les responsabilités relatives à la protection des RPS;
- une description en langage clair du DSE et une description générale des mesures de protection administratives, techniques et physiques en vigueur pour protéger le DSE et les RPS qu'il contient;
- les résumés des résultats des évaluations de l'impact sur la protection de la vie privée, au besoin.

cyberSanté Ontario examine les renseignements sur ses pratiques en matière de protection de la vie privée qu'elle met à la disposition du public sur une base annuelle et les met à jour au besoin ou à la demande du chef de la protection des renseignements personnels.

12 Principe 9 : Accès aux renseignements personnels

Le principe d'accès aux renseignements personnels signifie que, sur demande, une personne doit être informée de l'existence, de l'utilisation et de la divulgation de ses RPS et peut y avoir accès. Elle peut contester l'exactitude et l'intégralité de ces renseignements et les faire modifier, s'il y a lieu.

En vertu de la LPRPS, une personne a le droit d'accéder à un dossier de ses RPS qui est sous la garde et le contrôle d'un DRS (tel un médecin ou un hôpital). En réponse à une demande écrite d'accès, le DRS doit accorder cette permission et donner l'accès ou le refuser, en se fondant sur une série

d'exceptions énumérées dans la LPRPS. Les personnes ont également le droit de demander au DRS de corriger tout renseignement inexact ou incomplet.

En vertu des dispositions de la LPRPS, cyberSanté Ontario n'est pas responsable des demandes individuelles d'accès ou de corrections aux RPS. Si cyberSanté Ontario reçoit une demande d'accès ou de correction, elle doit renvoyer la personne au DRS approprié pour répondre à sa demande.

13 Principe 10 : Possibilité de porter plainte contre le non-respect des principes

Le principe consistant à porter plainte contre le non-respect des principes signifie qu'une personne doit être en mesure de se plaindre du non-respect des principes de protection de la vie privée en communiquant avec la ou les personnes responsables de les faire respecter au sein de l'organisme.

13.1 Plaintes relatives à cyberSanté Ontario

Toute personne peut soumettre une plainte et/ou d'autres commentaires (incluant des demandes de renseignements, des compliments et des suggestions) sur les sujets suivants :

- les pratiques de protection des renseignements personnels et des données de cyberSanté Ontario;
- les pratiques de gestion de l'information de cyberSanté Ontario;
- la non-conformité aux politiques de cyberSanté Ontario ou aux exigences de la loi ou des règlements.

Les plaintes et/ou autres commentaires peuvent être soumis et livrés par porteur, par la poste, par télécopieur, par courriel et par téléphone en utilisant les coordonnées suivantes :

Bureau de protection de la vie privée
cyberSanté Ontario
C.P. 148
777, rue Bay, bureau 701
Toronto (Ontario) M5G 2C8
Télec. : 416 586-6598
Courriel : privacy@ehealthontario.on.ca
Téléphone : 416 946-4767

cyberSanté Ontario accepte les plaintes et/ou autres commentaires anonymes. Cependant elle exige le nom et l'adresse de l'expéditeur, son numéro de téléphone ou son adresse électronique afin de lui envoyer une réponse.

cyberSanté Ontario affiche un formulaire sur son site Web que quiconque peut utiliser pour présenter une plainte confidentielle. Ce formulaire indique les délais exigés pour que cyberSanté Ontario amorce une enquête.

Les RPS ne doivent pas accompagner la description de la plainte ou d'autres commentaires. Cependant, cyberSanté Ontario peut demander ce niveau de détail pendant son enquête. Ce faisant, cyberSanté Ontario obtient le consentement approprié exigé.

Le directeur de la protection de la vie privée examine toutes les plaintes et/ou autres commentaires. cyberSanté Ontario appontera les changements à ses politiques et pratiques en se fondant sur les commentaires reçus.

cyberSanté Ontario accuse réception d'une plainte et/ou d'autres commentaires dans les cinq jours ouvrables suivant leur réception.

cyberSanté Ontario envoie une réponse relative au résultat de l'enquête à l'expéditeur dans les 30 jours ouvrables suivant la réception de la plainte et/ou d'autres commentaires. En cas de retard à envoyer la réponse, la personne sera prévenue par la poste du délai approximatif prévu.

Le chef de la protection des renseignements personnels maintient les procédures pour recevoir, transmettre, gérer, fermer et surveiller les plaintes et d'autres commentaires et les afficher sur son site Web. On peut également se procurer des exemplaires de ces procédures auprès du chef de la protection des renseignements personnels.

12.1 Plaintes relatives aux DRS

Si on communique avec cyberSanté Ontario relativement à une plainte contre les pratiques de gestion de l'information d'un DRS, elle sera acheminée au DRS approprié.

Si, selon cyberSanté Ontario, une plainte relative à un DRS peut avoir une influence sur la gestion du contrat et les activités de surveillance de la conformité, l'organisme peut choisir d'assurer le suivi de l'enquête et de l'atténuation d'une plainte relative à un DRS.

12.2 Plaintes au CIPVP

Le Commissaire à l'information et à la protection de la vie privée/Ontario (CIPVP) est un organisme de surveillance chargé d'informer le public de ses droits en vertu des lois sur la protection de la vie privée et de veiller à ce que les organismes respectent leurs obligations en vertu de la loi. Le CIPVP est nommé par l'Assemblée législative de l'Ontario et indépendant du gouvernement au pouvoir.

Les personnes peuvent déposer une plainte auprès du CIPVP si :

- elles estiment qu'on leur a refusé injustement l'accès à leurs RPS;
- un DRS a refusé d'apporter une correction demandée à leurs RPS;
- plus de 30 jours se sont écoulés depuis la demande d'accès ou de correction et la personne n'a pas obtenu de décision;
- elles ont l'impression que l'estimation des honoraires du DRS est excessive.

Toutes les plaintes au CIPVP doivent être formulées par écrit. Les plaignants potentiels doivent soit écrire une lettre au CIPVP ou remplir le formulaire affiché sur son site Web: www.ipc.on.ca/docs/cudfrm-e.pdf . Le formulaire ne peut pas être transmis électroniquement. Il doit être imprimé et posté au registraire du CIPVP. Toute documentation pertinente doit être jointe au formulaire de plainte.

Les plaignants ont un an à partir du moment où ils ont constaté le problème pour déposer une plainte. Dans le cas des plaintes relatives à l'accès et à la correction, les plaignants ont un délai de six mois à partir du moment où ils reçoivent une décision du DRS pour déposer ces plaintes.

Les plaintes doivent être envoyées au :

Commissaire à l'information et à la protection de la vie privée/Ontario
2, rue Bloor Est, bureau 1400
Toronto (Ontario) M4W 1A8
Téléphone : 416 326-3333 • 1 800 387-0073
Télécopieur : 416 325-9195
ATS : 416 325-7539
Site Web : <http://www.ipc.on.ca/french/home-page/default.aspx>

14 Approbation et examen des politiques

Lorsqu'il existe une divergence ou un écart entre la présente politique et la loi ou le règlement, la loi ou le règlement doivent prévaloir. Lorsqu'il existe une divergence ou un écart entre cette politique et les politiques secondaires de protection des renseignements personnels et des données de cyberSanté Ontario, la présente politique prévaut.

La présente politique sera mise à jour ou révisée annuellement ou plus fréquemment, au besoin, avec l'approbation du chef de la protection des renseignements personnels.

Tous les membres du personnel de cyberSanté Ontario et les tiers fournisseurs de services retenus par cyberSanté Ontario sont responsables du traitement des RPS conformément à cette politique et à la loi qui s'applique. La conformité sera vérifiée de façon constante par le chef de la protection des renseignements personnels.

15 Glossaire

Terme	Définition
Mandataire	Même signification que la définition de la LPRPS et, en général, signifie une personne ou un organisme qui agit au nom du DRS, en matière de collecte, d'utilisation ou de divulgation des RPS qui sont sous la garde du DRS, avec l'autorisation de ce dernier et non à ses propres fins.
Personne autorisée	Une personne qui exige l'accès aux RPS dans le cadre de ses tâches et qui a un niveau d'autorité, de formation et de contrôle de sécurité approprié justifiant cet accès.

Terme	Définition
Entrepôt de données	Un partitionnement logique des données où sont stockées plusieurs bases de données qui s'appliquent à des applications ou à des séries d'applications définies. À titre d'exemple, plusieurs bases de données qui appuient les demandes de soins de santé pourraient être stockées dans un seul entrepôt de données sur les soins de santé.
Responsable des données	Une personne chargée de la gestion et de la surveillance d'un entrepôt de données sur les RPS.
Magasin de données	Un endroit où les données sont entreposées, données au repos. Ce terme inclut les bases de données et les fichiers plats.
Services de cyberSanté	Un ou plusieurs services visant à promouvoir la prestation de services de soins de santé en Ontario qui utilisent des systèmes et des processus électroniques, la technologie de l'information et la technologie des communications pour faciliter la disponibilité et l'échange électroniques de renseignements relatifs aux questions de santé, incluant les renseignements personnels et les renseignements personnels sur la santé par les patients et entre eux, les fournisseurs de soins de santé et d'autres utilisateurs qui en ont la permission. (Règlement d'habilitation, art. 1)
Dossier de santé électronique (DSE)	Même signification que celle définie dans la LPRPS et signifie généralement un dossier de RPS en format électronique créé et tenu par cyberSanté Ontario.
Fournisseur de services électroniques (FSE)	Même signification que celle définie dans la LPRPS et signifie généralement un tiers retenu par un DRS pour aider à fournir des services à un DRS. Ces services visent à permettre à un DRS d'utiliser des moyens électroniques pour recueillir, utiliser, modifier, divulguer, conserver ou éliminer des RPS.
Utilisateur final	Une personne qui est autorisée par un DRS à utiliser un service de cyberSanté Ontario.
Gestion interne des incidents touchant la sécurité et la protection de la vie privée (ESPIM)	Plan, processus et capacité de cyberSanté Ontario servant à d'établir, contenir, trier, transmettre de façon efficace et efficiente les incidents touchant la sécurité et la protection de la vie privée et d'y remédier afin de réduire au minimum l'impact de tels incidents.
Dépositaire de renseignements sur la santé (DRS)	Même signification que celle définie dans la LPRPS et signifie généralement une personne ou un organisme qui fournit des services de soins de santé. Les médecins, les hôpitaux, les pharmacies, les laboratoires, les centres d'accès aux soins communautaires et le MSSLD sont des DRS. cyberSanté Ontario n'est pas un DRS.
Fournisseur d'un réseau d'information sur la santé (FRIS)	Même signification que celle définie dans la LPRPS et signifie généralement un organisme qui fournit des services à un ou plusieurs DRS principalement pour leur permettre d'utiliser des moyens électroniques pour divulguer des RPS entre eux.
Gestionnaire de l'information (GI)	Terme utilisé pour décrire le rôle de cyberSanté Ontario lorsqu'elle crée ou tient un ou plusieurs dossiers de santé électroniques en vertu de l'article 6.2 de la LPRPS, Règl. de l'Ont. 339/04.
Renseignements personnels sur la santé (RPS)	Même signification que celle définie dans la LPRPS et signifie généralement les renseignements sur une personne sous forme orale ou enregistrée, si ces renseignements ont trait à sa santé physique ou mentale. Entre autres exemples, les antécédents familiaux en matière de santé, le numéro de carte Santé et toute autre information propre une personne et qui la relie à un fournisseur de soins de santé.
Loi de 2004 sur la protection des renseignements personnels sur la santé, chapitre 3. (LPRPS)	Une loi provinciale sur la protection des renseignements personnels sur la santé qui établit des règles pour la gestion des RPS et la protection de la confidentialité de ces renseignements, tout en facilitant la prestation efficace des services de soins de santé.

Terme	Définition
Personnel	Employés et personnel temporaire de cyberSanté Ontario (entrepreneurs, personnel d'agence temporaire, participants au Programme d'enseignement coopératif et personnes détachées.) Les entrepreneurs sont des personnes fournies par une entreprise pour une période précise de plus de trois mois pour occuper un emploi permanent à plein temps temporairement, au jour le jour, et qui sont gérés directement par la direction de cyberSanté Ontario.
Évaluation de l'impact sur la protection de la vie privée (ÉIPVP)	Une évaluation détaillée entreprise afin d'évaluer les répercussions d'un service nouveau ou modifié de façon importante dans le but de déterminer son impact réel et potentiel sur la protection des renseignements personnels et les RPS inclus dans le service. Cette évaluation mesure la conformité à la loi sur la protection des renseignements personnels qui s'applique et les répercussions plus vastes à ce chapitre. L'évaluation aborde tous les éléments techniques, les processus administratifs, le cheminement des renseignements personnels, les contrôles de gestion de l'information et les processus des ressources humaines liés à un service et établit des façons dont les risques d'entrave à la vie privée qui y sont liés peuvent être atténués.
Incident touchant la protection de la vie privée	Un incident touchant la protection de la vie privée inclut des circonstances où il y a une contravention aux politiques, aux procédures ou aux pratiques de protection de la vie privée mises en œuvre par cyberSanté Ontario ou aux accords conclus par cyberSanté Ontario avec des intervenants externes et des tiers fournisseurs de services, y compris mais non exclusivement à la LPRPS, aux accords avec les mandataires, aux accords d'échange de données, aux accords confidentialité et de non-divulgaration ainsi qu'aux accords avec les tiers fournisseurs de services retenus par cyberSanté Ontario, lorsque cette contravention ne constitue pas une non-conformité à la loi relative au respect de la vie privée qui s'applique. Un incident touchant la protection de la vie privée peut aussi être soupçonné d'être une infraction à la protection de la vie privée.
Évaluation du seuil de protection de la vie privée	Une analyse préliminaire, normalisée, d'évaluation de la protection de la vie privée utilisée pour déterminer si un service nécessitera ou non une évaluation plus poussée à ce chapitre.
Tiers fournisseur de services	Une personne ou une entité à laquelle cyberSanté attribue un contrat pour agir au nom de l'organisme et aider à la prestation des services de celle-ci. Ce terme inclut les fournisseurs et les consultants.

16 Références et documents connexes

- *Loi de 2004 sur la protection des renseignements personnels sur la santé (LPRPS)*
- *Politique sur la protection de la vie privée et des données de cyberSanté Ontario*
- *eHealth Ontario Privacy Impact Assessment Policy (Politique d'évaluation de l'impact sur la protection de la vie privée de cyberSanté Ontario)*
- *eHealth Ontario Privacy Incident Management Policy (Politique de gestion des incidents touchant la protection de la vie privée de cyberSanté Ontario)*
- *Procédure des plaintes et des enquêtes en matière de vie privée de cyberSanté Ontario*
- *eHealth Ontario Privacy Policy on the Responsibilities of Third Party Service Providers (Politique sur les responsabilités des tiers fournisseurs de services en matière de protection des renseignements personnels)*
- *eHealth Ontario Standard of Conduct (Norme de conduite de cyberSanté Ontario)*

- *eHealth Ontario Information Security policies and procedures* (Politiques et procédures sur la sécurité de l'information de cyberSanté Ontario)