eHealth Ontario

Politique sur la protection des renseignements personnels sur la santé

Bureau de la protection de la vie privée

Identificateur de document : 2478

Version : 6.3

Propriétaire : Directrice de la protection de la vie privée

Niveau de confidentialité : Faible

Ontario
eHealth Ontario

Table des matières

1 But et objectif 1

2 Portée 1

3 Aperçu de la LPRPS 2

3.1 Généralités 2

3.2 Dépositaire de renseignements sur la santé 2

3.3 Règlement de l'Ontario 329/04 (LPRPS) 3

3.4 Fournisseur d'un réseau d'information sur la santé 3

3.5 Fournisseur de services électroniques 3

3.6 Mandataire 3

4 Politique 4

4.1 Principe 1 : Responsabilité 4

4.1.1 Responsabilité de cyberSanté Ontario 4

4.1.2 Accords 5

4.1.3 Gestion de l'information 6

4.1.4 Surveillance de la conformité 6

4.1.5 Gestion des incidents et des violations touchant la protection de la vie privée 7

4.1.6 Formation et sensibilisation 7

4.1.7 Norme de conduite 8

4.1.8 Responsabilité à l'égard du public et transparence 8

4.2 Principe 2 : Détermination des fins de la collecte de renseignements 8

4.3 Principe 3 : Connaissance et consentement 8

4.3.1 Rôle de cyberSanté Ontario dans la gestion du consentement 9

4.4 Principe 4 : Limitation de la collecte 9

4.5 Principe 5 : Limitation de l'utilisation, de la divulgation et de la conservation 9

4.5.1 Utilisation des RPS par cyberSanté Ontario 10

4.5.2 Divulgation des RPS par cyberSanté Ontario 10

4.5.3 Conservation des RPS par cyberSanté Ontario 10

4.5.4 Contrôle de l'accès 10

4.6 Principe 6 : Exactitude 12

4.7 Principe 7 : Mesures de sécurité 13

4.7.1 Mécanismes de sécurité 13

4.7.2 Surveillance de la conformité 13

4.7.3 Évaluation de l'impact sur la protection de la vie privée 14
4.8 Principe 8 : Transparence 14
4.9 Principe 9 : Accès aux renseignements personnels 15
4.10 Principe 10 : Possibilité de porter plainte en raison du non-respect des principes 15
4.10.1 Plaintes relatives à cyberSanté Ontario 15
4.10.2 Plaintes relatives aux DRS 16
4.10.3 Plaintes au CIPVP 16
5 Responsabilités 17
6 Glossaire 17
7 Références et documents connexes 20
8 Interprétation 21

Tableaux

Tableau 1: Politique sur la protection des renseignements personnels sur la santé – Glossaire 20
Tableau 2: Politique sur la protection des renseignements personnels sur la santé – Références et documents connexes 21

1 But et objectif

La présente politique sur la protection de la vie privée 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. Cela inclut, par exemple, les antécédents médicaux de la famille, le numéro de la carte Santé et tout renseignement permettant d'identifier une personne et de l'associer à un fournisseur de soins de santé.

cyberSanté Ontario s'engage à être un chef de file en matière de protection de la vie privée et à encourager la confiance de ses clients et du public. Par conséquent, les exigences énoncées dans la présente politique vont au-delà de 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.

2 Portée

La présente politique s'applique à tous les membres du personnel de cyberSanté Ontario et aux tiers fournisseurs de services dont les services sont retenus par cyberSanté Ontario aux fins d'exécuter ses activités et de fournir 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 :
  - à l'article 10
  - à l'article 17
- au *Règlement de l'Ontario 329/04* adopté en vertu de la LPRPS, et plus particulièrement :
  - à l'article 6
  - à l'article 6.1
  - à l'article 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 du Règlement de l'Ontario 329/4 de la LPRPS, comme modifié par le Règlement de l'Ontario 331/11 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 considéré comme rassemblant ou diffusant des RPS en créant ou en tenant des DSE. Cette modification s'applique à cyberSanté Ontario jusqu'au 1er janvier 2017, lors de l'expiration de l'article du règlement modifié ou jusqu'à ce qu'il en soit déterminé autrement.

Consulter la section 3 ci-après 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.

Lorsque le dépôt ou le système est régi par les politiques de confidentialité en matière de DSE, respectez les politiques et procédures appropriées décrites dans les *politiques de confidentialité des dossiers de santé électronique de cyberSanté Ontario.*

Application

La présente politique s'applique à tout le personnel de cyberSanté Ontario et aux tiers fournisseurs de services retenus. Elle s'applique à tous les services et activités de l'organisme susceptibles d'avoir une incidence sur la confidentialité des RPS confiés à cyberSanté Ontario. Les dispositions pertinentes de la présente politique seront abordées dans les accords de cyberSanté Ontario avec les tiers fournisseurs de services et les usagers finaux des services de cyberSanté Ontario.

Autres politiques

La présente politique sur la protection de la vie privée doit être consultée de concert avec la *Politique sur la protection des renseignements personnels 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 comprennent notamment :

- *Politique d'évaluation de l'impact sur la protection de la vie privée de cyberSanté Ontario*
- *Politique de gestion des incidents et des violations touchant la protection de la vie privée de cyberSanté Ontario*
- *Politique et procédure relative aux plaintes et aux demandes de renseignements liées à la protection de la vie privée de cyberSanté Ontario*
- *Politique et procédure relative à la gestion des risques liés à la protection de la vie privée de cyberSanté Ontario*
- *Politique de protection de la vie privée reliée aux responsabilités des tiers fournisseurs de services de cyberSanté Ontario*

3 Aperçu de la LPRPS

3.1 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 que l'organisme 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 (DRS), fournisseur de services électroniques (FSE) ou fournisseur de services à un FRIS. Chacun de ces rôles est axé sur la relation de cyberSanté Ontario avec un ou plusieurs dépositaires de renseignements sur la santé (DRS).

3.2 Dépositaire de renseignements sur la santé

Un DRS 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 des DRS. 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 dossiers

imprimés, les ordinateurs ou les systèmes de technologie de l'information), les patients sont les propriétaires de leurs RPS.

3.3 Règlement de l'Ontario 329/04 (LPRPS)

L'article 6.2 du Règlement de l'Ontario 329/04 pris en application 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.

3.4 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 du 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'il fournit des services. Cependant, le DRS doit rendre compte au patient des pratiques de confidentialité relatives aux RPS.

3.5 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.

3.6 Mandataire

En qualité de mandataire d'un DRS, cyberSanté Ontario agit pour ou au nom du DRS en matière de collecte, d'utilisation ou de 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.

4 Politique

La présente 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.

4.1 Principe 1 : 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.

4.1.1 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 engagé 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 chef de la direction l'autorité de mettre en œuvre des mesures de protection des renseignements personnels et des données chez cyberSanté Ontario. Celui-ci peut déléguer une personne qui agira en son nom et nomme la directrice ou le directeur de la protection de la vie privée.

La directrice ou le directeur de la protection de la vie privée est chargé de surveiller le Bureau de la protection de la vie privée de cyberSanté Ontario. Cette personne est chargée de mettre en œuvre les politiques et les programmes de protection de la vie privée de cyberSanté Ontario à l'échelle de l'organisme.

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 complet de formation et de sensibilisation du personnel et des tiers fournisseurs de services;
- 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 de la directrice ou du directeur de la protection de la vie privée consistent notamment à :

- veiller à ce que le Bureau de la 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 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 de cyberSanté Ontario*;
- 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;

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

- mettre en œuvre les recommandations des évaluations du seuil de protection de la vie privée ou des évaluations de l'impact sur la protection de la vie privée.

Le vice-président, 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 la directrice ou le directeur de la protection de la vie privée 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 et les tiers fournisseurs de services doivent 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 ou à ses tiers fournisseurs de services agissant en son nom qui enfreignent la présente politique selon les politiques et procédures disciplinaires et d'approvisionnement de l'organisme, et peut se prévaloir de mesures pouvant aller jusqu'au licenciement ou à la résiliation de contrat.

4.1.2 Accords

Les accords ont pour objet d'établir officiellement les rôles et responsabilités liés à la gestion et la 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 le personnel et les tiers fournisseurs de services de cyberSanté Ontario.

Les accords doivent porter, le cas échéant, 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 et des violations touchant la vie privée 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, le cas échéant).

En vertu de la LPRPS, lorsque cyberSanté Ontario agit aux termes de l'article 6.2 de la LPRPS, Règlement de l'Ontario 329/04 aux fins de créer et de maintenir 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 finaux, le MSSLD 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.

cyberSanté Ontario conserve et gère les accords par l'entremise 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 lié.

4.1.3 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 4.5.

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, en particulier en ce qui concerne les services de sécurité, mais aussi les services d'approvisionnement, les services juridiques, la gestion des risques et les 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 tient à jour le *Répertoire des dossiers de cyberSanté Ontario* qui est disponible sur le site Web de cyberSanté Ontario. cyberSanté Ontario examine périodiquement le *Répertoire des dossiers de cyberSanté Ontario* afin de veiller à ce que les renseignements qu'il contient soient exacts et complets.

cyberSanté Ontario doit veiller à ce que :

- la confidentialité des données contenues dans le *Répertoire des dossiers de cyberSanté Ontario* soit protégée adéquatement;
- l'accès soit limité aux membres du personnel ou aux tiers fournisseurs de services dont le rôle exige un tel accès;
- l'accès soit enregistré, y compris le nom de la personne qui a accédé aux renseignements, le motif de l'accès, ainsi que la date et l'heure de l'accès;
- les registres d'accès soient examinés périodiquement afin de veiller à ce que tout accès aux RPS soit encore pertinent, compte tenu des motifs invoqués;
- les dépôts de données ne soient maintenus que tant et aussi longtemps que les données continuent de servir aux fins pour lesquelles elles ont été recueillies.

4.1.4 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 l'organisme 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. La directrice de la protection de la vie privée présente régulièrement un compte rendu des résultats de la surveillance de la conformité au comité de direction de cyberSanté Ontario et, le cas échéant, au 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 4.6.

4.1.5 Gestion des incidents et des violations touchant la protection de la vie privée

cyberSanté Ontario prend toutes les mesures nécessaires afin de corriger tout accès, collecte, utilisation, divulgation, reproduction, modification, conservation ou élimination des RPS dans ses systèmes qui ne sont pas conformes à la loi pertinente, en particulier à la LPRPS, ou aux politiques et procédures de cyberSanté Ontario.

La *Politique de gestion des incidents et des violations touchant la protection de la vie privée de cyberSanté Ontario* décrit l'approche utilisée par l'organisme en matière de gestion des incidents et des violations touchant la protection de la vie privée. Le processus selon lequel un incident ou une violation touchant la protection de la vie privée et un incident lié à la sécurité sont confinés, examinés et corrigés est défini par le programme de gestion des incidents touchant la protection de la vie privée et le programme d'intervention relatifs aux incidents touchant la sécurité.

Conformément à la *Politique de gestion des incidents et des violations touchant la protection de la vie privée*, cyberSanté Ontario doit confiner les effets de l'incident ou de la violation en déterminant sa nature et sa portée et émettre tous les avis nécessaires par l'entremise d'un processus clair de communication et de paliers d'intervention, le premier avis étant envoyé au DRS ou aux DRS qui ont la garde réelle des RPS visés par l'incident ou la violation.

4.1.6 Formation et sensibilisation

cyberSanté Ontario s'engage à encourager une culture solide de sensibilisation à la protection de la vie privée au sein de son personnel et parmi les tiers fournisseurs de services. Par conséquent, l'organisme a mis en place 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 et aux tiers fournisseurs de services :

- un aperçu de la LPRPS 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 des incidents et des violations 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 de la directrice de la protection de la vie privée. 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 la directrice de la protection de la vie privée juge appropriée.

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

cyberSanté Ontario doit 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 du personnel de cyberSanté Ontario qui peuvent avoir accès aux RPS dans le cadre de leurs tâches doivent suivre une formation axée sur les rôles 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'il offre (p. ex., les politiques relatives à la gestion des incidents et des violations touchant la protection de la vie privée). Les tiers fournisseurs de services de cyberSanté Ontario doivent suivre la formation en matière de protection de la vie privée et de sécurité donnée par cyberSanté Ontario.

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.

4.1.7 Norme de conduite

Tous les membres du personnel de cyberSanté Ontario et les tiers fournisseurs de services doivent reconnaître et accepter formellement la *Norme de conduite en matière de confidentialité et de sécurité de cyberSanté Ontario* avant le début de leur entrée en fonction au sein de l'organisme et annuellement par la suite.

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

4.1.8 Responsabilité à l'égard du public et transparence

cyberSanté tient à rendre son programme de protection de la vie privée et les mesures qu'il prend pour protéger les RPS aussi clairs et accessibles que possible. cyberSanté Ontario décrit en langage clair ses services et ses mesures de protection et, dans la présente politique, explique clairement la législation et les règlements pertinents, en particulier la LPRPS et le Règlement de l'Ontario 329/04 pris en application de la LPRPS.

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 la présente politique, aux sections 4.6, 4.7, 4.8 et 4.9.

4.2 Principe 2 : 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 4.5 de la présente politique. Le *Répertoire des dossiers 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'il gère.

4.3 Principe 3 : Connaissance et 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 ni coercition.

Une personne a le droit d'établir une directive relative au 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 relatives au consentement incluent :

- le retrait du consentement à partager ou à utiliser des RPS à des fins de soins de santé (ce qui entraîne le blocage du dossier du patient);
- le rétablissement du consentement à 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, d'utiliser et de 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.

4.3.1 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.

4.4 Principe 4 : 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 il fournit des services lorsqu'il agit à titre de mandataire aux termes de la LPRPS.

Lorsque cyberSanté Ontario crée ou maintient un ou plusieurs DSE, il 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.

4.5 Principe 5 : Limitation de l'utilisation, de la divulgation et de la conservation

Le principe de limitation de l'utilisation, de la divulgation 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.

cyberSanté Ontario ne doit pas fournir de RPS si d'autres renseignements, à savoir des renseignements anonymes ou des données agrégées, serviront aux fins recherchées. L'organisme ne doit pas non plus fournir davantage de RPS que ce qui est raisonnablement nécessaire pour atteindre le but recherché. Lorsque les RPS sont rendus anonymes, l'anonymisation sera effectuée conformément au document intitulé *De-identification Protocols: Essential for Protecting Privacy, 2014* du CIPVP, ou une autre norme comparable relative aux meilleures pratiques.

4.5.1 Utilisation des RPS par cyberSanté Ontario

cyberSanté Ontario n'utilise les RPS que sous la direction des DRS auxquels il fournit des services lorsqu'il 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 accessoire aux RPS aux fins de fournir des services incluant l'entretien, le soutien, les enquêtes sur les incidents et les violations et la surveillance (voir la section 4.5.4).

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.

4.5.2 Divulgation des RPS par cyberSanté Ontario

cyberSanté Ontario ne doit divulguer les RPS qu'à la demande des DRS auxquels il fournit des services lorsqu'il 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 maintenir un ou plusieurs DSE, on ne considère pas que le DRS *divulgue* les RPS à cyberSanté Ontario, ni que celui-ci *recueille* les RPS, selon la définition de ces termes dans la LPRPS.

cyberSanté Ontario ne *divulgue* pas de RPS aux DRS lorsqu'il 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.

4.5.3 Conservation des RPS par cyberSanté Ontario

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

Lorsqu'il agit à titre de mandataire ou de fournisseur de services électroniques, cyberSanté Ontario conserve les RPS pendant le temps exigé par les DRS, selon les exigences règlements 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.

- Les données conservées par cyberSanté Ontario au nom du MSSLD seront conservées pour une période indéterminée, conformément au document intitulé *Interim Electronic Health Record Data Retention Schedule* (30 septembre 2013) du MSSLD.

Lorsque cyberSanté Ontario crée ou maintient un ou plusieurs DSE, il conserve les DSE conformément à la *Politique de conservation des DSE*.

4.5.4 Contrôle de l'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 et les tiers fournisseurs de services 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. Il 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.

4.5.4.1 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, comme décrites dans la section 4.5 de la présente politique. L'autorisation est donnée par le Bureau de la protection de la vie privée par l'entremise du *processus de demande d'accès logique de cyberSanté Ontario*. 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 Services 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 a besoin d'accéder au fonds de renseignements à distance doit obtenir l'approbation du Bureau de protection de la vie privée et de l'équipe des Services de sécurité avant de se voir accorder un accès à distance.

4.5.4.2 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 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.

Il incombe aux personnes qui sont autorisées à consulter des RPS de protéger la nature confidentielle de ces renseignements et la vie privée des personnes sur qui portent ces renseignements. 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.

4.5.4.3 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.

cyberSanté Ontario 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 finaux 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 ou appellation d'emploi);
- l'attribution d'un identificateur d'utilisateur sans ambigüité.

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.

4.5.4.4 Accès par les fournisseurs de services

cyberSanté Ontario définit l'accès autorisé aux RPS pour les fournisseurs de services par l'entremise 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.

4.6 Principe 6 : 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 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 4.7 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.

4.7 Principe 7 : 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.

4.7.1 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 des renseignements de cyberSanté Ontario précisent la façon dont il 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 de 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'il a mis sur pied pour protéger l'intégrité, la sécurité et la confidentialité des RPS. On peut trouver ces renseignements sur le site Web de cyberSanté Ontario.

4.7.2 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 concernant la conformité en matière de protection des renseignements personnels selon le calendrier proposé par la directrice de la protection de la vie privée et accepté par le Comité de vérification du conseil d'administration de cyberSanté Ontario ou à la demande de ce dernier.

cyberSanté Ontario peut imposer des sanctions aux membres de son personnel ou à des tiers agissants au nom de cyberSanté Ontario qui ont enfreint la présente politique, conformément aux politiques et procédures disciplinaires et d'approvisionnement de l'organisme, jusqu'à 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, le cas échéant, 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 autre;
    - 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 violations 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 comme le temps nécessaire à confiner les incidents et les violations ou la fréquence de la mise à jour de la formation en matière de protection de la vie privée.

4.7.3 Évaluation de l'impact sur la protection de la vie privée

Conformément à sa *Politique d'évaluation de l'impact sur la protection de la vie privée*, cyberSanté Ontario procède à une évaluation de l'impact sur la protection de la vie privée (EIPVP) dans le cas de chaque service de cyberSanté Ontario en lien avec des RPS.

cyberSanté Ontario examine le plus rapidement possible tous les risques et enjeux cernés dans son EIPVP, à la lumière des recommandations de l'EIPVP ou des plans de traitement des risques relatifs à la protection de la vie privée élaborés par cyberSanté Ontario en réaction aux conclusions des EIPVP.

La *Politique d'évaluation de l'impact sur la protection de la vie privée de cyberSanté Ontario* fait état de l'approche de cyberSanté Ontario en matière de tenue et de suivi des EIPVP.

4.8 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 il 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 explication en langage clair des dispositions de la LPRPS et de son règlement qui s'appliquent à cyberSanté Ontario;
- les rôles et les obligations de cyberSanté Ontario en vertu de la LPRPS et son règlement;
- 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'il met à la disposition du public sur une base annuelle et les met à jour au besoin ou à la demande de la directrice de la protection de la vie privée.

4.9 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, le cas échéant.

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 (comme 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, il doit renvoyer la personne au DRS approprié pour répondre à sa demande.

4.10 Principe 10 : Possibilité de porter plainte en raison du non-respect des principes

Le principe consistant à porter plainte en raison du 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.

4.10.1 Plaintes relatives à cyberSanté Ontario

Toute personne peut soumettre une plainte ou des 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 ou 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 la protection de la vie privée
cyberSanté Ontario
C.P. 148
Toronto (Ontario) M5G 2C8
Télécopieur : 416 586-4397 ou 1 866 831-0107

Courriel : privacy@ehealthontario.on.ca
Téléphone : 416 946-4767 ou 1 888 411-7742, poste 64767

cyberSanté Ontario accepte les plaintes ou commentaires anonymes. Cependant il 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 des commentaires. Cependant, cyberSanté Ontario peut demander ce niveau de détail pendant son enquête. Ce faisant, cyberSanté Ontario obtient le consentement approprié exigé.

La directrice de la protection de la vie privée examine toutes les plaintes et tous les commentaires. cyberSanté Ontario modifiera ses politiques et ses pratiques en se fondant sur les commentaires reçus.

cyberSanté Ontario accuse réception d'une plainte ou de commentaires dans les quatre (4) 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 ou de commentaires. En cas de retard à envoyer la réponse, la personne sera prévenue par la poste du délai approximatif prévu.

La directrice de la protection de la vie privée 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 de la directrice de la protection de la vie privée.

4.10.2 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, la plainte sera acheminée au DRS approprié et le plaignant sera informé qu'il recevra une réponse directement de celui-ci.

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.

4.10.3 Plaintes au CIPVP

Le Commissaire à l'information et à la protection de la vie privée de l'Ontario (CIPVP) est un organisme de supervision qui est chargé de sensibiliser le public concernant ses droits à la protection de la vie privée et de veiller à ce que les organismes respectent leurs obligations aux termes de la loi. Le CIPVP est nommé par l'Assemblée législative de l'Ontario et indépendant du gouvernement au pouvoir.

Les particuliers peuvent déposer une plainte auprès du CIPVP si :

- ils 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;
- ils 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 http://www.ipc.on.ca/images/Resources/up-1cmpfrm_f.pdf. Le formulaire ne peut pas être transmis par voie électronique. 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 de l'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

5 Responsabilités

La directrice de la protection de la vie privée est considérée comme ayant le pouvoir final en matière d'interprétation, de mise en œuvre, d'exécution et de maintien de la présente politique.

La surveillance de la conformité à la présente politique est assurée par la directrice de la protection de la vie privée.

Tous les membres du personnel de cyberSanté Ontario et les tiers fournisseurs de services retenus par cyberSanté Ontario ont la responsabilité de traiter les RPS conformément à la présente politique et à la loi qui s'applique.

6 Glossaire

La terminologie et les acronymes suivants sont associés à la présente politique :

TERME	DÉFINITION
Mandataire	Même signification que la définition de la LPRPS et, en général, signifie une personne ou un organisme qui agit a 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.
Personnes autorisées	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.
Dépôt 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 dépôt de données sur les soins de santé.
Anonymisation	A la même signification que celle donnée dans la *Loi de 2004 sur la protection des renseignements personnels sur la santé* (LPRPS) et signifie généralement la suppression de tout renseignement permettant d'identifier une personne.

Dossiers de cyberSanté Ontario	Tout dossier créé dans le cadre des activités de cyberSanté Ontario.
Services de santé électronique	Un ou des services pour promouvoir la prestation de services de santé en Ontario utilisant des systèmes et des processus électroniques, des technologies de l'information et des technologies des communications pour faciliter l'accessibilité électronique et l'échange de renseignements reliés à des questions de santé, notamment des RP et des RPS, par et parmi les patients, les fournisseurs de soins de santé et d'autres utilisateurs autorisés. (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.
Dépositaire de renseignements sur la santé (DRS)	A la même signification que celle donnée à l'article 3 de la *Loi de 2004 sur la protection des renseignements personnels sur la santé* (LPRPS) et signifie généralement une personne ou une organisation qui offre des services de santé. Inclut, par exemple, les médecins, les hôpitaux, les pharmacies, les laboratoires, les centres d'accès aux soins communautaires et le ministère de la Santé et des Soins de longue durée, mais pas cyberSanté Ontario.
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.
Renseignements personnels sur la santé (RPS)	S'entend au sens de l'article de la *Loi de 2004 sur la protection des renseignements personnels sur la santé*, et il s'agit généralement de renseignements identificatoires concernant un particulier, qui se présentent sous forme verbale ou autre forme consignée, liés à la santé de cette personne ou à des services de santé fournis à ce particulier. Cela inclut, par exemple, les antécédents médicaux de la famille, le numéro de la carte Santé et tout renseignement permettant d'identifier une personne et de l'associer à un fournisseur de soins de santé.
***Loi de 2004 sur la protection des renseignements personnels sur la santé*, L.O. 2004,**	Une loi provinciale sur la protection des renseignements sur la santé qui définit des règles relatives à la gestion des renseignements personnels sur la santé et la protection de leur confidentialité, tout en facilitant la prestation des services de santé.

chap. 3 (LPRPS)

cyberSanté Ontario	Collectivement, les personnes suivantes : les employés actuels et les anciens employés; les fournisseurs actuels; les personnes nommées actuelles et les anciennes personnes nommées. Où : • Employé : S'entend d'une personne qui, par l'entremise de la signature d'un contrat de service, a conclu une relation d'emploi avec cyberSanté Ontario et est classée dans une des catégories suivantes, définies par le service de ressources humaines de cyberSanté Ontario : employé permanent à temps plein, employé temporaire à temps plein; employé permanent à temps partiel ou étudiant. • Fournisseur : Également appelé tiers fournisseur de services. S'entend d'un particulier ou d'une entité qui fournit des produits ou des services à cyberSanté Ontario, et qui est payé par l'entremise du système des comptes créditeurs de cyberSanté Ontario. • Personne nommée : S'entend d'un particulier nommé par le lieutenant-gouverneur en conseil comme membre du conseil d'administration de cyberSanté Ontario en vertu du Règlement de l'Ontario 43/02, « cyberSanté Ontario », pris en application de la *Loi de 1990 sur les sociétés de développement*, et ses modifications successives.
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 elle établit des façons dont les risques d'entrave à la vie privée qui y sont liés peuvent être atténués.
Violation touchant la protection de la vie privée	Une violation touchant la protection de la vie privée consiste en la collecte, l'utilisation ou la divulgation de RP ou de RPS faite de manière non conforme aux dispositions législatives concernant la protection de la vie privée, ou toute circonstance dans laquelle des RP et RPS sont volés ou perdus, ou sont recueillis, utilisés, divulgués, copiés, modifiés, conservés ou détruits de façon non autorisée ou inappropriée.
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 de confidentialité et de non-divulgation 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	Une analyse préliminaire, normalisée, d'évaluation de la protection de la vie privée utilisée

seuil de protection de la vie privée	pour déterminer si un service nécessitera ou non une évaluation plus poussée à ce chapitre.

Tableau 1: Politique sur la protection des renseignements personnels sur la santé – Glossaire

7 Références et documents connexes

Les documents qui suivent sont des textes législatifs de référence et des politiques de cyberSanté Ontario associés à la présente politique :

RÉFÉRENCE	EMPLACEMENT
Loi de 2004 sur la protection des renseignements personnels sur la santé et ses règlements	http://www.elaws.gov.on.ca/html/statutes/french/elaws_statutes_04p03_f.htm
Politique sur la protection de la vie privée et des données de cyberSanté Ontario	http://www.ehealthontario.on.ca/fr/privacy
Politique d'évaluation de l'impact sur la protection de la vie privée de cyberSanté Ontario	http://emerge/spaces/privacy/Documents/Forms/AllItems.aspx
Politique de gestion des incidents et des violations touchant la protection de la vie privée de cyberSanté Ontario	http://www.ehealthontario.on.ca/fr/privacy
Politique et procédure relative aux plaintes et aux demandes de renseignements liées à la protection de la vie privée de cyberSanté Ontario	http://www.ehealthontario.on.ca/fr/privacy
Politique de protection de la vie privée reliée aux responsabilités des tiers fournisseurs de services de cyberSanté Ontario	http://www.ehealthontario.on.ca/fr/privacy
Répertoire des dossiers de cyberSanté Ontario	http://www.ehealthontario.on.ca/fr/privacy
Politique et procédure relative à la gestion des risques liés à la protection de la vie privée de cyberSanté Ontario	http://emerge/spaces/privacy/Documents/Forms/AllItems.aspx
Politique de cyberSanté Ontario sur les demandes d'accès à l'information et la protection de la vie privée	http://emerge/spaces/privacy/Documents/Forms/AllItems.aspx
Norme de conduite en matière de protection de la vie privée et de sécurité pour les employés de cyberSanté Ontario	http://emerge/spaces/privacy/Documents/Forms/AllItems.aspx

Norme de conduite en matière de protection de la vie privée et de sécurité pour les fournisseurs de services de cyberSanté Ontario	http://emerge/spaces/privacy/Documents/Forms/AllItems.aspx
Politiques et procédures de sécurité de l'information de cyberSanté Ontario	http://emerge/spaces/privacy/Documents/Forms/AllItems.aspx
Politique sur la protection des dossiers de santé électronique de cyberSanté Ontario	http://www.ehealthontario.on.ca/fr/initiatives/resources/

Tableau 2: Politique sur la protection des renseignements personnels sur la santé – Références et documents connexes

8 Interprétation

Les exigences de la politique précédées de

- « doivent » ou « doit » sont obligatoires;
- « peuvent », « peut » ou « pouvant » sont optionnelles;
- « devraient » sont des recommandations.

En cas de divergence entre la présente politique et la *Loi sur l'accès à l'information et la protection de la vie privée*, la *Loi de 2004 sur la protection des renseignements personnels sur la santé*, les règlements aux termes de ces Lois, ou les règlements de l'organisme, les textes législatifs ou la réglementation ont préséance.

En cas de divergence entre la présente politique et toute autre politique de cyberSanté Ontario en matière de protection de la vie privée, la *Politique sur la protection de la vie privée et des données de cyberSanté Ontario* a préséance.