L'accès non autorisé aux renseignements personnels sur la santé : détection et dissuasion

Information and Privacy Commissioner of Ontario

Commissaire à l'information et à la protection de la vie privée de l'Ontario

TABLE DES MATIÈRES

INTRODUCTION

On entretient avec son fournisseur de soins de santé une relation qui est fondée sur la confiance. On lui donne des détails intimes sur sa santé et son bien-être, en toute confidentialité, afin de recevoir les meilleurs soins et traitements. On s'attend à ce que les renseignements ainsi fournis soient utilisés et divulgués s'ils sont raisonnablement nécessaires aux fins de la prestation de soins de santé ou d'une aide à cet égard. Personne ne s'attend à ce que ses renseignements personnels sur la santé soient recueillis, utilisés ou divulgués par des personnes qui ne leur fournissent pas de soins de santé, sans leur consentement exprès ou à des fins qui ne sont pas reliées à la prestation de soins de santé ou autorisées par la loi. Ne pas respecter les attentes des particuliers en matière de vie privée et de confidentialité porterait atteinte de façon irrémédiable à la relation entre eux et les fournisseurs de soins de santé, ce qui aurait des conséquences sérieuses pour les particuliers, ces fournisseurs et l'ensemble du secteur de la santé.

En Ontario, la *Loi sur la protection des renseignements personnels sur la santé* (*LPRPS*) établit des règles concernant la collecte, l'utilisation et la divulgation de renseignements personnels sur la santé par les dépositaires de renseignements sur la santé (les « dépositaires ») et leurs mandataires. Les dépositaires sont des personnes et des organismes, tels que des professionnels de la santé et des hôpitaux, qui ont la garde ou le contrôle de renseignements personnels sur la santé à des fins liées à la prestation de soins de santé. Les mandataires sont des personnes, telles que des employés, des entrepreneurs indépendants, des médecins ayant des privilèges et des bénévoles, qui agissent au nom des dépositaires en ce qui concerne les renseignements personnels sur la santé.

La *LPRPS* permet aux dépositaires de recueillir, d'utiliser et de divulguer des renseignements personnels sur la santé aux fins de la prestation de soins de santé ou d'une aide à cet égard, sur la base d'un consentement implicite ou présumé, mais elle interdit la collecte, l'utilisation et la divulgation de renseignements personnels sur la santé à toute autre fin sans le consentement exprès de la personne concernée, à moins qu'elle ne l'autorise ou ne l'exige par ailleurs. La *LPRPS* oblige les dépositaires de renseignements sur la santé à prendre des mesures qui sont raisonnables dans les circonstances pour veiller à ce que les renseignements personnels sur la santé dont ils ont la garde ou le contrôle soient protégés contre le vol, la perte et une utilisation ou une divulgation non

autorisée et à ce que les dossiers qui les contiennent soient protégés contre une duplication, une modification ou une élimination non autorisée.

Il est arrivé récemment que des dépositaires ou leurs mandataires utilisent ou divulguent des renseignements personnels sur la santé, sans le consentement des personnes concernées, à des fins qui ne sont pas autorisées ou exigées par la *LPRPS*. Si bon nombre de ces cas concernaient l'accès aux dossiers électroniques de renseignements personnels sur la santé de membres de la famille, d'amis, de collègues de travail et de voisins, ainsi que de personnalités, de politiciens et d'autres personnes bien connues, d'autres cas concernaient l'accès aux dossiers électroniques de personnes qui n'avaient aucune relation avec le dépositaire ou le mandataire. L'utilisation ou la divulgation de renseignements personnels sur la santé à de telles fins est communément appelée « accès non autorisé ». L'accès non autorisé, y compris la consultation de renseignements personnels sur la santé dans les systèmes d'information électroniques, peut être motivé par un certain nombre de facteurs, notamment les conflits interpersonnels, la curiosité, le gain personnel ou le souci pour la santé et le bien-être des particuliers en question.

L'accès non autorisé semble représenter un problème croissant dans le secteur de la santé en Ontario. Le présent document a pour but de faire la lumière sur l'ampleur de ce problème et ses conséquences éventuelles pour les particuliers, les dépositaires et leurs mandataires, ainsi que pour l'ensemble du secteur de la santé, et de fournir des conseils aux dépositaires sur la façon de minimiser le risque d'accès non autorisé par leurs mandataires.

LES AVANTAGES ET LES RISQUES DES DOSSIERS ÉLECTRONIQUES

Le secteur de la santé passe progressivement des dossiers papier aux dossiers électroniques. Ainsi, un sondage national auprès des médecins réalisé en 2013 a révélé que 64 % des médecins de famille et omnipraticiens du Canada utilisent des dossiers électroniques pour saisir et récupérer des notes cliniques[1]. Selon l'Inforoute Santé du Canada, on compte plus de 62 000 utilisateurs de dossiers électroniques de renseignements personnels sur la santé au Canada, en hausse de plus de 700 % depuis 2006[2].

Les avantages des dossiers électroniques sont nombreux. Les personnes qui participent à la prestation de soins de santé à un particulier peuvent retrouver rapidement et facilement un dossier électronique, où qu'elles se trouvent. De plus, ces dossiers sont généralement plus faciles à lire et à localiser que les dossiers sur papier, dont certains sont écrits à la main, parfois de manière illisible, incomplets et dispersés en divers endroits. Les dossiers électroniques peuvent contribuer à rehausser la prise de décisions cliniques, ce qui se traduit par un diagnostic et un traitement plus efficaces; à une plus grande sécurité grâce à une meilleure disponibilité de renseignements personnels sur la santé complets, à jour et exacts; à une efficacité accrue; et à un meilleur accès aux services. Les dossiers électroniques peuvent également être conçus pour améliorer la protection de la vie privée des particuliers et la sécurité des renseignements personnels sur la santé grâce à des mesures de précaution telles que des contrôles d'accès, des fonctions de consignation et de vérification, et le chiffrement.

Si les dossiers électroniques présentent de nombreux avantages éventuels, tels qu'une accessibilité, une transférabilité et une portabilité accrues, ces caractéristiques posent également des risques uniques en matière de protection de la vie privée. Les dossiers électroniques peuvent éventuellement permettre de recueillir, d'utiliser et de divulguer de grandes quantités de renseignements personnels sur la santé provenant de diverses sources en appuyant simplement sur une touche, et sont plus susceptibles d'attirer les pirates informatiques et d'autres personnes mal intentionnées. Les dossiers électroniques peuvent

1 Collège des médecins de famille du Canada, Association médicale canadienne, Collège royal des médecins et chirurgiens du Canada. *Sondage national des médecins 2013 = National Physician Survey 2013*. Sur Internet : http://nationalphysiciansurvey.ca/surveys/2013-survey/survey-results/.

2 Inforoute Santé du Canada. *Rapport annuel 2013-2014*. Sur Internet : https://www.infoway-inforoute.ca/fr/component/edocman/ressources/activites-i-inforoute-i/rapports-annuels/1953-rapport-annuel-2013-2014.

également accroître le risque d'accès non autorisé aux renseignements personnels sur la santé par les dépositaires et leurs mandataires disposant de privilèges d'accès fondés sur des rôles. Un rapport analysant plus de 63 000 atteintes à la sécurité dans 95 pays a révélé que « l'utilisation abusive des privilèges par les initiés », définie comme toute utilisation interne non approuvée ou malveillante des ressources de l'organisation, représentait 15 % des atteintes subies par les organismes de soins de santé et que 85 % de ces atteintes concernaient des dossiers électroniques plutôt que des dossiers papier[3].

Les renseignements personnels sur la santé contenus dans les dossiers électroniques peuvent être recueillis, utilisés et divulgués plus facilement et plus rapidement à des fins non autorisées, ce qui peut accroître l'ampleur et la gravité d'une atteinte à la vie privée.

L'accès non autorisé aux renseignements personnels est problématique dans tous les secteurs d'activité. Selon une étude menée par l'institut Ponemon auprès d'utilisateurs privilégiés, tels que des administrateurs de bases de données, des ingénieurs de réseaux et des responsables de la sécurité informatique dans divers secteurs d'activité aux États-Unis, 65 % des répondants ont déclaré qu'il était très probable ou probable que les utilisateurs privilégiés accèdent à des renseignements sensibles ou confidentiels par curiosité[4]. D'après une autre étude du Ponemon Institute menée auprès de professionnels de l'informatique de différents secteurs aux États-Unis, 78 % des répondants ont indiqué que des employés négligents ou malveillants ou d'autres initiés avaient été responsables d'au moins une atteinte à la vie privée au sein de leur organisation au cours des deux dernières années[5].

L'accès non autorisé aux renseignements personnels sur la santé conservés dans des systèmes d'information électroniques constitue également un problème majeur pour le secteur de la santé en particulier. Il n'existe pas de statistiques propres à l'Ontario sur la fréquence des accès non autorisés aux renseignements personnels sur la santé par les dépositaires et leurs mandataires. Cependant, le nombre de cas signalés en Ontario et dans d'autres territoires de compétence au Canada, ainsi que des rapports provenant des États-Unis, semblent indiquer que ce problème est omniprésent dans le secteur de la santé au Canada et aux États-Unis. Par exemple, selon

3 Verizon. *2014 Data Breach Investigations Report*. Sur Internet : http://www.verizonenterprise.com/DBIR/2014/ et http://www.verizonenterprise.com/resources/factsheets/fs_2014-dbir-industries-healthcare-services-threat-landscape_en_xg.pdf.

4 Ponemon Institute LLC. *Privileged User Abuse & The Insider Threat*, mai 2014. Sur Internet : http://www.trustedcs.com/resources/whitepapers/Ponemon-RaytheonPrivilegedUserAbuseResearchReport.pdf.

5 Ponemon Institute LLC. *The Human Factor in Data Protection*, janvier 2012. Sur Internet : http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_trend-micro_ponemon-survey-2012.pdf.

un rapport américain, 52 % des organismes de soins de santé se considèrent vulnérables ou très vulnérables aux menaces de l'intérieur et 61 % des professionnels de la sécurité des soins de santé affirment que les employés non techniciens ayant un accès légitime aux renseignements personnels sur la santé et aux actifs de la technologie de l'information constituent la plus grande menace d'attaque de l'intérieur[6].

6 Jon Oltsik. *Vormetric/ESG Insider Threat Report: Profile on Health Care*, janvier 2014. Sur Internet : http://enterprise-encryption.vormetric.com/2014-Vormetric-Insider-Threat-Report-Healthcare.html (connexion requise).

LES CONSÉQUENCES DE L'ACCÈS NON AUTORISÉ

PRÉJUDICES AUX PARTICULIERS

L'accès non autorisé à des renseignements personnels sur la santé peut avoir des conséquences importantes pour toutes les personnes concernées. Les particuliers dont les renseignements personnels sur la santé font l'objet d'un accès non autorisé peuvent être victimes de discrimination, de stigmatisation et de préjudices émotionnels ou psychologiques. Ces préjudices peuvent être aggravés lorsque l'accès non autorisé survient à un moment où la personne est atteinte d'une maladie grave ou mortelle et est plus vulnérable aux effets néfastes du stress. Les particuliers peuvent être dissuadés de demander des tests ou des traitements à l'avenir, et dissimuler ou falsifier les renseignements personnels sur la santé fournis aux dépositaires et à leurs mandataires par crainte d'un accès non autorisé. Ils peuvent également perdre leur confiance dans le système de santé. Un sondage parrainé par l'Inforoute Santé du Canada a révélé que 85 % des Canadiens croient que des gens évitent de divulguer des renseignements personnels sur la santé de leur médecin, 33 % d'entre eux estimant que c'est parce qu'ils craignent que d'autres membres du personnel ne consultent les renseignements personnels sur la santé qui les concernent[7].

ATTEINTE À LA RÉPUTATION

L'accès non autorisé aux renseignements personnels sur la santé peut causer des dommages irréparables à la réputation des dépositaires et de leurs mandataires, ainsi qu'aux relations qu'ils entretiennent avec les particuliers qui leur ont confié leurs renseignements personnels sur la santé. Les particuliers qui perdent confiance dans la capacité des dépositaires et de leurs mandataires à protéger leurs renseignements personnels sur la santé sont susceptibles de ne pas communiquer certains renseignements essentiels ou d'imposer des conditions ou des restrictions à la collecte, à l'utilisation et à la divulgation de leurs renseignements personnels sur la santé.

La prestation efficace et efficiente des soins de santé dépend de la disponibilité de renseignements personnels sur la santé exacts, complets et à jour. Si les particuliers ne fournissent pas ces renseignements en raison d'un manque de confiance et de préoccupations concernant la protection de la vie privée, cela

7 Ipsos Reid. Le point de vue des Canadiens : Sondage 2012 sur les renseignements de santé électroniques et la protection des renseignements personnels. Sur Internet : https://www.infoway-inforoute.ca/fr/component/edocman/ressources/rapports/protection-de-la-confidentialite/462-sondage-d-ipsos-reid-sur-les-renseignements-de-sante-electroniques-et-la-protection-de-la-vie-privee.

peut avoir une incidence sur la qualité des soins de santé fournis, ainsi que sur la sécurité des patients. Cela peut également avoir une incidence sur la qualité des renseignements sur la santé qui sont disponibles à des fins secondaires, comme la recherche sur la santé et la planification du système de santé. En outre, si les particuliers imposent des conditions ou des restrictions à la collecte, à l'utilisation et à la divulgation de leurs renseignements personnels sur la santé au lieu de permettre aux dépositaires de s'appuyer sur un consentement implicite, cela peut non seulement entraver ou retarder la prestation des soins de santé, mais aussi augmenter les coûts administratifs pour les dépositaires et l'ensemble du système de santé.

MESURES DISCIPLINAIRES

Les mandataires qui accèdent sans autorisation à des renseignements personnels sur la santé peuvent faire l'objet de mesures disciplinaires telles que la fin ou la suspension de leur emploi ou de leur relation contractuelle ou autre avec le dépositaire. Les professionnels de la santé réglementés peuvent également être signalés à leur ordre professionnel, ce qui peut éventuellement donner lieu à une enquête, à un constat de faute professionnelle et à d'autres mesures disciplinaires. Cela peut avoir de graves conséquences sur leurs perspectives professionnelles.

Par exemple, une infirmière autorisée qui a consulté le dossier électronique de renseignements personnels sur la santé de la conjointe séparée de son petit ami a été sanctionnée par l'Ordre des infirmières et infirmiers de l'Ontario. Son certificat d'inscription a été suspendu pendant six semaines et assujetti à des conditions et restrictions, et elle a été réprimandée par le sous-comité. Parmi les conditions imposées, elle devait fournir à ses employeurs, pendant une période d'un an après avoir recommencé à exercer, une copie de l'ordonnance et de l'avis d'audience ou, si possible, de la décision écrite et des motifs[8].

En Alberta, une pharmacienne qui a consulté les dossiers d'un certain nombre de femmes de son église et a publié des renseignements sur des ordonnances sur Facebook, en contravention de la loi sur les renseignements sur la santé (*Health Information Act*) de l'Alberta, a été sanctionnée par l'Ordre des pharmaciens. Son permis d'exercice a été suspendu pour quatre mois, elle a reçu une réprimande verbale et a dû payer une amende de 4 000 $, en plus des frais d'audience. De plus, une copie de la décision, y compris le nom de la pharmacienne, a été envoyée à tous les organismes de réglementation des pharmaciens au Canada[9].

8 Comité de discipline de l'Ordre des infirmières et infirmiers de l'Ontario. *Between: College of Nurses of Ontario and Registration No.HB00883*, entendu en juillet 2008. Sur Internet : https://registry.cno.org/Search/OpenPublicRegisterDocument?PublicRegisterDocumentId=6a4ebd76-8838-ea11-940b-00155d200c18

9 Sur Internet : https://pharmacists.ab.ca/sites/default/files/SonggadanDecision.pdf.

Dans une autre affaire en Alberta, un médecin qui avait utilisé le dossier de santé électronique provincial, Alberta Netcare, pour accéder à des renseignements personnels sur la santé au cours d'une instance de divorce a été sanctionné par le College of Physicians and Surgeons of Alberta. Son permis d'exercice a été suspendu pour 60 jours et on lui a ordonné de suivre un cours d'éthique et de payer les frais de l'audience et de l'enquête[10].

ENQUÊTES SUR LA PROTECTION DE LA VIE PRIVÉE

L'accès non autorisé à des renseignements personnels sur la santé peut donner lieu à une enquête et à une ordonnance du Commissaire à l'information et à la protection de la vie privée de l'Ontario. À ce jour, le CIPVP a rendu trois ordonnances concernant l'accès non autorisé à des renseignements personnels sur la santé par des dépositaires et leurs mandataires.

En 2006, une ordonnance a été rendue dans le cas d'une infirmière autorisée qui, à dix reprises, avait consulté le dossier électronique de la conjointe séparée de son petit ami, à qui elle ne fournissait pas de soins. L'ordonnance a conclu que l'infirmière avait utilisé et divulgué des renseignements personnels sur la santé en contravention de la *LPRPS*, et que l'hôpital n'avait pas pris de mesures raisonnables dans les circonstances pour protéger ces renseignements. Le personnel de l'hôpital n'a pas respecté les politiques internes de protection de la vie privée, et l'hôpital n'a pas pris de mesures immédiates pour empêcher toute autre utilisation ou divulgation non autorisée de renseignements personnels sur la santé[11].

Dans une autre affaire impliquant le même hôpital, une technologue en imagerie diagnostique a consulté, à six occasions distinctes, le dossier électronique de renseignements personnels sur la santé de la conjointe actuelle de son ancien conjoint, à qui elle ne fournissait pas de soins. L'ordonnance a conclu que la technologue avait utilisé des renseignements personnels sur la santé en contravention de la *LPRPS* et que l'hôpital n'avait pas respecté ses pratiques relatives aux renseignements ni pris de mesures raisonnables dans les circonstances pour protéger les renseignements personnels sur la santé[12].

Plus récemment, en 2014, une ordonnance a été rendue dans le cas de deux employés d'hôpital occupant des postes de bureau qui avaient utilisé ou divulgué des renseignements personnels sur la santé de mères ayant récemment accouché dans le but de vendre ou de commercialiser des régimes enregistrés d'épargne-études (REEE). L'ordonnance a conclu que les renseignements personnels sur la santé avaient été utilisés ou divulgués en contravention de

10 College of Physicians and Surgeons of Alberta. *In the Matter of a Hearing Under the Health Professions Act*, *R.S.A. 2000, c.*C-7. Sur Internet : http://cpsa.ab.ca/Libraries/pro_complaints_disc/011469-000015972511-4.pdf.

11 Commissaire à l'information et à la protection de la vie privée de l'Ontario. *Order HO-002*, rendue en juillet 2006. Sur Internet : http://www.ipc.on.ca/images/Findings/up-HO_002.pdf.

12 Commissaire à l'information et à la protection de la vie privée de l'Ontario. *Order HO-010*, rendue en décembre 2010. Sur Internet : http://www.ipc.on.ca/images/Findings/ho-010.pdf.

la *LPRPS* et que l'hôpital n'avait pas pris de mesures raisonnables dans les circonstances pour protéger les renseignements personnels sur la santé, qu'il n'avait pas respecté ses pratiques relatives aux renseignements et que celles-ci n'étaient pas conformes à la *LPRPS*[13]. Dans ces trois cas d'accès non autorisé, les hôpitaux ont reçu l'ordre de prendre un certain nombre de mesures correctives afin d'éliminer ou de réduire le risque que de telles atteintes à la vie privée ne se reproduisent.

D'autres organismes de surveillance de la protection de la vie privée au Canada ont également publié de nombreux rapports concernant l'accès non autorisé à des renseignements personnels sur la santé. Par exemple, le commissaire à l'information et à la protection de la vie privée de l'Alberta a publié un rapport d'enquête concernant un médecin qui a utilisé Alberta Netcare pour consulter les renseignements personnels sur la santé de l'ex-conjoint d'un partenaire, ainsi que de la mère et de la petite amie de l'ex-conjoint, à qui le médecin ne fournissait pas de soins, au cours d'une instance de divorce. Le médecin a accédé à des renseignements personnels sur la santé 21 fois sur une période de 15 mois en utilisant les comptes de 12 collègues différents qui n'avaient pas fermé leur session sur Alberta Netcare[14]. Le commissaire à l'information et à la protection de la vie privée de la Saskatchewan a publié un rapport d'enquête concernant un pharmacien qui a consulté les profils pharmaceutiques de trois personnes auxquelles il ne fournissait plus de soins, par souci pour leur bien-être[15]. Toujours en Saskatchewan, un rapport d'enquête a été publié concernant trois cas distincts où des employés de la Regina Qu'Appelle Regional Health Authority avaient consulté ou modifié des renseignements personnels sur la santé dans des systèmes d'information électroniques, en contravention de la loi sur la protection des renseignements sur la santé (*Health Information Protection Act*)[16]. Au Manitoba, l'ombudsman a publié un rapport concernant un employé d'ActionCancer Manitoba qui avait consulté un dossier électronique nouvellement créé contenant le nom et le numéro du registre des cancers d'un enfant dont la famille avait une relation tendue avec l'employé. Ce dernier ne fournissait pas de soins à l'enfant quand il a consulté les renseignements personnels sur la santé[17].

13 Commissaire à l'information et à la protection de la vie privée de l'Ontario. *Order HO-013*, rendue en décembre 2014. Sur Internet : http://www.ipc.on.ca/images/Findings/ho-013.pdf.

14 Information and Privacy Commissioner of Alberta. *Report of an investigation concerning misuse of the Alberta Electronic Health Record (Netcare) Covenant Health Investigation Report H2011-IR-004*, publié en novembre 2011. Sur Internet : http://www.oipc.ab.ca/downloads/documentloader.ashx?id=2912.

15 Office of the Saskatchewan Information and Privacy Commissioner. *Investigation Report H-2010-001 L & M Pharmacy Inc. Sunrise Regional Health Authority Ministry of Health*, publié en mars 2010. Sur Internet : http://www.oipc.sk.ca/Reports/H-2010-001,%20March%2023%202010.pdf.

16 Office of the Saskatchewan Information and Privacy Commissioner. *Investigation Report H-2013-001 Regina Qu'Appelle Regional Health Authority*, publié en février 2013. Sur Internet : http://www.oipc.sk.ca/What's%20New/IR-H-2013-001/Investigation%20Report%20H-2013-001.pdf.

17 Ombudsman du Manitoba. *Report with Recommendations Issued on July 20, 2012 and Response to the Recommendations under The Personal Health Information Act Cases 2011-0513 and 2011-0514* CancerCare Manitoba. Sur Internet : https://www.ombudsman.mb.ca/uploads/document/files/cases2011-0513-0514-en.pdf.

POURSUITES ET AMENDES EN CAS D'INFRACTION

L'accès non autorisé à des renseignements personnels sur la santé peut également donner lieu à des poursuites judiciaires. En Ontario, est coupable d'une infraction quiconque, recueille, utilise ou divulgue volontairement des renseignements personnels sur la santé contrairement à la *LPRPS* ou à ses règlements d'application. La personne qui est déclarée coupable d'une telle infraction est passible d'une amende d'au plus 50 000 $ dans le cas d'une personne physique ou d'au plus 250 000 $ dans le cas d'une personne morale.

À ce jour, une seule poursuite pour une infraction a été intentée en vertu de la *LPRPS*. En 2011, le Centre régional de santé de North Bay a conclu qu'une infirmière avait accédé aux renseignements personnels sur la santé de 5 800 patients en contravention de la *LPRPS*. L'infirmière a été accusée d'avoir volontairement recueilli, utilisé ou divulgué des renseignements personnels sur la santé en contravention de la *LPRPS* ou de ses règlements d'application[18].

Le fait que des accusations puissent être portées ne constitue un moyen de dissuasion efficace que dans la mesure où les dépositaires et leurs mandataires croient qu'elles le seront effectivement dans les circonstances pertinentes. Étant donné la généralisation du problème de l'accès non autorisé, il pourrait être nécessaire d'intenter plus de poursuites pour faire comprendre aux dépositaires et à leurs mandataires que l'accès non autorisé est inacceptable et ne sera pas toléré.

Il y a eu un certain nombre de poursuites pour accès non autorisé dans d'autres provinces. Par exemple, en Alberta, une employée d'un cabinet médical a été accusée en vertu de la loi sur les renseignements sur la santé (*Health Information Act*) d'avoir accédé aux renseignements personnels sur la santé de la femme d'un homme avec qui elle avait une liaison. Elle a plaidé coupable et a été condamnée à une amende de 10 000 $[19]. La pharmacienne de l'Alberta qui a consulté les dossiers des femmes de son église et a publié des renseignements relatifs à des ordonnances sur Facebook a également été accusée en vertu de la loi sur les renseignements sur la santé et a dû payer une amende et des frais d'audience totalisant 15 000 $[20]. De même, en Alberta, une femme a été reconnue coupable d'avoir sciemment accédé aux renseignements personnels sur la santé de 34 personnes en contravention de la loi sur les renseignements sur la santé, ainsi que de trois infractions au *Code criminel* liées à la falsification de documents. Elle a été condamnée à une peine d'emprisonnement avec sursis de quatre mois, suivie de huit mois de probation, pour les infractions criminelles

18 Maria Calabrese. « Hospital Ordered to Disclose Records », *North Bay Nugget*, juillet 2013. Sur Internet : http://www.nugget.ca/2013/07/05/hospital-ordered-to-disclose-record.

19 Michael Whitt et LeRoy Brower. « Health Service Provider Fined $10,000 », *Healthcare Information Management & Communications*, Canada, avril 2007. Sur Internet : http://www.healthcareimc.com/sites/default/files/previous/Volume%2021/Volume%2021%20Number%202/Health%20 Service%20Provider%20Fined%2010,000.pdf

20 Sur Internet : https://pharmacists.ab.ca/sites/default/files/SonggadanDecision.pdf.

et à une amende de 500 $ pour l'infraction à la loi sur les renseignements sur la santé[21]. En 2014, à Terre-Neuve-et-Labrador, un ancien employé de Western Health a plaidé coupable d'avoir recueilli, utilisé ou divulgué des renseignements personnels sur la santé en contravention de la loi sur les renseignements personnels sur la santé (*Personal Health Information Act*) et a été condamné à une amende de 5 000 $[22]. Toujours en 2014, un ancien employé d'Eastern Health à Terre-Neuve-et-Labrador a été condamné à une amende de 1 000 $ pour avoir recueilli, utilisé ou divulgué des renseignements personnels sur la santé en contravention de la loi sur les renseignements personnels sur la santé[23].

ACTIONS EN JUSTICE

En Ontario, une personne visée par une ordonnance du CIPVP ou touchée par une conduite qui a donné lieu à une infraction à la *LPRPS* dont une personne a été reconnue coupable et dont la déclaration de culpabilité est devenue définitive peut introduire une instance en recouvrement de dommages-intérêts pour le préjudice réel qu'elle a subi. La *LPRPS* prévoit que si le préjudice en question a résulté d'actes commis volontairement ou avec insouciance, le tribunal peut inclure dans les dommages-intérêts qu'il adjuge des dommages moraux d'au plus 10 000 $.

En 2012, la Cour d'appel de l'Ontario a reconnu une nouvelle cause d'action en common law pour atteinte à la vie privée, le délit d'« intrusion dans l'intimité »[24]. Pour établir cette cause d'action, il faut prouver que le défendeur s'est conduit de façon intentionnelle et inconsidérée, qu'il s'est ingéré, sans justification légitime, dans les affaires privées ou les préoccupations personnelles du plaignant, et qu'une personne raisonnable considérerait l'invasion comme étant très choquante et causant de la détresse, de l'humiliation ou de l'angoisse. La preuve d'un préjudice n'est pas un élément de la cause d'action. La Cour d'appel a statué que d'ordinaire, les dommages-intérêts dans une telle affaire se limitent à un maximum de 20 000 $, et que des dommages-intérêts majorés et punitifs peuvent être accordés dans des cas exceptionnels[25].

---

21 Office of the Information and Privacy Commissioner of Alberta. *Conviction in Health Information Act Investigation*, avril 2014. Sur Internet : http://oipc.ab.ca/downloads/documentloader.ashx?id=3405.

22 Office of the Information and Privacy Commissioner. *Sentence Handed Down in Personal Health Information Act Matter*, septembre 2014. Sur Internet : http://www.releases.gov.nl.ca/releases/2014/oipc/0911n08.aspx.

23 Office of the Information and Privacy Commissioner. *Sentence Handed Down in Personal Health Information Act Matter*, octobre 2014. Sur Internet : http://www.releases.gov.nl.ca/releases/2014/oipc/1009n09.aspx.

24 *Jones c. Tsige*, 2012 ONCA 32 (CanLII) Sur Internet : https://www.canlii.org/fr/on/onca/doc/2012/2012onca32/2012onca32.html.

25 Selon une décision en instance devant la Cour d'appel de l'Ontario, un hôpital a soutenu que les plaignants ne peuvent intenter une action fondée sur le délit d'intrusion dans l'intimité parce que la *LPRPS* confère au Commissaire à l'information et à la protection de la vie privée de l'Ontario la compétence exclusive sur toutes les plaintes relatives au traitement irrégulier de renseignements personnels sur la santé assujettis à la *LPRPS.* Le prononcé de la décision a été reporté. Pour des précisions, voir *Hopkins v. Kay*, 2014 ONSC 321 (CanLII). Sur Internet : http://www.canlii.org/en/on/onsc/doc/2014/2014onsc321/2014onsc321.html.

Les recours collectifs sont également de plus en plus fréquents à la suite de cas d'accès non autorisé à des renseignements personnels sur la santé. Un recours collectif d'un montant de 5,6 millions de dollars a été intenté en Ontario, invoquant le délit d'intrusion dans l'intimité. Selon les allégations, 280 dossiers de renseignements personnels sur la santé ont été intentionnellement et illégalement consultés et, dans un certain nombre de cas, diffusés de manière inappropriée, sans consentement, par le Centre régional de santé de Peterborough et sept de ses employés. La poursuite demande également des dommages-intérêts majorés et punitifs de 1 million de dollars à l'hôpital et de 50 000 $ à chaque ancien employé[26]. Un recours collectif de 412 millions de dollars a également été intenté en Ontario après que le Rouge Valley Health System eut signalé que d'anciens employés avaient utilisé ou divulgué de manière inappropriée les renseignements personnels sur la santé de près de 8 300 patients afin de vendre ou de commercialiser des REEE. L'un des anciens employés a également été accusé par la Commission des valeurs mobilières de l'Ontario d'avoir effectué des transactions non enregistrées, en contravention de la *Loi sur les valeurs mobilières*[27].

Des recours collectifs ont également été intentés ailleurs au Canada, par exemple, à Terre-Neuve-et-Labrador et en Nouvelle-Écosse, contre de nombreuses autorités sanitaires après que les plaignants eurent été informés de l'accès inapproprié à leurs renseignements personnels sur la santé[28].

26 MyKawartha.com. *Class action lawsuit filed against hospital, former staff and Fleming College*, mars 2013. Sur Internet : http://www.mykawartha.com/community-story/3715923-class-action-lawsuit-filed-against-hospital-former-staff-and-fleming-/ et *Hopkins v. Kay*, 2014 ONSC 321 (CanLII). Sur Internet : http://www.canlii.org/en/on/onsc/doc/2014/2014onsc321/2014onsc321.html.

27 Marco Chown Oved. « *Rouge Valley hospital clerk charged with misusing confidential patients records* », *Toronto Star*, novembre 2014. Sur Internet : http://www.thestar.com/news/crime/2014/11/24/hospital_clerk_charged_with_misusing_records_after_confidential_patient_files_were_sold.html.

28 Bob Buckingham Law. *Class Action Proceedings Initiated*. Sur Internet : https://www.buckinghamlaw.ca/index.php/lawsuits-filings/medical-records-privacy-breach; Patterson Law. *Class Proceeding Against Capital District Health Authority*. Sur Internet : http://www.pattersonlaw.ca/classproceedings/CapitalDistrictHealthAuthority/tabid/980/Default.aspx; Wagners. *South West Health Privacy Breach*. Sur Internet : http://www.wagners.co/South-West-Health-Privacy-Breach/.

PRÉVENIR OU RÉDUIRE LE RISQUE D'ACCÈS NON AUTORISÉ

Les dépositaires sont responsables des renseignements personnels sur la santé dont ils ont la garde ou le contrôle et des actes de leurs mandataires à l'égard de ces renseignements. L'accès non autorisé aux renseignements personnels sur la santé par des mandataires ayant des privilèges d'accès fondés sur des rôles est un risque connu pour les renseignements personnels sur la santé dans les systèmes d'information électroniques. Par conséquent, pour remplir leur obligation de prendre des mesures raisonnables dans les circonstances pour protéger les renseignements personnels sur la santé contre une utilisation ou une divulgation non autorisée, les dépositaires doivent adopter une approche à multiples facettes pour détecter, prévenir et réduire le risque d'accès non autorisé. Diverses mesures doivent être mises en œuvre pour lutter contre l'accès non autorisé, notamment des politiques et procédures de protection de la vie privée, une formation et une sensibilisation à la protection de la vie privée, des avis et avertissements de confidentialité, des ententes de confidentialité, des ententes d'utilisation, la gestion des accès, la consignation, la vérification et la surveillance, la gestion des atteintes à la vie privée et les mesures disciplinaires. Chacune de ces mesures est décrite ci-dessous.

POLITIQUES ET PROCÉDURES DE PROTECTION DE LA VIE PRIVÉE

Les dépositaires doivent élaborer et mettre en œuvre des politiques et des procédures détaillées de protection de la vie privée qui définissent les attentes et les exigences s'appliquant à tous les mandataires. Ces politiques et procédures écrites sont nécessaires pour formaliser et clarifier les pratiques requises. Elles doivent être clairement rédigées, aisément accessibles et faciles à comprendre. Elles doivent être également approuvées par la direction, communiquées dans toute l'organisation et mises en œuvre de manière cohérente.

Les politiques et procédures de protection de la vie privée doivent se traduire par des pratiques concrètes et être opérationnalisées dans l'ensemble des activités de l'organisation. Le dépositaire doit envisager, pour chaque exigence énoncée dans les politiques et procédures, la manière la plus efficace de la satisfaire par une série de pratiques concrètes, réalisables et spécifiques. Ces éléments concrets doivent clairement indiquer qui est responsable de leur exécution et comment chaque exigence sera satisfaite[29].

29 *A Policy is Not Enough: It Must be Reflected in Concrete Practices*, Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario, septembre 2012. Sur Internet : https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-policy-not-enough.pdf.

Des politiques et procédures de protection de la vie privée doivent être mises en place pour détecter, prévenir et réduire le risque d'accès non autorisé aux renseignements personnels sur la santé par les dépositaires et leurs mandataires. Il faut indiquer les fins auxquelles les renseignements personnels sur la santé peuvent être recueillis, utilisés et divulgués, ainsi que les limites, conditions ou restrictions imposées à la collecte, à l'utilisation et à la divulgation. De même, les fins auxquelles il est interdit de recueillir, d'utiliser ou de divulguer des renseignements personnels sur la santé doivent être indiquées. Les politiques et procédures de protection de la vie privée doivent préciser que, comme l'exige la *LPRPS*, les dépositaires et leurs mandataires ne doivent pas recueillir, utiliser ou divulguer de renseignements personnels sur la santé à des fins que d'autres renseignements permettent de réaliser et ne doivent pas recueillir, utiliser ou divulguer plus de renseignements personnels sur la santé qu'il n'est raisonnablement nécessaire pour réaliser la fin visée. Les politiques et procédures doivent également décrire les responsabilités des dépositaires et de leurs mandataires en ce qui concerne les mesures de précaution d'ordre administratif, technique et matériel mises en œuvre pour protéger les renseignements personnels sur la santé. Elles doivent exiger des mandataires qu'ils informent le dépositaire à la première occasion raisonnable en cas de vol ou de perte de renseignements personnels sur la santé ou d'accès à ces renseignements par des personnes non autorisées. Des politiques et procédures détaillées de protection de la vie privée doivent être mises en place, y compris, mais sans s'y limiter, sur des sujets tels que la formation et la sensibilisation à la protection de la vie privée, la signature d'ententes de confidentialité et d'ententes d'utilisation, la consignation, la vérification et la surveillance, la gestion des accès, la gestion des atteintes à la vie privée et les mesures disciplinaires.

Toutes les politiques et procédures de protection de la vie privée doivent être examinées régulièrement, au moins une fois par année, afin de déterminer s'il y a lieu de les modifier ou d'en élaborer de nouvelles. Ces politiques et procédures doivent préciser la fréquence de cet examen, la personne chargée de l'effectuer, la procédure d'examen et le délai dans lequel l'examen aura lieu. Au moment d'entreprendre l'examen et de déterminer si des modifications ou de nouvelles politiques et procédures de protection de la vie privée s'imposent, il est important de tenir compte des ordonnances, lignes directrices, feuilles-info et pratiques exemplaires publiées par le Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario, de l'évolution des normes et des pratiques exemplaires des différents secteurs d'activité en matière de protection de la vie privée, des modifications apportées à la *LPRPS* et à ses règlements, des recommandations découlant des vérifications de la protection de la vie privée et de la sécurité, des évaluations de l'incidence sur la vie privée, des évaluations des risques et des menaces et des enquêtes sur les plaintes relatives à la protection de la vie privée, les atteintes à la vie privée et

les atteintes à la sécurité de l'information. En outre, l'examen doit permettre de s'assurer que les politiques et procédures de protection de la vie privée continuent de correspondre aux pratiques réelles et que les différentes politiques et procédures mises en œuvre sont uniformes. Chaque politique de protection de la vie privée doit également préciser que les mandataires doivent la respecter ainsi que ses procédures connexes, de même que la manière dont la conformité sera assurée et par qui, et les conséquences d'une infraction.

FORMATION ET SENSIBILISATION À LA PROTECTION DE LA VIE PRIVÉE

Une formation complète sur la protection de la vie privée est un outil essentiel pour réduire le risque d'accès non autorisé aux renseignements personnels sur la santé. Les dépositaires doivent s'assurer que les mandataires sont tenus de suivre une formation initiale et continue sur la protection de la vie privée et qu'ils la suivent effectivement. De plus, les dépositaires devraient prendre des mesures pour favoriser une culture de la protection de la vie privée et sensibiliser les mandataires à leurs responsabilités en vertu de la *LPRPS* et de ses règlements d'application ainsi qu'aux politiques et procédures de protection de la vie privée en vigueur.

Les dépositaires devraient élaborer et mettre en œuvre une politique et des procédures pour s'assurer que tous les mandataires, quel que soit leur rôle, soient tenus de suivre une formation sur la protection de la vie privée avant de commencer leur emploi ou leur relation contractuelle ou autre avec le dépositaire et avant d'avoir accès aux renseignements personnels sur la santé, ainsi qu'une formation annuelle continue sur la protection de la vie privée. La politique et les procédures doivent définir le contenu minimal requis de la formation initiale et de la formation continue sur la protection de la vie privée afin que celle-ci soit formalisée et normalisée. La politique et les procédures doivent exiger que le matériel de formation à la protection de la vie privée soit examiné et mis à jour régulièrement et définir la fréquence de ces examens et mises à jour. Idéalement, le matériel de formation sur la protection de la vie privée devrait être examiné et mis à jour chaque année. La politique et les procédures doivent définir qui est responsable de l'élaboration du matériel de formation sur la protection de la vie privée, de son examen et de sa mise à jour, et de la prestation de la formation. Elles doivent également indiquer la ou les méthodes de formation qui seront utilisées. La formation sur la protection de la vie privée basée sur les rôles permet de s'assurer que les mandataires comprennent comment appliquer les politiques et procédures de protection de la vie privée dans le cadre de leurs responsabilités professionnelles, contractuelles ou autres au quotidien.

La politique et les procédures doivent exiger que la formation à la protection de la vie privée comprenne, au minimum, les éléments suivants :

- les fins auxquelles les mandataires sont autorisés à recueillir, utiliser et divulguer des renseignements personnels sur la santé;
- les conditions ou restrictions auxquelles le dépositaire assujettit la collecte, l'utilisation et la divulgation de renseignements personnels sur la santé;
- les politiques et procédures de protection de la vie privée que le dépositaire a mises en œuvre et les obligations qu'elles imposent aux mandataires;
- les obligations que la *LPRPS* et ses règlements imposent aux mandataires, y compris celle d'aviser le dépositaire à la première occasion raisonnable en cas de vol ou de perte de renseignements personnels sur la santé, ou d'accès à ces renseignements par des personnes non autorisées, et la procédure à suivre pour ce faire;
- un avis précisant que tous les cas de collecte, d'utilisation et de divulgation de renseignements personnels sur la santé seront vérifiés;
- les conséquences possibles, pour le dépositaire, de la collecte, de l'utilisation ou de la divulgation de renseignements personnels sur la santé par des mandataires en contravention de la *LPRPS*, de ses règlements ou des politiques et procédures de protection de la vie privée;
- les conséquences auxquelles s'exposent les mandataires qui recueillent, utilisent ou divulguent des renseignements personnels sur la santé en contravention de la *LPRPS*, de ses règlements ou des politiques et procédures de protection de la vie privée;
- les conséquences qu'ont déjà subies des mandataires qui ont recueilli, utilisé ou divulgué des renseignements personnels sur la santé en contravention de la *LPRPS*, de ses règlements ou des politiques et procédures de protection de la vie privée;
- les mesures de précaution d'ordre administratif, technique et matériel que le dépositaire a mises en place pour protéger les renseignements personnels sur la santé, et les obligations des mandataires quant à leur application;
- un exposé de la nature, de l'objet et des principales dispositions de l'entente de confidentialité que les mandataires doivent signer et respecter.

La politique et les procédures doivent exiger que le matériel de formation sur la protection de la vie privée soit examiné et mis à jour régulièrement afin de tenir compte, au minimum, des aspects suivants :

- les ordonnances, lignes directrices, feuilles-info et pratiques exemplaires que le CIPVP publie en vertu de la *LPRPS* ou de ses règlements;
- l'évolution des normes et pratiques exemplaires en matière de protection de la vie privée;
- l'implantation de nouvelles technologies ou la prestation de nouveaux programmes ou services;
- les modifications apportées à la *LPRPS* ou à ses règlements, ainsi que les nouvelles politiques et procédures de protection de la vie privée que le dépositaire a instaurées ou les modifications qu'il y a apportées;
- des recommandations découlant de vérifications de la protection de la vie privée et de la sécurité, d'évaluations de l'incidence sur la vie privée, d'évaluations des menaces et des risques et d'enquêtes sur des plaintes concernant la protection de la vie privée, des atteintes à la vie privée et des atteintes à la sécurité des renseignements.

La politique et les procédures doivent exiger qu'un registre soit tenu pour documenter la présence des dépositaires et de leurs mandataires à la formation initiale et continue sur la protection de la vie privée. La politique et les procédures doivent identifier la personne responsable et la procédure à suivre pour documenter les présences, identifier les mandataires qui ne se sont pas présentés à la formation sur la protection de la vie privée et s'assurer que cette formation est suivie. De même, les conséquences du défaut de participation à la formation doivent être abordées. Il est également utile de fournir aux mandataires des documents de référence tels que des manuels, des guides, des aide-mémoire ou des tableaux à conserver une fois la formation terminée. En outre, des copies des politiques et procédures de protection de la vie privée devraient être fournies ou rendues facilement accessibles en ligne.

Si la formation initiale et continue à la protection de la vie privée est cruciale, le développement d'une culture de la protection de la vie privée revêt également de l'importance et repose sur un niveau de sensibilisation à la protection de la vie privée qui va au-delà de la formation. Des communications régulières sur la protection de la vie privée constituent une démarche importante pour prévenir ou réduire le risque d'accès non autorisé aux renseignements personnels sur la santé. La politique et les procédures doivent identifier la personne responsable de promouvoir et de favoriser une culture de la protection de la vie privée et de faire de la sensibilisation à cet égard, et elles doivent définir la fréquence, la méthode et la nature des communications sur la protection de la vie privée. Un plan de communication doit également être élaboré pour rappeler fréquemment aux mandataires les politiques et procédures de protection de la vie privée mises en œuvre par le dépositaire et les obligations que ces politiques et procédures ainsi que la *LPRPS* et ses règlements lui imposent. Ce plan de

communication doit souligner les obligations des mandataires quant à l'accès aux renseignements personnels sur la santé et les conséquences possible d'un accès non autorisé. Les méthodes de communication peuvent inclure, par exemple, des courriels, des bulletins d'information et des affiches.

AVIS ET AVERTISSEMENTS DE CONFIDENTIALITÉ

Les avis rappelant aux dépositaires et à leurs mandataires leurs obligations et les conséquences d'un accès non autorisé à des renseignements personnels sur la santé en contravention de la *LPRPS*, de ses règlements et des politiques et procédures de protection de la vie privée en vigueur, peuvent également prévenir ou réduire le risque d'accès non autorisé à des renseignements personnels sur la santé.

Avant d'accéder à des renseignements personnels sur la santé dans un système d'information électronique, il y a lieu d'afficher de manière bien visible un avis de confidentialité qui, au moins :

- établit les fins auxquelles il est permis de recueillir, d'utiliser et de divulguer des renseignements personnels sur la santé;
- oblige les dépositaires et leurs mandataires à reconnaître qu'ils recueilleront, utiliseront et divulgueront des renseignements personnels sur la santé uniquement aux fins en question;
- oblige les dépositaires et leurs mandataires à reconnaître qu'ils ont lu les politiques et procédures de protection de la vie privée en vigueur, qu'ils les comprennent et qu'ils acceptent de s'y conformer;
- oblige les dépositaires et leurs mandataires à accepter de respecter leurs obligations en vertu de la *LPRPS* et de ses règlements;
- précise les conséquences en cas de non-conformité.

Les avertissements de confidentialité peuvent également servir de moyens de dissuasion importants contre l'accès non autorisé aux renseignements personnels sur la santé et peuvent aider à consigner, vérifier et surveiller les accès. Il s'agit d'une alerte ou d'un avertissement associé au dossier électronique d'un particulier. Il peut y être associé à la demande du particulier concerné ou lorsque celui-ci a refusé ou retiré son consentement à la collecte, à l'utilisation ou à la divulgation de renseignements personnels sur la santé à des fins de soins de santé. Ces avertissements sont destinés au mandataire qui tente d'accéder aux renseignements personnels sur la santé, l'informant que l'accès à ces renseignements est étroitement surveillé et qu'une alerte sera automatiquement générée et envoyée au bureau de la protection de la vie privée ou à un autre mandataire désigné du dépositaire chaque fois que l'avertissement

de confidentialité est contourné et que des renseignements personnels sur la santé sont consultés. D'après notre expérience, la possibilité d'assortir d'un avertissement les dossiers électroniques est un moyen efficace de prévenir et de détecter l'accès non autorisé aux renseignements personnels sur la santé.

Les particuliers devraient également être informés de la possibilité d'associer un avertissement de confidentialité à leur dossier électronique de renseignements personnels sur la santé. Par exemple, la déclaration publique écrite du dépositaire, qui est requise par la *LPRPS*, pourrait inclure une description de l'avertissement de confidentialité, la manière dont il peut être demandé et à qui cette demande doit être adressée.

ENTENTES DE CONFIDENTIALITÉ

Il pourrait également être possible de réduire ou d'éliminer le risque d'accès non autorisé aux renseignements personnels sur la santé en obligeant les mandataires à signer une entente de confidentialité régulièrement. Selon une telle entente, le mandataire reconnaît ses obligations et les attentes qu'il doit respecter en matière de protection de la vie privée, y compris les conséquences d'une atteinte à la vie privée.

Une entente de confidentialité devrait être signée au début de l'emploi ou de la relation contractuelle ou autre avec le dépositaire, et chaque année par la suite. Cette entente devrait au moins :

- indiquer les fins auxquelles les mandataires sont autorisés à recueillir, utiliser et divulguer des renseignements personnels sur la santé, ainsi que les limites, conditions ou restrictions imposées à la collecte, à l'utilisation et à la divulgation de ces renseignements;
- interdire aux mandataires de recueillir, d'utiliser ou de divulguer des renseignements personnels sur la santé à une fin que d'autres renseignements permettent de réaliser et de recueillir, d'utiliser ou de divulguer plus de renseignements personnels sur la santé que ce qui est raisonnablement nécessaire pour réaliser la fin visée;
- exiger des mandataires qu'ils reconnaissent avoir lu, et compris, les politiques et procédures de protection de la vie privée en vigueur et qu'ils acceptent de s'y conformer;
- exiger des agents qu'ils rendent de façon sécuritaire tous les biens du dépositaire, y compris les clés et les dossiers de renseignements personnels sur la santé, le cas échéant, à la fin de leur emploi, de leur contrat ou de toute autre relation avec le dépositaire;
- préciser que des vérifications aléatoires seront effectuées;

- exiger que les mandataires se conforment à la *LPRPS* et à ses règlements;
- exiger des agents qu'ils informent le dépositaire à la première occasion raisonnable, conformément à la politique et aux procédures de gestion des atteintes à la vie privée, d'une infraction réelle ou présumée de l'entente de confidentialité, de la *LPRPS* ou de ses règlements, ou des politiques et procédures de protection de la vie privée;
- préciser les conséquences d'une infraction, par exemple des mesures disciplinaires comprenant la fin ou une suspension de l'emploi, de la relation contractuelle ou autre avec le dépositaire et, le cas échéant, un rapport à l'ordre professionnel de la santé du mandataire.

ENTENTES D'UTILISATION

Afin de réduire le risque d'accès non autorisé, l'utilisation de chaque système d'information électronique contenant des renseignements personnels sur la santé devrait être assujettie à une entente d'utilisation qui définit les rôles et les obligations de toutes les parties qui utilisent le système. Les dépositaires devraient veiller à ce que leurs mandataires signent une entente d'utilisation avant d'obtenir l'accès à des renseignements personnels sur la santé dans des systèmes d'information électroniques et, au moins, chaque année par la suite. L'entente d'utilisation doit :

- définir les fins auxquelles les renseignements personnels sur la santé peuvent être recueillis, utilisés et divulgués au moyen du système d'information électronique;
- exiger des dépositaires et de leurs mandataires qu'ils reconnaissent avoir lu et compris les politiques et procédures de protection de la vie privée relatives au système d'information électronique et qu'ils acceptent de s'y conformer;
- exiger que les dépositaires et leurs mandataires se conforment à la *LPRPS* et à ses règlements;
- exiger des dépositaires et de leurs mandataires qu'ils mettent en œuvre les mesures de précaution d'ordre administratif, technique et matériel prévues dans l'entente d'utilisation pour protéger les renseignements personnels sur la santé conservés dans le système d'information électronique;
- préciser les conséquences d'une infraction à l'entente d'utilisation;
- exiger un avis, conformément à la politique et aux procédures de gestion des atteintes à la vie privée, si une atteinte à la vie privée réelle ou présumée s'est produite ou est sur le point de se produire.

GESTION DES ACCÈS

Le fait de restreindre l'accès aux renseignements personnels sur la santé en fonction du besoin de connaître contribue à minimiser le risque d'accès non autorisé. Une politique et des procédures devraient être mises en place pour limiter l'accès aux renseignements personnels sur la santé et leur utilisation en fonction du principe du besoin de connaître. L'objectif de cette politique et de ces procédures est de s'assurer que, comme l'exige la *LPRPS*, les renseignements personnels sur la santé ne sont pas recueillis, utilisés ou divulgués à une fin que d'autres renseignements permettent de réaliser, et qu'on ne recueille, utilise ou divulgue pas plus de renseignements qu'il n'est raisonnablement nécessaire pour réaliser la fin visée.

La politique et les procédures doivent indiquer la personne responsable et le processus à suivre pour accorder l'accès initial aux renseignements personnels sur la santé en fonction du rôle et pour réviser ou révoquer l'accès aux renseignements personnels sur la santé lorsque le niveau d'accès requis change, par exemple lorsque l'emploi du mandataire ou sa relation contractuelle ou autre avec le dépositaire est suspendu ou prend fin ou que ses fonctions changent. La politique et les procédures doivent également définir les différents niveaux d'accès basés sur les rôles qui peuvent être accordés, ainsi que les exigences qui doivent être satisfaites avant d'approuver ou de refuser une demande d'accès.

Si le mandataire n'a besoin d'accéder à des renseignements personnels sur la santé que pendant une période déterminée, la politique et les procédures doivent définir le processus permettant de s'assurer que l'accès et l'utilisation des renseignements personnels sur la santé ne sont autorisés que pendant cette période.

La politique et les procédures devraient exiger que le dépositaire tienne un registre des mandataires qui se voient accorder l'accès à des renseignements personnels sur la santé et désigner la personne responsable de la tenue de ce registre. Le registre devrait, à tout le moins, comprendre l'identité du mandataire à qui l'accès a été accordé, une description des renseignements personnels sur la santé auxquels le mandataire a été autorisé à accéder, le niveau d'accès accordé, la date d'approbation, la date à laquelle l'accès a été accordé et la date de révocation, le cas échéant. Le registre doit être examiné régulièrement pour s'assurer que seuls les mandataires qui ont besoin d'accéder à des renseignements personnels sur la santé dans le cadre de leurs fonctions y ont accès, et que les mandataires n'ont pas accès à plus de renseignements personnels sur la santé que ce qui est raisonnablement nécessaire dans le cadre de leurs fonctions.

La politique et les procédures doivent également définir des mesures d'ordre matériel, technique et administratif supplémentaires pour limiter l'accès des

mandataires aux renseignements personnels sur la santé. Par exemple, des contrôles par mots de passe et des contrôles de recherche sont deux mesures importantes qui peuvent contribuer à minimiser le risque d'accès non autorisé.

En ce qui concerne les contrôles par mots de passe, il faut souligner que le mandataire peut contourner la détection d'un accès non autorisé à des renseignements personnels sur la santé en utilisant les données d'accès d'un autre mandataire du dépositaire pour accéder à des renseignements. Par exemple, dans un cas d'accès non autorisé, le médecin a pu accéder à des renseignements personnels sur la santé en utilisant les données d'accès d'autres mandataires qui n'avaient pas fermé leur session sur Alberta Netcare[30]. Les mots de passe forts constituent la première ligne de défense contre l'accès non autorisé aux renseignements personnels sur la santé. En général, les mots de passe forts ne contiennent aucun mot du dictionnaire et sont composés d'une combinaison d'au moins huit lettres, chiffres et symboles, l'idéal étant d'en avoir au moins 14. Il devrait également être interdit aux mandataires de noter ou de partager leurs mots de passe et leurs noms d'utilisateur uniques et ils devraient être tenus de changer régulièrement leurs mots de passe. Les mandataires doivent également être tenus de se déconnecter des systèmes d'information électroniques après les avoir utilisés, afin de réduire le risque qu'un autre mandataire puisse utiliser leurs données d'accès pour accéder à des renseignements personnels sur la santé à des fins non autorisées. Le cas échéant, il est possible de mettre en place des contraintes de temps automatiques prévoyant la déconnexion de l'utilisateur ou le verrouillage de l'écran de l'ordinateur après une courte période d'inactivité.

En ce qui concerne les contrôles de recherche, il est important de noter que la fonctionnalité de recherche ouverte peut faciliter l'accès non autorisé aux renseignements personnels sur la santé dans les systèmes d'information électroniques. Par exemple, dans le cas de l'atteinte à la vie privée impliquant l'utilisation et la divulgation de renseignements personnels sur la santé dans le but de vendre ou de commercialiser des REEE, des mandataires de l'hôpital ont pu obtenir des listes de femmes ayant récemment accouché en effectuant des recherches ouvertes dans un index de patients. Pour éviter ce genre de situation, les dépositaires doivent veiller à ce que la quantité de renseignements personnels sur la santé qui s'affiche à la suite d'une recherche soit limitée, tout en permettant aux mandataires de s'acquitter de leurs tâches professionnelles, contractuelles ou autres. Les fonctionnalités et les capacités de recherche des systèmes d'information électroniques contenant des renseignements personnels sur la santé devraient interdire les recherches illimitées de personnes. Idéalement, ces systèmes devraient être configurés de manière à ce que les critères de recherche ne permettent de localiser qu'un seul dossier de renseignements personnels sur la santé. Si cela n'est pas possible, ils devraient

30 Information and Privacy Commissioner of Alberta, *supra*, note 14.

être configurés afin qu'un maximum de cinq dossiers de renseignements personnels sur la santé soient affichés à la suite d'une recherche.

CONSIGNATION, VÉRIFICATION ET SURVEILLANCE

Il importe de consigner, de vérifier et de surveiller tous les accès aux dossiers électroniques de renseignements personnels sur la santé pour assurer la protection de la vie privée des particuliers et la confidentialité de leurs renseignements personnels sur la santé. La capacité de consigner tous les cas où des renseignements personnels sur la santé sont recueillis, utilisés et divulgués par des mandataires permettra aux dépositaires de répondre aux demandes d'information et aux plaintes concernant la collecte, l'utilisation ou la divulgation de renseignements personnels sur la santé concernant un particulier; de vérifier et de surveiller toutes les collectes, utilisations et divulgations de renseignements personnels sur la santé par tous leurs mandataires; et d'enquêter sur les atteintes réelles ou présumées à la vie privée, y compris les cas d'accès non autorisé.

La consignation, la vérification et la surveillance peuvent constituer un moyen efficace de dissuader les mandataires d'accéder à des renseignements sans autorisation, si les mandataires sont informés que toutes leurs activités liées aux dossiers électroniques de renseignements personnels sur la santé seront consignées, vérifiées et surveillées de façon continue, ciblée et aléatoire, comme il est décrit ci-dessous. Les mandataires doivent également être informés de la détection de cas antérieurs d'accès non autorisé par d'autres mandataires du dépositaire et des mesures disciplinaires qui ont été imposées dans ces circonstances.

Les dépositaires devraient élaborer une politique et des procédures de consignation, de vérification et de surveillance de tous les systèmes d'information électroniques contenant des renseignements personnels sur la santé. La politique devrait, au minimum, exiger du dépositaire qu'il veille à ce que tous ces systèmes soient en mesure de consigner tous les cas où tout ou partie des renseignements sont recueillis, utilisés et divulgués par tous leurs mandataires, ainsi que tous les cas où tout ou partie des renseignements sont recueillis, utilisés ou divulgués à la suite d'une dérogation à une directive en matière de consentement ou du contournement d'un avertissement de confidentialité.

En ce qui concerne la consignation de toutes les collectes, utilisations et divulgations de renseignements personnels sur la santé, la politique et les procédures doivent préciser les types de registres que le dépositaire est tenu de créer et de conserver, le contenu minimal de chaque type de registre, la durée minimale de conservation de chacun et la personne responsable de sa conservation.

La politique et les procédures doivent exiger la consignation de tous les cas où tout ou partie des renseignements personnels sur la santé contenus dans un système d'information électronique sont recueillis, utilisés et divulgués afin, au minimum, de déterminer :

- le particulier auquel se rapportent les renseignements personnels sur la santé;
- les types de renseignements personnels sur la santé qui ont été recueillis, utilisés ou divulgués;
- le mandataire qui a recueilli, utilisé ou divulgué les renseignements personnels sur la santé;
- la date, l'heure et le lieu de la collecte, de l'utilisation et de la divulgation des renseignements personnels sur la santé.

La politique et les procédures devraient exiger que les registres de tous les cas où la totalité ou une partie des renseignements personnels sur la santé contenus dans un système d'information électronique sont recueillis, utilisés ou divulgués à la suite du contournement d'une directive en matière de consentement ou d'un avertissement de confidentialité indiquent également le but de la collecte, de l'utilisation ou de la divulgation des renseignements personnels sur la santé, le cas échéant. Par exemple, lorsqu'une directive en matière de consentement est retirée avec le consentement exprès du particulier concerné, le registre doit le préciser.

Dans le cas des systèmes d'information électroniques que se partagent des dépositaires, les registres devraient également identifier le dépositaire qui a fourni les renseignements personnels sur la santé au système d'information électronique partagé et le dépositaire au nom duquel le mandataire a recueilli, utilisé ou divulgué les renseignements.

En ce qui concerne la vérification et la surveillance des registres, la politique et les procédures doivent définir les types de vérification et de surveillance qui doivent être effectués à l'aide des registres; la procédure à suivre pour chaque type de vérification et de surveillance; la personne responsable de chaque type; la fréquence à laquelle chaque type de vérification et de surveillance doit être effectué; les critères à utiliser pour chacun; la procédure à suivre pour examiner les résultats de la vérification et de la surveillance et y donner suite; et la procédure à suivre si une atteinte réelle ou présumée à la vie privée est décelée.

La politique et les procédures doivent obliger le dépositaire à effectuer une vérification et une surveillance continues, ciblées (réactives) et aléatoires (proactives) des registres, comme décrit ci-dessous.

La politique et les procédures doivent exiger une vérification et une surveillance continues lorsqu'il existe une directive de consentement ou un avertissement

de confidentialité. Plus précisément, la politique et les procédures devraient exiger que, chaque fois que des renseignements personnels sur la santé sont recueillis, utilisés ou divulgués à la suite de la dérogation à une directive de consentement ou du contournement d'un avertissement de confidentialité, une alerte ou un avis soit envoyé au bureau de la protection de la vie privée ou à un autre mandataire désigné du dépositaire au nom duquel les renseignements personnels sur la santé ont été recueillis, utilisés ou divulgués. La politique et les procédures devraient exiger que le bureau de la protection de la vie privée ou l'autre mandataire désigné vérifie et surveille tous les cas où des renseignements personnels sur la santé sont recueillis, utilisés ou divulgués à la suite de la dérogation à une directive en matière de consentement ou du contournement d'un avertissement de confidentialité afin d'assurer la conformité aux préférences de consentement d'une personne et à la *LPRPS*. La politique et les procédures devraient également exiger que le bureau de la protection de la vie privée ou l'autre mandataire désigné avise la personne à laquelle les renseignements se rapportent chaque fois que des renseignements personnels sur la santé sont recueillis, utilisés ou divulgués à la suite d'une dérogation à une directive en matière de consentement ou du contournement d'un avertissement de confidentialité afin d'assurer la conformité.

La politique et les procédures doivent exiger qu'une vérification et une surveillance ciblées soient effectuées en réponse aux demandes ou aux plaintes de particuliers concernant la collecte, l'utilisation ou la divulgation de leurs renseignements personnels sur la santé, et chaque fois qu'une atteinte réelle ou présumée à la vie privée est décelée.

La politique et les procédures devraient également exiger du dépositaire qu'il effectue une vérification et une surveillance aléatoires de toutes les collectes, utilisations et divulgations de renseignements personnels sur la santé que font tous ses mandataires. Afin de décourager et de détecter les accès non autorisés, la vérification et la surveillance aléatoires peuvent comprendre l'examen, par exemple, de tous les mandataires qui ont accédé à un système d'information électronique pendant une période déterminée; de tous les mandataires qui ont accédé aux renseignements personnels sur la santé d'une personne en particulier, comme une personnalité, un politicien ou un autre personnage bien connu, pendant une période déterminée; de tous les mandataires qui ont accédé aux renseignements personnels sur la santé d'une ou de plusieurs personnes portant le même nom de famille que le mandataire; de tous les mandataires qui ont accédé aux renseignements personnels sur la santé d'une ou de plusieurs personnes portant leur nom de famille; et de toutes les personnes dont les renseignements personnels sur la santé ont été consultés par un mandataire particulier pendant une période déterminée[31].

31 Association des hôpitaux de l'Ontario et Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario. *Preventing/Reducing Unauthorized Access to Personal Health Information*, novembre 2012. Sur Internet : http://www.oha.com/KnowledgeCentre/Library/Documents/Final%20-%20PHIPA%20Primer.pdf.

Il existe également des outils de vérification tiers qui peuvent analyser systématiquement et automatiquement les registres des accès et générer des rapports en fonction de critères de recherche définis. En automatisant les processus manuels grâce à une variété de requêtes basées sur les exigences spécifiques d'un dépositaire, les outils tiers peuvent contribuer à améliorer l'efficacité des vérifications et permettre des examens plus efficaces des tendances d'utilisation. Les outils de vérification spécialisés peuvent aider à prévenir et à détecter l'accès non autorisé aux renseignements personnels sur la santé en enregistrant les tendances relatives à l'accès et à l'activité des mandataires dans les systèmes d'information électroniques, en surveillant et en analysant le comportement des mandataires pour déceler les tendances qui pourraient indiquer une utilisation abusive, et en générant des alertes ou des rapports afin de limiter les activités non autorisées et de déclencher d'autres vérifications.

GESTION DES ATTEINTES À LA VIE PRIVÉE

En ce qui concerne les atteintes à la vie privée, les dépositaires et leurs mandataires sont soumis à un certain nombre d'obligations énoncées dans la *LPRPS*. Celle-ci exige que les dépositaires prennent des mesures raisonnables dans les circonstances pour s'assurer que les renseignements personnels sur la santé dont ils ont la garde ou le contrôle sont protégés contre le vol, la perte, l'utilisation ou la divulgation non autorisée et que les dossiers contenant des renseignements personnels sur la santé sont protégés contre la duplication, la modification ou l'élimination non autorisée. La *LPRPS* exige également que les dépositaires avisent les particuliers à la première occasion raisonnable en cas de perte ou de vol de leurs renseignements personnels sur la santé ou d'accès par des personnes non autorisées. Les mandataires sont également tenus d'aviser le dépositaire à la première occasion raisonnable si des renseignements personnels sur la santé traités par le mandataire au nom du dépositaire sont volés, perdus ou consultés par des personnes non autorisées.

Afin de se conformer à leurs obligations en vertu de la *LPRPS*, les dépositaires devraient être en mesure de réagir rapidement et efficacement lorsqu'un accès non autorisé à des renseignements personnels sur la santé est soupçonné ou décelé. Ils doivent élaborer et mettre en œuvre une politique et des procédures de gestion des atteintes à la vie privée prévoyant comment déceler et signaler les atteintes à la vie privée présumées ou réelles, les maîtriser, notifier les personnes concernées, mener une enquête à leur sujet et prendre des mesures correctives. Cette politique et ces procédures devraient permettre au dépositaire de réagir rapidement et de manière coordonnée, de clarifier les rôles et les responsabilités, de documenter les processus permettant de déceler de maîtriser les atteintes à la vie privée, d'enquêter à leur sujet de prendre des

mesures correctives, de veiller à ce que les particuliers, la haute direction et éventuellement d'autres tiers soient informés des atteintes à la vie privée et de préparer le dépositaire à une éventuelle intervention du Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario[32].

La politique et les procédures de gestion des atteintes à la vie privée doivent imposer aux mandataires l'obligation d'aviser le dépositaire en cas de vol ou de perte de renseignements personnels sur la santé ou d'accès à ceux-ci par des personnes non autorisées, et préciser qui, au sein de l'organisation, doit être avisé et dans quel délai. La politique doit exiger des mandataires qu'ils signalent toute atteinte à la vie privée à la haute direction et préciser qui est responsable de ce signalement, le délai dans lequel ce signalement doit être effectué et à qui l'atteinte à la vie privée doit être signalée. Elle doit également préciser les circonstances dans lesquelles une atteinte à la vie privée doit être signalée à d'autres personnes, notamment à la police, aux ordres professionnels de la santé et au Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario.

La politique et les procédures de gestion des atteintes à la vie privée doivent exiger que des mesures raisonnables dans les circonstances soient prises immédiatement pour maîtriser l'atteinte à la vie privée et protéger les renseignements personnels sur la santé contre tout vol et toute perte, utilisation ou communication non autorisée et protéger les dossiers de renseignements personnels sur la santé contre toute duplication, modification ou élimination non autorisée. En cas d'accès non autorisé, le dépositaire doit prendre toutes les mesures nécessaires pour maîtriser l'atteinte à la vie privée, par exemple en suspendant immédiatement l'accès du mandataire soupçonné de l'atteinte à la vie privée aux renseignements personnels sur la santé, en attendant les résultats d'une enquête. Il doit récupérer toutes les copies papier des renseignements personnels sur la santé qui ont été divulguées et s'assurer qu'aucune copie n'a été faite ou conservée par des personnes non autorisées. Le dépositaire devrait déterminer si l'atteinte à la vie privée permettrait la collecte, l'utilisation ou la divulgation non autorisée de tout autre renseignement personnel sur la santé et prendre des mesures pour s'assurer que d'autres atteintes à la vie privée ne puissent se produire par des moyens identiques ou similaires.

La politique et les procédures de gestion des atteintes à la vie privée doivent exiger la notification des personnes concernées conformément à la *LPRPS*, et indiquer qui est responsable de la notification et les informations à fournir.

Lorsqu'ils informent des particuliers d'une atteinte à la vie privée, les dépositaires doivent leur fournir les informations suivantes :

32 Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario. *Que faire en cas d'atteinte à la vie privée : Lignes directrices pour le secteur de la santé*. Sur Internet : https://www.ipc.on.ca/wp-content/uploads/2016/10/what-to-do-when-faced-with-a-privacy-breach-fr.pdf.

- le nom de chaque mandataire qui a causé l'atteinte à la vie privée;
- la date et l'heure auxquelles a eu lieu l'atteinte à la vie privée;
- une description de la nature et de la portée de l'atteinte à la vie privée;
- une description des renseignements personnels sur la santé qui ont fait l'objet de l'atteinte à la vie privée;
- les mesures prises pour maîtriser l'atteinte à la vie privée;
- un avis indiquant qu'à la suite de l'enquête, le dépositaire fournira au particulier un résumé des résultats de l'enquête et des mesures qui ont été ou seront prises pour remédier à l'atteinte à la vie privée et pour prévenir des atteintes semblables à l'avenir;
- les mesures que le particulier peut prendre pour protéger sa vie privée ou pour minimiser les conséquences de cette atteinte à la vie privée;
- le nom et les coordonnées de la personne à qui le particulier peut adresser ses demandes de renseignements et ses préoccupations;
- des renseignements sur la façon de déposer une plainte auprès du Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario.

La politique et les procédures de gestion des atteintes à la vie privée doivent exiger qu'une enquête sur l'atteinte à la vie privée soit menée, y compris un examen de tous les systèmes d'information électroniques pertinents et des politiques et procédures de protection de la vie privée; elles doivent préciser qui est responsable de la conduite de l'enquête, la nature et la portée de celle-ci et le processus à suivre pour la mener à bien. Elles doivent aussi décrire le processus par lequel les conclusions de l'enquête, y compris les recommandations, sont communiquées et mises en œuvre, le calendrier de mise en œuvre et la personne responsable.

Une fois l'enquête terminée, la politique et les procédures de gestion des atteintes à la vie privée devraient exiger que le dépositaire fournisse au particulier un résumé des résultats de l'enquête et des mesures qui ont été ou seront mises en œuvre pour remédier à l'atteinte à la vie privée et pour prévenir des atteintes similaires à l'avenir.

La politique et les procédures de gestion des atteintes à la vie privée doivent exiger du dépositaire qu'il tienne un registre des atteintes à la vie privée, qu'il en définisse le contenu et qu'il désigne une personne responsable de la tenue de ce registre. Celui-ci doit comprendre les éléments suivants pour chaque atteinte à la vie privée :

- le nom du mandataire à l'origine de cette atteinte à la vie privée, lorsqu'il est jugé pertinent, comme dans le cas d'un accès non autorisé;
- la date et l'heure auxquelles a eu lieu l'atteinte à la vie privée;
- la nature, la portée et la cause de l'atteinte à la vie privée;
- une description des renseignements personnels sur la santé qui ont fait l'objet de l'atteinte à la vie privée;
- les mesures prises pour maîtriser l'atteinte à la vie privée;
- les mesures qui ont été ou seront mises en œuvre pour remédier à cette atteinte à la vie privée et pour prévenir des atteintes similaires à l'avenir;
- les échéanciers et les personnes responsables de la mise en œuvre des mesures visant à remédier à cette atteinte à la vie privée et à prévenir des atteintes similaires à l'avenir;
- la manière dont chaque mesure a été ou est censée être mise en œuvre.

La politique et les procédures de gestion des atteintes à la vie privée devraient exiger du dépositaire qu'il vérifie et surveille le registre des atteintes à la vie privée afin de repérer les tendances en la matière, de déterminer les mesures de précaution d'ordre administratif, matériel ou technique qui devraient être mises en place pour prévenir ou réduire au minimum le risque d'atteinte à la vie privée et de s'assurer que des mesures sont prises pour remédier aux atteintes à la vie privée et prévenir des atteintes semblables à l'avenir. Par exemple, si le dépositaire détecte une augmentation de la fréquence des atteintes à la vie privée impliquant un accès non autorisé à des renseignements personnels sur la santé, il pourrait être amené à revoir ses politiques et procédures de consignation, de vérification et de surveillance ou les mesures disciplinaires imposées pour ces atteintes à la vie privée.

MESURES DISCIPLINAIRES

L'imposition de mesures disciplinaires cohérentes, appropriées et proportionnelles fait savoir aux mandataires que les atteintes à la vie privée sont prises au sérieux et peut servir de moyen de dissuasion efficace contre l'accès non autorisé aux renseignements personnels sur la santé. Les dépositaires doivent adopter une politique et des procédures concernant les mesures disciplinaires et correctives. Cette politique et ces procédures devraient traiter de l'enquête sur les questions disciplinaires; des types de mesures disciplinaires et correctives qui peuvent être imposées, par exemple, une lettre d'avertissement, une suspension avec ou sans salaire, et la fin de l'emploi ou de la relation contractuelle ou autre avec le dépositaire; des circonstances dans lesquelles les actions des mandataires seront signalées à des tiers, y compris la police, leur ordre professionnel de la santé ou

le procureur général, pour qu'une poursuite soit intentée en vertu de la *LPRPS*; et des facteurs à prendre en considération pour déterminer les mesures disciplinaires et correctives appropriées.

Les mandataires doivent être informés de la politique et des procédures disciplinaires du dépositaire, ainsi que des conséquences éventuelles de l'accès non autorisé aux renseignements personnels sur la santé en vertu de la *LPRPS*. Par exemple, les mandataires peuvent être informés des mesures disciplinaires et des autres conséquences d'un accès non autorisé dans le cadre d'une formation sur la protection de la vie privée et de communications de sensibilisation à la protection de la vie privée et par la signature d'ententes de confidentialité contenant des dispositions relatives aux mesures disciplinaires. Les mandataires doivent être informés d'exemples précis d'atteintes à la vie privée survenues au sein de l'organisation et des mesures disciplinaires qui ont été imposées. Le fait de rappeler à plusieurs reprises aux mandataires que l'accès non autorisé aux renseignements personnels sur la santé n'est pas toléré, tant dans les politiques que dans la pratique, peut avoir un effet dissuasif et prévenir les atteintes à la vie privée.

CONCLUSION

L'accès non autorisé aux renseignements personnels sur la santé par les dépositaires et leurs mandataires semble être un problème répandu dont les conséquences négatives sont vastes et de grande portée. Il peut causer des préjudices aux particuliers et porter atteinte irrémédiablement aux relations de confiance entre les dépositaires et les personnes à qui ils fournissent des soins de santé. Parmi les autres répercussions éventuelles de l'accès non autorisé, mentionnons les procédures disciplinaires, les enquêtes et les ordonnances relatives à la protection de la vie privée, les poursuites pour des infractions à la *LPRPS* et les poursuites judiciaires.

Il faut que les dépositaires et leurs mandataires reconnaissent que la question de l'accès non autorisé aux renseignements personnels sur la santé, quel qu'en soit le motif, est importante et qu'elle doit être prise au sérieux. La protection de la vie privée devrait faire partie intégrante de la prestation des soins de santé et être intégrée dans la culture des organisations de soins de santé. L'élaboration et la mise en œuvre d'une approche globale, comprenant une variété de mesures et veillant à ce que les mandataires soient au courant des politiques et procédures pertinentes en matière de protection de la vie privée, peuvent grandement contribuer à minimiser le risque d'accès non autorisé aux renseignements personnels sur la santé. Un message fort doit être envoyé : l'accès non autorisé aux renseignements personnels sur la santé par les dépositaires et leurs mandataires est inacceptable et ne sera pas toléré, et les coupables s'exposent à de graves conséquences.

DÉCELER ET PRÉVENIR L'ACCÈS NON AUTORISÉ ET EN RÉDUIRE LE RISQUE

1. Élaborer et mettre en œuvre des politiques et des procédures détaillées de protection de la vie privée qui définissent les attentes et les obligations de tous les mandataires en matière de protection des renseignements personnels sur la santé.

2. Élaborer et mettre en œuvre un programme complet de formation et de sensibilisation à la protection de la vie privée qui exige que tous les mandataires suivent une formation sur la protection de la vie privée au début de leur emploi ou de leur relation contractuelle ou autre avec le dépositaire et avant d'avoir accès aux renseignements personnels sur la santé, ainsi qu'une formation annuelle continue sur la protection de la vie privée, afin de s'assurer qu'ils comprennent les attentes et leurs obligations en matière de protection des renseignements personnels sur la santé en vertu des politiques et procédures de protection de la vie privée du dépositaire et de la *LPRPS*.

3. Veiller à ce que les systèmes d'information électroniques qui contiennent des renseignements personnels sur la santé dont le dépositaire a la garde ou le contrôle comportent des avis et des avertissements de confidentialité.

4. Exiger de tous les mandataires qu'ils signent une entente de confidentialité avant d'avoir accès à des renseignements personnels sur la santé et, par la suite, tous les ans, afin de reconnaître les attentes et leurs obligations en matière de protection des renseignements personnels sur la santé en vertu des politiques et procédures de protection de la vie privée du dépositaire ainsi que de la *LPRPS*.

5. Exiger que tous les mandataires signent des ententes d'utilisation reconnaissant les attentes et leurs obligations relatives aux renseignements personnels sur la santé dans les systèmes d'information électroniques avant de se voir accorder l'accès et chaque année par la suite.

6. Élaborer et mettre en œuvre des politiques et des procédures détaillées ainsi que des mesures d'ordre matériel, technique et administratif, telles que des contrôles par mots de passe et des contrôles de recherche, afin de limiter l'accès aux renseignements personnels sur la santé et leur utilisation par les mandataires, selon le principe du besoin de connaître.

7. Veiller à ce que tous les accès aux renseignements personnels sur la santé dans les systèmes d'information électroniques soient consignés, vérifiés et surveillés de manière continue, ciblée (réactive) et aléatoire (proactive).

8. Élaborer et mettre en œuvre une politique et des procédures détaillées de gestion des atteintes à la vie privée qui permettent de déceler les atteintes présumées ou réelles à la vie privée, de les signaler, de les maîtriser, d'aviser les personnes concernées, de faire enquête à leur sujet et d'y remédier.

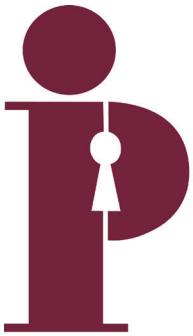
9. Élaborer et mettre en œuvre une politique et des procédures qui définissent les types de mesures disciplinaires ou correctives qui peuvent être imposées aux mandataires en cas d'atteinte à la vie privée, y compris la fin de l'emploi ou de la relation contractuelle ou autre avec le dépositaire, et les circonstances dans lesquelles les actes des mandataires peuvent être signalés à des tiers, y compris la police, leur ordre professionnel de la santé ou le procureur général, pour qu'une poursuite soit intentée en vertu de la *LPRPS*.

AU SUJET DU COMMISSAIRE À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE

Le rôle du Commissaire à l'information et à la protection de la vie privée est prévu dans trois lois : la Loi sur l'accès à l'information et la protection de la vie privée, la Loi sur l'accès à l'information municipale et la protection de la vie privée et la Loi sur la protection des renseignements personnels sur la santé. La commissaire est indépendante du gouvernement et s'emploie à promouvoir la transparence du gouvernement et la protection de la vie privée.

Aux termes de ces trois lois, la commissaire :

- traite les plaintes et tranche les appels concernant l'accès à l'information lorsque le gouvernement ou les praticiens de la santé et organismes de santé refusent d'accorder l'accès aux renseignements demandés ou leur rectification;
- mène des enquêtes sur les plaintes relatives aux renseignements personnels que le gouvernement ou les praticiens de la santé et organismes de santé détiennent;
- effectue des recherches sur les questions touchant l'accès à l'information et la protection de la vie privée;
- formule des observations sur des lois et des programmes proposés par le gouvernement;
- informe le public concernant les lois ontariennes sur l'accès à l'information et la protection de la vie privée.



Information and Privacy
Commissioner of Ontario

Commissaire à l'information et à la
protection de la vie privée de l'Ontario

Commissaire à l'information et à la protection de la vie privée
de l'Ontario
2, rue Bloor Est
Toronto, Ontario
Canada M4W 1A8

Site web : www.ipc.on.ca/fr/
Téléphone: 416-326-3333
Courriel : info-fr@ipc.on.ca

Janvier 2015