eHealth Ontario

# Politique de gestion des incidents et des violations touchant la protection de la vie privée

## Bureau de la protection de la vie privée

Identificateur du document : 2480

Version : 2.2

Propriétaire : Directrice générale de la protection de la vie privée

Niveau de confidentialité : Faible

Ontario
eHealth Ontario

# Table des matières



# Tableaux

# 1 But et objectif

La présente politique décrit la façon dont cyberSanté Ontario procèdera afin d'identifier, de confiner, de divulguer et de corriger les incidents et les violations touchant la protection de la vie privée, selon les définitions données dans la présente politique, d'enquêter sur ceux-ci et d'envoyer des avis à ce sujet.

La *Politique de gestion des incidents et des violations touchant la protection de la vie privée de cyberSanté Ontario* doit être consultée de concert avec la *Politique sur la protection de la vie privée et des données*, la *Politique sur la protection des renseignements personnels sur la santé* et la *Politique sur la protection des renseignements personnels de cyberSanté Ontario*, ainsi que tous les documents pertinents relatifs à la gestion des violations de 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. Les dispositions pertinentes de la présente politique doivent, le cas échéant, être abordées dans les ententes entre cyberSanté Ontario et les tiers fournisseurs de services. La présente politique s'applique aux services de cyberSanté Ontario susceptibles d'avoir une incidence sur la confidentialité des renseignements personnels (RP) et des renseignements personnels sur la santé (RPS) confiés à l'organisme.

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 Exigences prévues par la loi

cyberSanté Ontario peut exercer plusieurs fonctions, de la manière décrite dans la *Loi de 2004 sur la protection des renseignements personnels sur la santé* (LPRPS) et à son Règlement; en vertu de l'article 17 de la LPRPS; en vertu du paragraphe 6.2 du Règlement de l'Ontario 329/04; en vertu de l'article 6 du Règlement de l'Ontario 329/04 comme fournisseur d'un réseau d'information sur la santé (FRIS), fournisseur de services électroniques, mandataire ou fournisseur de services à un réseau d'information sur la santé. Chacun de ces rôles est axé sur la relation de cyberSanté Ontario avec un ou plusieurs dépositaires de renseignements sur la santé (DRS).

L'article 6 et le paragraphe 6.2 du Règlement de l'Ontario 329/04 exigent que cyberSanté Ontario mette en place des mesures de protection administrative, technique et physique afin de protéger les RPS contre le vol et la perte, ainsi que l'utilisation ou la divulgation non autorisée ou inappropriée et qui est non conforme aux dispositions législatives pertinentes en matière de protection de la vie privée. Le règlement exige également que cyberSanté Ontario informe tous les DRS concernés, dès la première possibilité raisonnable, si des RPS qui ont été fournis à cyberSanté Ontario ont été volés, perdus ou consultés par des personnes non autorisées.

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 assujetti à ses dispositions. cyberSanté Ontario s'est engagé à protéger les renseignements personnels assujettis à la LAIPVP et à élargir ses pratiques de protection de la

vie privée à son traitement des renseignements personnels lorsque ces renseignements peuvent ne pas être assujettis à des lois ou à des règlements sur la protection de la vie privée.

# 4 Définitions

Un incident touchant la protection de la vie privée comprend :

- une contravention aux politiques, procédures ou pratiques de protection de la vie privée mises en œuvre par cyberSanté Ontario, lorsque cette contravention ne donne pas lieu à la collecte, à l'utilisation, à la divulgation et à la destruction non autorisées de RP ou de RPS ou n'entraîne pas une non-conformité par rapport aux dispositions législatives pertinentes en matière de protection de la vie privée;
- une contravention aux accords qui ont été conclus par cyberSanté Ontario avec les intervenants externes et les tiers fournisseurs de services, y compris notamment les accords avec les mandataires de la LPRPS, les accords relatifs au partage de données, les accords de confidentialité et de non-divulgation et les accords avec les tiers fournisseurs de services retenus par cyberSanté Ontario, lorsque cette contravention n'entraîne pas une non-conformité par rapport aux dispositions législatives pertinentes en matière de protection de la vie privée;
- une violation présumée touchant la protection de la vie privée.

Une violation touchant la protection de la vie privée comprend :

- la collecte, l'utilisation ou la divulgation de RPS en violation de la LPRPS et de ses règlements;
- la collecte, l'utilisation ou la divulgation de RP en violation de la LAIPVP et de ses règlements;
- les situations dans lesquelles des RP ou des RPS sont volés, perdus ou recueillis, utilisés, divulgués, copiés, modifiés, conservés ou éliminés de façon non autorisée ou inappropriée.

Les incidents et les violations touchant la protection de la vie privée peuvent être intentionnels ou accidentels.

# 5 Politique

La directrice de la protection de la vie privée de cyberSanté Ontario est chargée de diriger la conception et le fonctionnement du programme de protection de la vie privée de l'organisme, y compris la mise en place de processus, de pratiques et d'outils visant à gérer, à mener des enquêtes et à corriger les incidents ou les violations touchant la protection de la vie privée. L'équipe de gestion des violations touchant la protection de la vie privée est responsable des activités complètes de gestion des violations touchant la protection de la vie privée.

Les membres du personnel et les tiers fournisseurs de services sont tenus de signaler immédiatement au Service de dépannage de cyberSanté Ontario tout incident et toute violation touchant la protection de la vie privée. Les membres du personnel et les tiers fournisseurs de services sont tenus de fournir une description de l'incident ou de la violation, des personnes concernées et des mesures immédiates prises, le cas échéant, afin de confiner l'incident ou la violation.

cyberSanté Ontario étend la protection des dénonciateurs aux membres du personnel et aux tiers fournisseurs de services qui signalent un incident ou une violation touchant la protection de la vie privée et aux personnes qui refusent d'effectuer une transaction qu'elles jugent être non conforme aux rôles de cyberSanté Ontario en vertu de la LPRPS ou de la LAIPVP, aux accords pertinents ou aux politiques et procédures de protection de la vie privée de cyberSanté Ontario.

Les membres du personnel et les tiers fournisseurs de services ont la responsabilité d'appuyer activement le Bureau de la protection de la vie privée en matière de confinement et de correction d'un incident ou d'une violation de la protection de la vie privée et d'enquête à ce sujet, le cas échéant. Certaines de ces activités peuvent se produire simultanément.

## 5.1 Confinement

La phase de confinement du processus de gestion d'un incident et d'une violation touchant la protection de la vie privée met l'accent sur la confirmation de l'existence d'un incident ou d'une violation touchant la protection de la vie privée, les mesures préventives visant à empêcher que d'autres produits d'information soient touchés, l'assurance que les produits d'information concernés ne sont pas davantage compromis, l'atténuation des répercussions défavorables sur l'organisme et le rétablissement du fonctionnement normal aussi rapidement que possible.

Les activités de confinement peuvent comprendre, par exemple :

- la suspension de la pratique non autorisée qui a donné lieu à l'incident ou à la violation;
- la récupération des dossiers de RP ou de RPS touchés;
- l'arrêt du système qui a fait l'objet de la violation;
- la révocation permanente ou temporaire de l'accès à un système;
- la communication avec la police (si la violation consiste en un vol ou toute autre activité criminelle).

Les incidents et les violations touchant la protection de la vie privée qui sont signalés doivent être confinés immédiatement, conformément au document intitulé *Privacy Incident and Breach Management Reference Guide for the Privacy Office*. Le confinement immédiat des incidents touchant la protection de la vie privée permettra d'éviter qu'ils deviennent des violations et préviendra la poursuite de toute collecte, utilisation ou divulgation non autorisée de RP ou de RPS.

Lorsque l'on soupçonne qu'un incident ou une violation est de nature intentionnelle, la question doit être immédiatement transmise à la directrice de la protection de la vie privée.

## 5.2 Enquête et mesures correctives

Une fois qu'un incident ou une violation touchant la protection de la vie privée a été confiné de façon adéquate, l'équipe de gestion des violations touchant la protection de la vie privée mène une enquête afin d'en déterminer la cause et de connaître également les produits d'information, les personnes, les organismes ainsi que les systèmes et le matériel de TI impliqués dans l'incident ou la violation.

À la lumière des conclusions de l'enquête, l'équipe de gestion des violations touchant la protection de la vie privée détermine les stratégies de correction à court et à long terme qui sont documentées dans un rapport de gestion de la violation touchant la protection de la vie privée. Le rapport et les recommandations découlant de l'enquête doivent être approuvés par la directrice de la protection de la vie privée et mis en œuvre dans les délais indiqués.

## 5.3 Communication et avis

Le service de relation avec les intervenants et de communications de cyberSanté Ontario détermine les communications obligatoires ou facultatives qui seront diffusées auprès des intervenants internes de cyberSanté Ontario (c.-à-d. le comité de haute direction et le conseil d'administration) à la suite d'un incident ou d'une violation touchant la protection de la vie privée. Les communications internes peuvent être obligatoires ou à la discrétion de la directrice de la protection de la vie privée (ou la personne désignée) en consultation avec la personne responsable de la gestion des violations touchant la protection de la vie privée. Les communications internes sont réalisées conformément aux exigences énoncées dans la procédure intitulée *Privacy Incident and Breach Communication with Internal Stakeholder*, contenue dans le document intitulé *Privacy Incident and Breach Management Reference Guide for the Privacy Office*.

L'obligation de cyberSanté Ontario d'émettre des avis concernant les incidents ou les violations touchant la protection de la vie privée aux dépositaires de RP ou de RPS, aux personnes concernées par les RP ou les RPS ou d'autres intervenants externes est déterminée par les dispositions législatives pertinentes ou les accords entre cyberSanté Ontario et des tiers. Les exigences en matière de communication externe et d'avis sont énoncées dans la procédure intitulée *Privacy Incident and Breach Communication with External Stakeholders*.

## 5.4 Consignation des données et conservation des documents

Le Bureau de la protection de la vie privée doit tenir un registre des incidents et des violations touchant la protection de la vie privée, ainsi que des recommandations découlant des enquêtes relatives à ces incidents et violations. Le registre sera utilisé pour préparer des rapports réguliers à la haute direction de cyberSanté Ontario au sujet du nombre et de la nature des incidents ou des violations touchant la protection de la vie privée.

Tous les documents relatifs à l'identification, au confinement, aux enquêtes, aux mesures correctives, aux communications et aux avis concernant les incidents ou les violations touchant la protection de la vie privée doivent être conservés de façon sécuritaire par le Bureau de la protection de la vie privée, conformément aux documents pertinents relatifs à la gestion des incidents ou des violations touchant la protection de la vie privée.

# 6 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. Lorsqu'un incident ou une violation touchant la protection de la vie privée est intentionnel ou découle de pratiques de travail négligentes, des mesures disciplinaires seront prises, lesquelles pourraient aller jusqu'au congédiement.

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 doivent se conformer à cette procédure.

# 7 Glossaire

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

| TERME | DÉFINITION |
|---|---|
| **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 habilitant, art. 1) |
| ***Loi sur l'accès à l'information et la protection de la vie privée*, L.R.O. 1990, chap. F.31 (LAIPVP)** | 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. |

| | |
|---|---|
| **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) 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. |
| **Commissaire à l'information et à la protection de la vie privée** | Le 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. |
| **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. |
| ***Loi de 2004 sur la protection des renseignements personnels sur la santé*, L.O. 2004, chap. 3 (LPRPS)** | 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. |
| **Renseignements personnels (RP)** | S'entend au sens de l'article 2 de la *Loi sur l'accès à l'information et la protection de la vie privée* comme : renseignements consignés ayant trait à un particulier qui peut être identifié, notamment : 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; 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; c) d'un numéro d'identification, d'un symbole ou d'un autre signe individuel qui lui est attribué; d) de l'adresse, du numéro de téléphone, des empreintes digitales ou du groupe sanguin de ce particulier; e) de ses opinions ou de ses points de vue personnels, sauf s'ils se rapportent à un autre particulier; 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; g) des opinions et des points de vue d'une autre personne au sujet de ce particulier; 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. |
| **Personnel** | Collectivement, les personnes suivantes : les employés actuels et les anciens employés; les fournisseurs actuels; les personnes nommées actuelles et les anciennes personnes nommées.<br><br>Où :<br><br>• 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.<br>• 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.<br>• 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. |
| **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 donne pas lieu à une collecte, à une utilisation, à une divulgation ou à une destruction non autorisée de RP ou de RPS ou 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. |

**Tableau 1:Politique de gestion des incidents et des violations touchant la protection de la vie privée : Glossaire**

# 8 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 sur l'accès à l'information et la protection de la vie privée* et ses règlements | http://www.elaws.gov.on.ca/html/statutes/french/elaws_statutes_90f31_f.htm |
| *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 | www.ehealthontario.on.ca/fr/privacy |
| Politique sur la confidentialité des renseignements personnels de cyberSanté Ontario | www.ehealthontario.on.ca/fr/privacy |
| Politique sur la protection des renseignements | www.ehealthontario.on.ca/fr/privacy |

| | |
|---|---|
| personnels sur la santé de cyberSanté Ontario | |
| Privacy Incident and Breach Management Reference Guide for the Privacy Office de cyberSanté Ontario | Point d'accès interne du Bureau de la protection de la vie privée |
| Politique sur la protection des dossiers de santé électronique de cyberSanté Ontario | http://www.ehealthontario.on.ca/fr/initiatives/resources/ |
| Privacy and Security Breach Management Protocols for MOHLTC datasets used in Electronic Health Records – cyberSanté Ontario et MSSLD | Point d'accès interne du Bureau de la protection de la vie privée |

**Tableau 2: Politique de gestion des incidents et des violations touchant la protection de la vie privée : Références et documents connexes**

# 9 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.