

***eHealth Ontario***

# Politique sur la protection de la vie privée

Bureau de la protection de la vie privée

Identificateur du document : 1194

Version : 9.4

Propriétaire : directrice de la protection de la vie privée

Niveau de confidentialité : Faible

## **Avis de droit d'auteur**

Copyright © cyberSanté Ontario, 2016.

## **Tous droits réservés.**

Aucune partie du présent document ne peut être reproduite d'une façon quelconque, y compris par photocopie ou transmission électronique vers un ordinateur, sans le consentement écrit préalable de cyberSanté Ontario. Les renseignements contenus dans le présent document appartiennent exclusivement à cyberSanté Ontario et ne peuvent être ni utilisés ni divulgués, sauf si cyberSanté Ontario l'autorise expressément par écrit.

## **Marques de commerce**

D'autres noms de produits mentionnés dans le présent document pourraient être des marques de commerce ou des marques déposées de leurs sociétés respectives et sont reconnus ainsi.

## Table des matières

---

1	But et objectif.....	1
2	Portée .....	1
3	Politique .....	2
3.1	Collecte de renseignements personnels par cyberSanté Ontario.....	2
3.2	Exigences en matière d’avis et de consentement.....	3
3.3	Utilisation des renseignements personnels .....	3
3.4	Divulgence de renseignements personnels par cyberSanté Ontario.....	3
3.5	Gestion des incidents et des violations.....	3
3.6	Obligation de procéder à des évaluations de l’impact sur la protection de la vie privée.....	3
3.7	Accès individuel aux renseignements personnels.....	4
3.8	Précision, intégrité et demandes de correction des renseignements personnels .....	4
3.9	Conservation et destruction des renseignements personnels .....	4
3.10	Banques de renseignements personnels.....	4
3.11	Gestion de l’information .....	5
4	Responsabilités .....	5
5	Glossaire.....	5
6	Références et documents connexes .....	8
7	Interprétation .....	9

## Tableaux

---

Tableau 1 : Politique sur la protection de la vie privée : Glossaire.....	7
Tableau 2 : Politique sur la protection de la vie privée : Références et documents connexes .....	9

---

# 1 But et objectif

La *Politique sur la protection de la vie privée de cyberSanté Ontario* vise à régir la collecte, l'utilisation et la divulgation de renseignements personnels (RP) de manière à faciliter les activités opérationnelles et la prestation des services de cyberSanté Ontario, tout en protégeant les droits et la vie privée du personnel et de la clientèle de cyberSanté Ontario, ainsi que du public.

cyberSanté Ontario est une « institution » selon la définition de la *Loi sur l'accès à l'information et la protection de la vie privée*, L.R.O. 1990, chap. F.31, (LAIPVP) modifiée, et est assujéti à ses dispositions. cyberSanté Ontario s'est engagé à protéger les RP assujéti à la LAIPVP et à élargir ses pratiques de protection de la vie privée à son traitement des RP lorsque ces renseignements peuvent ne pas être assujéti à des lois ou à des règlements sur la protection de la vie privée.

# 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 également aux renseignements sur des personnes identifiables sous la garde ou le contrôle de cyberSanté Ontario, peu importe le support, y compris l'information recueillie par l'entremise du site Web de cyberSanté Ontario. Elle régit l'accès, la collecte, l'utilisation, la divulgation, la conservation et l'élimination des RP qui se trouvent dans les dossiers de cyberSanté Ontario.

Aux fins de la présente politique, on a donné à l'expression « renseignements personnels » (RP) le même sens que celui donné à l'article 2 de la LAIPVP. Les coordonnées d'affaires du personnel de cyberSanté Ontario, à savoir le nom, le titre et l'adresse de travail des membres du personnel de cyberSanté Ontario, ne constituent pas des RP. La présente politique s'applique à tous les RP recueillis, utilisés et divulgués par cyberSanté Ontario, que ces RP soient assujéti ou non à la LAIPVP.

La présente politique ne tient pas compte des renseignements personnels sur la santé traités par cyberSanté Ontario, puisque cette modalité est définie dans la *Loi de 2004 sur la protection des renseignements personnels sur la santé*, L.R.O. 2004, chapitre 3, Annexe A, dans sa version modifiée (LPRPS), de l'Ontario. Les renseignements personnels sur la santé recueillis directement auprès d'une personne par cyberSanté Ontario, et non auprès d'un dépositaire de renseignements sur la santé, ne sont pas assujéti à la LPRPS.

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*. Cette politique s'inscrit dans une série de procédures courantes, de lignes directrices et de politiques subordonnées de cyberSanté Ontario qui, ensemble, constituent un programme global de protection des renseignements personnels. 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*

- *Politique de cyberSanté Ontario sur les demandes d'accès à l'information et la protection de la vie privée*
- Lorsque l'entrepôt ou le système est régi par les politiques de confidentialité en matière de dossiers de santé électronique (DSE), respectez les politiques et procédures appropriées décrites dans les *politiques de confidentialité des dossiers de santé électronique* de cyberSanté Ontario.

## 3 Politique

cyberSanté Ontario considère les RP sous sa garde ou son contrôle comme étant confidentiels et les rendra accessibles uniquement aux utilisateurs autorisés et en conformité à la LAIPVP. Sous réserve des limitations et exceptions, les personnes (ou leurs mandataires autorisés) peuvent avoir accès aux renseignements personnels figurant dans leurs dossiers sous la charge ou le contrôle de cyberSanté Ontario en engageant les procédures d'accès indiquées à la section 3.7 de la présente politique. Aux fins de cette politique, les limitations et exceptions spécifiques sont celles énoncées dans la LAIPVP.

Les membres du personnel et les tiers fournisseurs de services de cyberSanté Ontario qui ont été retenus par cyberSanté Ontario ont l'obligation de recueillir, d'utiliser et de divulguer uniquement les RP essentiels à la bonne exécution de leurs tâches professionnelles. En signant l'*accord et le code de conduite sur la protection de la vie privée et la sécurité de cyberSanté Canada*, tous les membres du personnel et tous les tiers fournisseurs de services de cyberSanté Ontario acceptent de se conformer aux modalités de la présente politique.

Les tiers fournisseurs de services sont des particuliers ou des organismes dont les services ont été retenus par cyberSanté Ontario pour l'aider à mener à bien ses activités et à offrir ses services. Les tiers fournisseurs de services et leurs employés qui ont à traiter des RP détenus par cyberSanté Ontario doivent se conformer à toutes les politiques et procédures pertinentes de cyberSanté Ontario.

Les personnes autorisées sont des particuliers qui sont appelés à consulter des RP pour s'acquitter du rôle et des tâches qui leur ont été confiés par cyberSanté Ontario. Il incombe aux personnes qui sont autorisées à consulter des RP 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 en respectant la totalité des lois, des règlements et des politiques applicables. Les personnes autorisées n'ont accès aux RP que si elles ont besoin de les connaître.

### 3.1 Collecte de renseignements personnels par cyberSanté Ontario

cyberSanté Ontario est habilité à offrir des programmes et des services aux termes du Règlement de l'Ontario 43/02 comme modifié par le Règlement de l'Ontario 339/08 de la *Loi sur les sociétés de développement*, L.R.O. 1990, chapitre D. 10. La LAIPVP stipule que les RP peuvent être recueillis par cyberSanté Ontario ou en son nom uniquement lorsque la collecte de ces renseignements est expressément autorisée par la loi, et que ceux-ci sont utilisés à des fins d'application de la loi ou nécessaires à la bonne gestion d'une activité de cyberSanté Ontario dûment autorisée par la loi.

cyberSanté Ontario a recours à diverses méthodes pour recueillir des RP, y compris auprès du personnel et des tiers fournisseurs de services à des fins d'emploi, auprès de particuliers au moyen du site Web de cyberSanté Ontario et dans le cadre des activités visant à inscrire et à aider les utilisateurs finaux lors du déploiement de produits et de services de cyberSanté Ontario. cyberSanté Ontario doit recueillir des RP uniquement auprès des personnes concernées, à moins que ces personnes ou leurs mandataires consentent à un autre mode de collecte. cyberSanté Ontario doit recueillir des RP de façon indirecte uniquement lorsque la collecte indirecte de tels renseignements est autorisée par la loi.

## **3.2 Exigences en matière d’avis et de consentement**

cyberSanté Ontario doit aviser les personnes du motif de l’accès, de la collecte, de l’utilisation, de la conservation ou de la divulgation ultérieure de leurs RP. cyberSanté Ontario doit informer les personnes de tous les usages prévus de leurs RP au moment de la première collecte de renseignements. Les avis qui figurent dans les communications et dans les formulaires de cyberSanté Ontario et qui sont affichés au site Web de cyberSanté Ontario doivent être clairs, précis et révisés périodiquement afin d’en assurer l’actualité et l’exactitude.

Toute utilisation secondaire ou toute divulgation de RP recueillis par cyberSanté Ontario doit être autorisée par écrit par la personne à qui les renseignements ont trait ou, si autorisé, de son mandataire, sauf si cette utilisation ou cette divulgation est autrement permise ou exigée par la loi. Le consentement de la personne doit être dûment documenté et cette documentation doit être conservée en dossier et y demeurer pour la période de conservation prévue pour ce dossier.

## **3.3 Utilisation des renseignements personnels**

Seul le personnel dûment autorisé de cyberSanté Ontario a le droit d’utiliser les RP et ces renseignements doivent servir uniquement à la fin pour laquelle ils ont été obtenus ou à une fin déterminée.

cyberSanté Ontario a recours aux RP pour diverses raisons courantes, entre autres pour établir, gérer et administrer des relations de travail et des relations contractuelles, y compris l’administration de la paie et des avantages sociaux et l’utilisation de RP pour établir et tenir à jour les comptes et les services des clients finaux.

## **3.4 Divulgation de renseignements personnels par cyberSanté Ontario**

cyberSanté Ontario ne doit pas divulguer de RP à des organismes ou à des personnes externes sans le consentement de la personne à qui les renseignements ont trait, sauf si la divulgation est autorisée en vertu de l’article 42 de la LAIPVP. Les membres du personnel de cyberSanté Ontario et ses tiers fournisseurs de services doivent consulter la directrice de la protection de la vie privée avant de divulguer des RP sans consentement.

Toute divulgation de RP doit être documentée et cette documentation doit être conservée en dossier et gérée conformément aux politiques et procédures de cyberSanté Ontario.

## **3.5 Gestion des incidents et des violations**

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 ces programmes, 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.

## **3.6 Obligation de procéder à 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*, l’organisme 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 RP.

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.

### **3.7 Accès individuel aux renseignements personnels**

La LAIPVP garantit le droit d'accès des personnes à leurs RP sous la garde ou le contrôle de cyberSanté Ontario, sous réserve de limitations particulières précisées dans cette loi. Dans la mesure du possible, le personnel de cyberSanté Ontario doit aider les personnes à accéder à leurs RP sans qu'il soit nécessaire de présenter une demande officielle aux termes de la Loi. Les divisions de cyberSanté Ontario devraient définir des processus permettant de répondre aux demandes courantes d'accès aux RP.

En l'absence de processus ou en cas d'inquiétudes liées à la divulgation, on conseillera aux personnes de présenter une demande officielle aux termes de la LAIPVP. Ces demandes officielles devront être soumises directement au Bureau de l'accès à l'information, conformément à la *Politique sur l'accès à l'information et la protection de la vie privée de cyberSanté Ontario* et aux documents établissant la marche à suivre.

### **3.8 Précision, intégrité et demandes de correction des renseignements personnels**

cyberSanté Ontario doit veiller à assurer l'exactitude, l'actualité et l'intégrité des RP sous sa garde ou son contrôle. Lorsqu'une personne est d'avis qu'une erreur s'est glissée dans ses RP, elle peut demander que cette erreur soit corrigée. cyberSanté Ontario doit étudier la demande et y donner suite. Si la demande de correction peut être traitée de façon informelle, le personnel de cyberSanté Ontario doit tenter, dans la mesure du possible, d'assurer l'exactitude des RP de la personne. Toute demande officielle de correction de RP doit être acheminée à la directrice de la protection de la vie privée.

### **3.9 Conservation et destruction des renseignements personnels**

Le paragraphe 5(1) du Règlement 460 pris en application de la LAIPVP prévoit que les institutions doivent conserver les dossiers de RP des personnes pendant au moins un an suivant le dernier usage du dossier, sauf si les personnes consentent à leur destruction avant cette échéance.

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

cyberSanté Ontario a l'obligation de protéger tous les RP pour la durée de la période de conservation. La responsabilité de la gestion des dossiers de cyberSanté Ontario incombe au vice-président principal, Services internes, de cyberSanté Ontario. Le personnel de cyberSanté Ontario et les tiers fournisseurs de services retenus par cyberSanté Ontario doivent veiller à éliminer les dossiers contenant des RP conformément aux politiques et procédures de cyberSanté Ontario.

### **3.10 Banques de renseignements personnels**

La loi oblige cyberSanté Ontario à créer et à garder à jour une banque de renseignements personnels (BRP) qui identifie par type et par endroit les dossiers sous son contrôle qui renferment des RP. Cette information est fournie au ministre des Services gouvernementaux qui, à son tour, a l'obligation légale de la rendre accessible au public dans ses publications annuelles. Cette information est aussi accessible au public grâce au *Répertoire des dossiers de cyberSanté Ontario* décrit à la section 3.11.

Le personnel de cyberSanté Ontario doit s'assurer que les renseignements sur les dossiers et les catégories de fichiers sont transmis à la Gestion des documents, conformément à la *Norme de gestion des documents de cyberSanté Ontario*. Il incombe à tous les gestionnaires de programme de cyberSanté Ontario de fournir à la directrice ou au directeur de la protection de la vie privée, sur demande, tous les renseignements demandés sur les listes de fonds des BRP.

## 3.11 Gestion de l'information

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 RP 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 sont été recueillies.

## 4 Responsabilités

Le chef de la direction, sur les conseils de la directrice de la protection de la vie privée, ou de son délégué, est chargé d'interpréter les volets de la politique ayant trait aux RP régis par la LAIPVP. La responsabilité ultime de toute question relative à la LAIPVP à cyberSanté Ontario incombe au chef de la direction à titre de chef de l'institution, selon la définition du Règlement de l'Ontario 460 (LAIPVP, R.R.O. 1990, Règlement 460 - « General »). Les responsabilités liées aux demandes d'accès à l'information aux termes de la LAIPVP sont énoncées dans la *Politique sur l'accès à l'information et la protection de la vie privée de cyberSanté Ontario*.

La directrice de la protection de la vie privée est considérée comme ayant le pouvoir final en matière d'interprétation de la présente politique.

La directrice de la protection de la vie privée a la responsabilité d'assurer la mise en œuvre, l'application et le 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 RP conformément à la présente politique et à la loi qui s'applique.

## 5 Glossaire

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

TERME	DÉFINITION
<b>Accès</b>	S'entend de l'aptitude d'une personne à récupérer, à visionner ou traiter personnellement des renseignements identifiables.



<b>Utilisateurs autorisés ou personnes autorisées</b>	S'entend des employés ou des représentants de cyberSanté Ontario qui ont été autorisés à accéder à des bases de données particulières ou à d'autres dépôts de renseignements personnels nécessaires à la bonne exécution de leurs tâches. Il est entendu que les utilisateurs autorisés auront signé le Code de conduite sur la protection de la vie privée et la sécurité de cyberSanté Ontario et qu'ils auront suivi, au besoin, toute formation nécessaire sur la protection de la vie privée et la sécurité pertinente à leurs fonctions au sein de l'organisme.
<b>Collecte</b>	S'entend d'un regroupement de renseignements personnels sur des personnes identifiables qui peut survenir directement, indirectement, activement ou passivement.
<b>Dépôt de données</b>	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.
<b>Divulgation</b>	S'entend de la transmission de renseignements à des instances qui ne font pas partie de cyberSanté Ontario.
<b>Gestionnaires de cyberSanté Ontario</b>	Un gestionnaire est une personne dont les principales responsabilités consistent à superviser ou à diriger (ou les deux) les ressources humaines ou autres. À cyberSanté Ontario, les gestionnaires peuvent être le chef de la direction, les vice-présidents principaux, les vice-présidents, les directeurs principaux, les directeurs, les gestionnaires, les superviseurs, les responsables de programme, les gestionnaires de projet et les membres du personnel qui s'acquittent de fonctions de gestion.
<b>Personnel de cyberSanté Ontario</b>	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 temporairement un emploi permanent à plein temps, au jour le jour, et qui sont gérées directement par la direction de cyberSanté Ontario.
<b>Dossiers de cyberSanté Ontario</b>	Tout dossier créé dans le cadre des activités de cyberSanté Ontario.
<b>Loi sur l'accès à l'information et la protection de la vie privée, L.R.O. 1990, chap. F.31 (LAIPVP)</b>	Une loi provinciale sur la protection de la vie privée qui confère un droit d'accès aux renseignements sous le contrôle des institutions conformément aux principes selon lesquels les renseignements devraient être accessibles par le public; les exemptions nécessaires au droit d'accès devraient être limitées et spécifiques; et les décisions concernant la divulgation de renseignements appartenant au gouvernement devraient être examinées indépendamment du gouvernement. La LAIPVP protège également la confidentialité des renseignements personnels des personnes détenus par les institutions. Elle confère aux personnes le droit d'accéder à ces renseignements et de les corriger.
<b>Plus petite quantité de renseignements pertinents</b>	S'entend du plus petit regroupement possible de données nécessaire pour s'acquitter d'un rôle, d'une tâche ou d'une fonction en particulier.
<b>Nécessité de savoir</b>	S'entend du principe qui sous-tend l'accès d'un utilisateur autorisé, et l'usage par cet utilisateur, de la « plus petite quantité de renseignements pertinents » nécessaire pour

permettre à cyberSanté Ontario de mener ses activités adéquatement.

---

<b>Renseignements personnels (RP)</b>	<p>S'entend des renseignements consignés ayant trait à un particulier qui peut être identifié, notamment</p> <ul style="list-style-type: none"><li>a) des renseignements concernant la race, l'origine nationale ou ethnique, la couleur, la religion, l'âge, le sexe, l'orientation sexuelle, l'état matrimonial ou familial de celui-ci;</li><li>b) des renseignements concernant l'éducation, les antécédents médicaux, psychiatriques, psychologiques, criminels ou professionnels de ce particulier ou des renseignements reliés à sa participation à une opération financière;</li><li>c) d'un numéro d'identification, d'un symbole ou d'un autre signe individuel qui lui est attribué;</li><li>d) de l'adresse, du numéro de téléphone, des empreintes digitales ou du groupe sanguin de ce particulier;</li><li>e) de ses opinions ou de ses points de vue personnels, sauf s'ils se rapportent à un autre particulier;</li><li>f) de la correspondance ayant explicitement ou implicitement un caractère personnel et confidentiel, adressée par le particulier à une institution, ainsi que des réponses à cette correspondance originale susceptibles d'en révéler le contenu;</li><li>g) des opinions et des points de vue d'une autre personne au sujet de ce particulier;</li><li>h) du nom du particulier, s'il figure parmi d'autres renseignements personnels qui le concernent, ou si sa divulgation risque de révéler d'autres renseignements personnels au sujet du particulier.</li></ul>
<b>Conservation</b>	<p>S'entend du maintien en sa possession de renseignements personnels ou de renseignements personnels sur la santé par un organisme.</p>
<b>Droit d'accès</b>	<p>S'entend du droit d'une personne de voir ou d'obtenir copie de ses renseignements sous la charge ou le contrôle de cyberSanté Ontario, sous réserve des modalités limitées et spécifiques de la LAIPVP ou, dans les cas où la LAIPVP ne s'applique pas, à la discrétion raisonnable du dépositaire des renseignements personnels.</p>
<b>Droit de demander une correction</b>	<p>S'entend du droit d'une personne de demander à cyberSanté Ontario de mettre à jour ou d'autrement modifier ses renseignements personnels lorsque ces renseignements peuvent contenir une erreur.</p>
<b>Utilisation</b>	<p>S'entend du traitement de renseignements personnels au sein de l'organisme.</p>

---

**Tableau 1 : Politique sur la protection de la vie privée : Glossaire**

## 6 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
<i>Loi sur l'accès à l'information et la protection de la vie privée</i> et ses règlements	<a href="http://www.elaws.gov.on.ca/html/statutes/french/elaws_statutes_9of31_f.htm">http://www.elaws.gov.on.ca/html/statutes/french/elaws_statutes_9of31_f.htm</a>
Politique sur la protection de la vie privée et des données de cyberSanté Ontario	<a href="http://www.ehealthontario.on.ca/fr/privacy">http://www.ehealthontario.on.ca/fr/privacy</a>
Politique d'évaluation de l'impact sur la protection de la vie privée de cyberSanté Ontario	<a href="http://emerge/spaces/privacy/Documents/Forms/AllItems.aspx">http://emerge/spaces/privacy/Documents/Forms/AllItems.aspx</a>
Politique de gestion des incidents et des violations touchant la protection de la vie privée de cyberSanté Ontario	<a href="http://www.ehealthontario.on.ca/fr/privacy">http://www.ehealthontario.on.ca/fr/privacy</a>
Politique et procédure relative aux plaintes et aux demandes de renseignements liées à la protection de la vie privée de cyberSanté Ontario	<a href="http://www.ehealthontario.on.ca/fr/privacy">http://www.ehealthontario.on.ca/fr/privacy</a>
Politique de protection de la vie privée reliée aux responsabilités des tiers fournisseurs de services de cyberSanté Ontario	<a href="http://www.ehealthontario.on.ca/fr/privacy">http://www.ehealthontario.on.ca/fr/privacy</a>
Répertoire des dossiers de cyberSanté Ontario	<a href="http://www.ehealthontario.on.ca/fr/privacy">http://www.ehealthontario.on.ca/fr/privacy</a>
Politique et procédure relative à la gestion des risques liés à la protection de la vie privée de cyberSanté Ontario	<a href="http://emerge/spaces/privacy/Documents/Forms/AllItems.aspx">http://emerge/spaces/privacy/Documents/Forms/AllItems.aspx</a>
Politique de cyberSanté Ontario sur les demandes d'accès à l'information et la protection de la vie privée	<a href="http://emerge/spaces/privacy/Documents/Forms/AllItems.aspx">http://emerge/spaces/privacy/Documents/Forms/AllItems.aspx</a>
Norme de gestion des dossiers de cyberSanté Ontario	<a href="http://emerge/spaces/privacy/Documents/Forms/AllItems.aspx">http://emerge/spaces/privacy/Documents/Forms/AllItems.aspx</a>
Norme de conduite en matière de protection de la vie privée et de sécurité pour les employés de cyberSanté Ontario	<a href="http://emerge/spaces/privacy/Documents/Forms/AllItems.aspx">http://emerge/spaces/privacy/Documents/Forms/AllItems.aspx</a>
Norme de conduite en matière de protection de la vie privée et de sécurité pour les fournisseurs de	<a href="http://emerge/spaces/privacy/Documents/Forms/AllItems.aspx">http://emerge/spaces/privacy/Documents/Forms/AllItems.aspx</a>

**Tableau 2 : Politique sur la protection de la vie privée : Références et documents connexes**

## 7 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.