RAPPORT DES CONCLUSIONS DE L'ENQUÊTE DE LA COMMISSAIRE

Loi sur l'accès et la protection en matière de renseignements personnels sur la santé

Affaire de notification d'une atteinte à la vie privée : 2011-423-H-136
Affaires : 2011-491-H-151, 2011-492-H-152, 2011-494-H-153, 2011-495-H-154, 2011-497-H-156, 2011-502-H-157, 2011-508-H-158, 2011-516-H-161, 2011-522-H-164, 2011-569-H-182, 2011-591-H-190

Date : 9 février 2012
Commissariat à l'accès à l'information et à la protection de la vie privée du Nouveau-Brunswick

Atteinte à la vie privée

La Docteure S. Sanderson est une endocrinologue pédiatrique qui œuvre au sein du service de pédiatrie de la clinique externe de l'Hôpital régional de Saint John (ci-après « l'Hôpital »). Elle est médecin salarié à l'emploi du Réseau de santé Horizon. En novembre 2010, l'adjointe administrative de la Docteure Sanderson s'est rendu compte qu'une clé USB servant à la sauvegarde de renseignements sur la santé des patients avait disparu.

Mentionnons, en guise de mise en situation pour cette affaire, qu'une base de données contenant des renseignements sur les patients a été créée au bureau de la Docteure Sanderson il y a cinq ou six ans. Cette base de données contient des renseignements personnels sur la santé des enfants traités par la Docteure Sanderson au cours des 15 ou 16 dernières années, soit quelque 1 600 patients. La base de données était enregistrée sur l'ordinateur de bureau principal de la Docteure Sanderson, qui est intégré au système de technologie de l'information de l'Hôpital.

Pour pouvoir servir les patients, le personnel du bureau de la Docteure Sanderson devait récupérer des données dans cette base de données. Certaines tâches administratives telles que l'organisation des visites, la prise de rendez-vous, les tests et le suivi auprès des patients exigeaient un programme informatique capable de répondre à ces besoins. Autrement dit, le bureau de la Docteure Sanderson avait besoin d'un programme de gestion des données. Or, les services de technologie de l'information de l'Hôpital ne prennent pas en charge les logiciels de gestion des données. En fait, l'utilisation du logiciel Excel à cette fin était pratique courante à l'Hôpital, car ce logiciel répondait aux besoins particuliers des médecins pour servir leurs patients. Le bureau de la Docteure Sanderson a choisi, lui aussi, le logiciel Excel pour créer cette base de données servant à la gestion des renseignements sur les patients. L'adjointe administrative de la Docteure Sanderson se servait de cette base de données comme plan de travail pour inscrire les rendez-vous des patients et les tests de suivi.

Il s'est avéré qu'Excel n'était pas le logiciel le plus efficace pour tenir une base de données sur les patients, ce qui a mené le personnel de la Docteure Sanderson à procéder à la copie de sauvegarde des données médicales sur une source secondaire. Une clé USB a donc été choisie à cette fin et servait uniquement de source secondaire de secours.

La deuxième raison pour laquelle les renseignements sur la santé des patients ont été sauvegardés sur la clé USB était pour pouvoir récupérer ces renseignements lorsqu'il n'était pas possible d'accéder au système sécurisé de l'Hôpital (c.-à-d. celui du Réseau de santé Horizon).

La Docteure Sanderson, à l'instar d'autres médecins, stockait des données dans son ordinateur de bureau, et ces données étaient sauvegardées régulièrement sur le serveur principal de l'Hôpital. Le personnel de la Docteure Sanderson pouvait continuer à travailler dans Excel pendant ces périodes d'indisponibilité seulement en accédant aux données stockées sur la clé USB.

La clé USB dont il est question dans la présente affaire contenait, croit-on, des données sur quelque 900 patients, entre autres le nom des patients, le nom de leurs parents, leur adresse, leur numéro de téléphone, leur date de naissance, leur numéro d'assurance-maladie, leur diagnostic, les dates de leurs rendez-vous et les tests de suivi auxquels ils ont été soumis. Il n'a pas été possible d'établir avec certitude qui sont les 900 patients touchés parmi tous les patients de la Docteure Sanderson.

Aux dires de l'adjointe administrative de la Docteure Sanderson, une copie de sauvegarde du plan de travail dans Excel comportant des renseignements sur les patients était effectuée tous les mois ou tous les deux mois sur la clé USB. La dernière copie de sauvegarde aurait été faite en août 2010, et la prochaine devait avoir lieu en octobre. L'adjointe administrative a affirmé n'avoir eu l'occasion de voir à la copie de sauvegarde qu'aux environs du congé du jour du Souvenir, en novembre 2010, et c'est à ce moment qu'elle se serait rendu compte que la clé USB était introuvable. Par conséquent, on ne connaît pas le moment exact où la clé USB a disparu.

Enquête menée par la Commissaire

Pourquoi avoir attendu?

Lorsque l'adjointe administrative de la Docteure Sanderson s'est rendu compte que la clé USB était introuvable en novembre 2010, elle en a avisé la Docteure Sanderson, qui, bien qu'elle n'en garde aucun souvenir, ne doute pas qu'elle en ait été avertie à ce moment. Au cours de l'enquête menée sur cette affaire, la Docteure Sanderson a admis ne pas avoir porté attention à cet avis et, par conséquent, n'a pas agi sur cette question en novembre 2010.

Entre-temps, le personnel de la Docteure Sanderson, ainsi que trois autres employés travaillant pour d'autres médecins dans le service de pédiatrie, ont aidé à chercher la clé USB dans la pièce. Cet effort de groupe est demeuré vain. Ce n'est que neuf mois plus tard, en août 2011, que l'adjointe administrative a rappelé à la Docteure Sanderson que la clé USB était introuvable. La Docteure Sanderson en a alors pris bonne note et a agi sur-le-champ.

D'autres efforts ont été consacrés à retrouver la clé USB, mais, à ce jour, elle est toujours manquante.

Qu'est-ce qui explique que cette atteinte se soit produite?

Lorsqu'elle a été avisée, en août 2011, que la clé USB demeurait introuvable, la Docteure Sanderson en a informé l'infirmier gestionnaire de l'Hôpital, qui, à son tour, a communiqué avec la chef de la protection de la vie privée du Réseau de santé Horizon. Le lendemain, les cadres supérieurs de l'Hôpital, la chef de la protection des renseignements personnels du ministère de la Santé et le Commissariat à l'accès à l'information et à la protection de la vie privée ont été avisés informés de l'incident. La chef de la protection des renseignements personnels a rencontré la Docteure Sanderson et l'infirmier gestionnaire afin d'entreprendre son enquête.

La Commissaire a rencontré les cadres supérieurs de l'Hôpital, la Docteure Sanderson et son adjointe administrative ainsi que la chef de la protection de la vie privée du Réseau de santé Horizon afin de recueillir les faits entourant l'incident. Les parties ont discuté de la façon dont l'atteinte à la vie privée s'est produite et des raisons qui l'expliquent. La Commissaire a également visité le bureau et les environs de l'endroit d'où la clé USB était disparue.

Au moment de l'incident, la Docteure Sanderson et son adjointe administrative ne partageaient pas le même bureau. Celui de l'adjointe administrative se situait dans l'un des couloirs secondaires de l'Hôpital, et elle le partageait avec trois adjoints administratifs d'autres médecins. Ce bureau comptait deux portes : la porte principale, qui était ouverte pendant les heures de travail, et une porte secondaire, de l'autre côté de la pièce, qui demeurait fermée. Aucune de ces portes n'était verrouillée le jour, pas même lorsque personne n'était dans le bureau. Les employés disposaient de postes de travail modulaires et, par conséquent, leur bureau était facilement accessible à quiconque entrait dans cette pièce. Cet espace de bureau partagé servait aux patients venus s'enregistrer avant un rendez-vous et au personnel venu récupérer des impressions (désigné comme point central où récupérer tout document imprimé). Qui plus est, cette pièce servait également d'aire commune pour le personnel : celui-ci y avait accès à un réfrigérateur et à du café.

D'après les faits recueillis, les deux portes donnant accès à cette pièce étaient habituellement fermées lorsque le personnel s'en allait à la fin du quart de travail (à 16 h); par contre, elles demeuraient déverrouillées de 16 h jusqu'aux environs de 20 h, et aucun employé ne se trouvait dans la pièce pendant ces heures. Le personnel de sécurité qui effectuait des rondes de

sécurité régulières dans le service où se trouve cette pièce vérifiait que les deux portes étaient verrouillées le soir, la nuit, la fin de semaine et les jours fériés.

La clé USB en question était laissée dans un tiroir non verrouillé du bureau de l'adjointe administrative. Les renseignements stockés sur la clé USB n'étaient ni chiffrés, ni protégés par un mot de passe.

Notification des patients concernés

La Commissaire a aidé la Docteure Sanderson et le Réseau de santé Horizon à s'assurer que tous les patients touchés par l'atteinte à la vie privée en soient avisés le plus rapidement possible. À cet égard, le bureau de la Docteure Sanderson a dressé la liste à jour des patients dont les renseignements personnels sur la santé figuraient dans la base de données. Il y en avait 1 513.

Tous ces patients ont été avisés de la situation au début de septembre 2011. Les lettres d'avis informaient les patients de leur droit de déposer une plainte auprès du Commissariat en vertu de la *Loi sur l'accès et la protection en matière de renseignements personnels sur la santé* (« la *Loi* »). Parmi les centaines de patients avisés, nous savons qu'un certain nombre a communiqué directement avec la Docteure Sanderson et le Réseau de santé Horizon. Vingt-cinq personnes nous ont transmis une plainte, demandé des renseignements ou fait part de leurs préoccupations. De ceux qui ont communiqué avec notre bureau, onze ont déposé une plainte officielle en vertu de la *Loi*. Ces plaintes sont décrites ci-dessous.

Plaintes des personnes concernées

Lorsqu'une personne s'inquiète de ce que l'intégrité des renseignements personnels sur sa santé ait pu être compromise, elle a le droit de déposer une plainte auprès de notre bureau aux termes du paragraphe 68(2) de la *Loi*. La Commissaire dispose de 90 jours pour mener son enquête et déposer un rapport sur ses conclusions.

Nous avons reçu des plaintes de parents dont les renseignements personnels sur la santé de leurs enfants ont été perdus des suites de cet incident. La plupart des plaintes ont été déposées à la fin de septembre et certaines, en novembre 2011. Dans la présente affaire, l'échéancier de 90 jours a été prolongé jusqu'à la date du présent rapport sur les conclusions, prolongement qui a été nécessaire afin de nous permettre d'examiner à fond les circonstances entourant cette atteinte à la vie privée.

Pour l'essentiel, les plaintes ont soulevé les questions suivantes :

a) Pourquoi a-t-il fallu autant de temps pour nous aviser de l'atteinte à la vie privée?
b) Pourquoi les renseignements médicaux stockés sur une clé USB n'étaient-ils ni chiffrés, ni protégés par un mot de passe?
c) Quelles mesures sont prises actuellement pour corriger cette atteinte et pour empêcher que des incidents semblables ne se produisent à l'avenir?
d) La perte de renseignements personnels, dont ceux d'un enfant, peut-elle mener à un vol d'identité et avoir une incidence sur les antécédents financiers de la personne concernée?
e) Faut-il se procurer un nouveau numéro d'assurance-maladie?

Ces questions seront abordées à tour de rôle dans nos conclusions ci-après.

Grave retard de la notification

La réponse à cette première question a été exposée en détail au début du présent Rapport. S'il a fallu autant de temps avant que les patients ne soient avisés de cette atteinte à la vie privée, c'est-à-dire de novembre 2010 à août 2011, ce n'est que parce que la Docteure Sanderson n'a pas porté attention lorsque le personnel l'a avisée qu'une clé USB contenant des renseignements personnels sur la santé de ses patients était introuvable.

Selon l'article 49 de la *Loi*, il faut procéder à une notification au sujet de l'atteinte à la vie privée dans les cas suivants :

> 49(1) Le dépositaire est tenu :
>
> *c*) de notifier, la personne physique visée par les renseignements personnels sur la santé et le commissaire, à la première occasion raisonnable et conformément aux règlements, que ces renseignements ont été :
>
> (i) volés,
>
> (ii) perdus,
>
> (iii) éliminés, sauf dans les cas permis par la présente loi,
>
> (iv) communiqués par une personne non autorisée et que celle-ci y a eût accès.

La *Loi* oblige les dépositaires à protéger les renseignements personnels sur la santé leur étant confiés et, étant donné la nature très délicate de ces renseignements, les personnes concernées ont le droit de le savoir quand l'intégrité de leurs renseignements personnels a été compromise. Par conséquent, les règles sur l'avis obligatoire en cas d'atteinte à la protection de la vie privée dont fait mention l'article 49 doivent obligatoirement être respectées, sauf dans

des circonstances restreintes bien précises (décrites au paragraphe 49(2)). Ces exceptions ne s'appliquent pas dans cette affaire.

Aux termes de l'article 49, il faut émettre un avis aussitôt que possible. Le processus de notification vise à tenir les dépositaires responsables lorsqu'une atteinte se produit et à offrir de l'aide aux personnes dont l'intégrité des renseignements a été compromise, en réduisant les torts qui pourraient leur être causés en raison de cette atteinte.

Dans la présente affaire, la perte de la clé USB dont le contenu n'était ni chiffré, ni protégé par un mot de passe était clairement un cas où le dépositaire était dans l'obligation d'aviser les personnes concernées à la première occasion raisonnable. Cette occasion était en novembre 2010, mais personne n'a été avisé à ce moment. Par conséquent, la Docteure Sanderson a failli à son devoir d'aviser les personnes concernées et la commissaire, comme le stipule l'article 49 de la *Loi.*

Cela dit, lorsque le personnel a rappelé à la Docteure Sanderson, en août 2011, que la clé USB était toujours introuvable, elle en a pris bonne note et s'est empressée d'agir pour en aviser tous ses patients sur-le-champ.

Stockage de renseignements médicaux des patients sur une clé USB

Cette question concerne la règle générale sur la protection des renseignements personnels sur la santé, figurant à l'article 50 de la *Loi* qui s'intitule *Garanties :*

> **50**(1) Conformément aux exigences réglementaires, le dépositaire protège les renseignements personnels sur la santé en adoptant des pratiques relatives aux renseignements personnels sur la santé qui comportent des garanties administratives, techniques et physiques raisonnables afin que soient assurées la confidentialité, la sécurité, l'exactitude et l'intégrité des renseignements.
>
> **50**(2) Les pratiques visées au paragraphe (1) sont fondées sur des normes relatives à la sécurité de la technologie de l'information reconnues à l'échelle nationale ou par une autorité législative, qui sont appropriées au degré de sensibilité des renseignements personnels sur la santé devant être protégés.
> […]
> (*e*) veille à ce que ses mandataires se conforment aux mesures de sécurité.

> **50**(4) Le dépositaire qui maintient des renseignements personnels sur la santé sur support électronique met en œuvre toutes les mesures supplémentaires afin d'assurer la sécurité et la protection de ces renseignements qu'exigent les règlements.

Le *dépositaire* est un fournisseur de soins de santé et peut donc être, par exemple, un médecin, une infirmière ou un hôpital. La Docteure Sanderson et le Réseau de santé Horizon sont tous deux des dépositaires et ont tous deux le devoir de protéger les renseignements personnels sur la santé, comme l'exige l'article 50 de la *Loi*.

Dans cet article, l'accent est mis sur l'importance de protéger les renseignements personnels sur la santé en tout temps, et ce, grâce à des garanties qui doivent veiller à la confidentialité, à l'intégrité, à l'exactitude et, comme dans la présente affaire, à la sécurité de ces renseignements. Plus précisément, l'article 50 explique une façon pragmatique d'instaurer des garanties en fonction de deux normes : le caractère raisonnable et le degré de sensibilité des renseignements.

La première norme exige que les garanties soient raisonnables, ce qui signifie que les renseignements doivent être gardés en sécurité grâce à des garanties qui sont raisonnables d'un point de vue objectif et non d'après des choix personnels. En ce sens, les garanties de sécurité n'ont pas à être parfaites, mais elles doivent être raisonnables compte tenu des circonstances. À titre d'exemple, une dépositaire consulte, sur un bureau, le contenu d'une chemise ouverte dans laquelle se trouvent des dossiers médicaux de patients (en format papier). La dépositaire quitte la pièce sur l'heure du midi, mais ne range pas la chemise étant donné que ses employés restent sur place. Or, pendant l'heure du midi, un technicien entre dans cette pièce pour effectuer des réparations et des travaux d'entretien régulier sur l'imprimante de la dépositaire. Les renseignements personnels des patients sont clairement à la vue. La dépositaire croit que cette chemise est en sécurité dans son bureau, car le public n'y entre pas et que des employés sont présents. Ainsi, du point de vue subjectif de la dépositaire, la chemise était en sécurité. Par contre, d'un point de vue objectif, il est évident que cette chemise n'était pas en sécurité, car le technicien en réparations pouvait la voir et y accéder. Cette mesure n'était donc pas raisonnable. Vu la visite du technicien en réparations, la dépositaire ou ses employés auraient dû ranger la chemise avant qu'il ne puisse entrer dans le bureau. Voilà qui aurait été une mesure raisonnable.

Mentionnons que l'on peut aussi faire appel au gros bon sens lorsqu'il est question de prendre des mesures de sécurité raisonnables. Dans bien des cas, le simple verrouillage des portes et des tiroirs constitue une garantie de sécurité efficace. Malheureusement, c'est souvent le fait

de ne pas porter attention aux pratiques quotidiennes dans nos milieux de travail qui donne lieu aux plus grandes préoccupations en matière de sécurité.

La deuxième norme exige que les garanties soient établies en fonction du degré de sensibilité des renseignements. Plus les renseignements sont sensibles, plus la sécurité doit être grande. Encore une fois, ce sont les circonstances particulières à chaque cas qui détermineront les mesures de sécurité raisonnables nécessaires pour protéger les renseignements personnels sur la santé. À titre d'exemple, une liste sur laquelle ne figure que le nom des personnes qui participent à une enquête sur la santé n'exigera pas le même niveau de sécurité qu'une liste où figurent les diagnostics médicaux visant ces mêmes personnes.

Qui plus est, lorsque des renseignements personnels sur la santé sont stockés sur un support électronique, la *Loi* exige du dépositaire qu'il use d'extrême prudence et qu'il adopte des mesures de sécurité supplémentaires. Ces exigences figurent à l'article 20 du *Règlement du Nouveau-Brunswick 2010-112* de la *Loi*, et cet article contient également d'autres garanties de sécurité physiques, techniques et administratives, soit les suivantes :

> **20**(1) Le dépositaire établit et observe des directives écrites concernant les pratiques relatives à la protection des renseignements personnels sur la santé et contenant les exigences suivantes :
> *a*) des mesures visant à assurer la sécurité des renseignements personnels sur la santé au cours de leur collecte, de leur utilisation, de leur communication, de leur entreposage et de leur destruction;
> *b*) des mesures, telle que l'utilisation de mots de passe ou du chiffrement, visant à assurer la sécurité des supports électroniques amovibles utilisés lors de l'enregistrement, du transport ou du transfert de renseignements personnels sur la santé;
> *c*) des mesures visant à assurer que les supports électroniques amovibles utilisés pour enregistrer les renseignements personnels sur la santé sont entreposés en lieu sûr lorsqu'ils ne sont pas utilisés;
> *d*) des mesures visant à assurer que les renseignements personnels sur la santé sont maintenus dans une aire désignée et font l'objet d'un système de sécurité approprié;
> *e*) des mesures limitant aux personnes autorisées l'accès physique aux aires désignées où se trouvent les renseignements personnels sur la santé;
> *f*) une procédure relative à la consignation des atteintes à la sécurité des renseignements;
> *g*) des mesures correctives visant à remédier aux atteintes à la sécurité des renseignements.

> **20**(2) Le dépositaire tient un registre de toutes les atteintes à la sécurité des renseignements en consignant ces atteintes ainsi que les mesures correctives prises pour réduire le risque qu'elles se reproduisent.

Comme dans le cas des garanties de sécurité raisonnables dont il est question à l'article 50 de la *Loi* ci-dessus, les obligations supplémentaires stipulées dans le *Règlement* sensibilisent les dépositaires aux exigences supplémentaires à respecter relativement aux renseignements personnels sur la santé en format électronique. Les données stockées sur un support électronique doivent impérativement être chiffrées et protégées par un mot de passe, et ces mesures sont devenues la norme dans notre monde professionnel hautement technique et intégré où les ordinateurs portables, les systèmes de réseau sans fil et les autres supports électroniques amovibles comme les clés USB sont la réalité.

Dans la présente affaire, compte tenu du degré de sensibilité et de la quantité de renseignements personnels sur la santé que contenait la clé USB utilisée dans le bureau de la Docteure Sanderson, nous sommes d'avis qu'il était raisonnable d'exiger des garanties de sécurité très élevées. Or, la sécurité des renseignements n'a pas été protégée, comme le prouvent les faits suivants :

- une clé USB a servi à stocker des renseignements de nature très sensible sur les patients;
- les renseignements contenus dans la clé USB n'étaient ni chiffrés, ni protégés par un mot de passe;
- la clé USB était rangée dans un tiroir non verrouillé, dans une pièce également non verrouillée, parfois sans surveillance et souvent accessible au public;
- des dossiers de patients de nature très sensible étaient manipulés et rangés dans une pièce non verrouillée, parfois sans surveillance et souvent accessible au public.

Pour ces raisons, nous estimons que les pratiques de protection des renseignements adoptées et utilisées par le personnel du bureau de la Docteure Sanderson et le Réseau de santé Horizon au moment où l'atteinte à la vie privée s'est produite ne respectaient pas les normes qui incombent aux dépositaires en matière de protection des renseignements personnels sur la santé et n'étaient pas conformes à la *Loi*. À cet égard, la Docteure Sanderson et le Réseau de santé Horizon ont failli à leur devoir de mettre en place les garanties de sécurité requises pour protéger les renseignements personnels sur la santé de leurs patients, comme l'exige la *Loi*.

Mesures correctrices visant à empêcher des atteintes à la vie privée semblables à l'avenir

Stockage de données sur des supports électroniques amovibles

Des suites de cette atteinte, les politiques et pratiques du Réseau de santé Horizon en matière de stockage de données provenant des dossiers de santé ont fait l'objet d'un examen approfondi. Les nouvelles politiques et pratiques sont destinées à empêcher la perte de renseignements personnels sur la santé comme ce fut le cas dans la présente affaire.

Nous avons été avisés que le Réseau de santé Horizon élabore actuellement une politique sur les dispositifs de stockage USB. En octobre 2011, la chef de la protection de la vie privée du Réseau de santé Horizon a entrepris une évaluation dans le but de relever les diverses façons dont les renseignements sur la santé de nature délicate sont stockés dans l'ensemble du Réseau. Cette évaluation, ainsi que le questionnaire qui l'accompagne, vise à examiner les méthodes actuelles de stockage des données de nature délicate afin d'élaborer des pratiques exemplaires et des normes qui garantiront la protection adéquate de ces renseignements.

Lorsqu'il sera nécessaire de recourir à ce type de support, le chiffrage sera obligatoire. De nouvelles mesures seront créées en vue remplacer les pratiques actuelles qui consistent à stocker des dossiers médicaux sur des supports électroniques amovibles comme les clés USB. Ces nouvelles mesures comprendront :

- des restrictions sur l'utilisation de supports amovibles pour stocker des renseignements personnels et confidentiels ainsi que des renseignements personnels sur la santé;
- l'utilisation de mots de passe;
- l'obtention d'une approbation avant de recourir à ces supports;
- le chiffrage des données qu'ils contiennent;
- leur mise sous clé lorsqu'ils ne sont pas utilisés;
- l'interdiction de s'en servir pour faire une copie de secours des données.

Nous avons aussi été informés que les renseignements sur la santé des patients de la Docteure Sanderson provenant de la base de données Excel ne seront plus stockés sur une clé USB et que ces données continueront de n'être sauvegardées que sur le réseau sécurisé du Réseau de santé Horizon. Les autres employés de cette clinique à l'Hôpital ont été informés de cette décision.

Le directeur des techniques informatiques du Réseau de santé Horizon contribue actuellement à l'élaboration des lignes directrices pour la création de bases de données et des garanties

nécessaires pour protéger les renseignements qu'elles contiennent et il se penche actuellement sur la question de l'utilisation des supports amovibles.

De plus, les pratiques de gestion des renseignements ont été revues avec la Docteure Sanderson et ses employés.

La Commissaire sera tenue informée des futurs développements afin de s'assurer que les exigences relatives aux garanties de sécurité énoncées dans la *Loi* y sont bel et bien intégrées.

Nouveaux bureaux

En février 2011, soit avant la notification de la présente affaire d'atteinte à la vie privée, l'adjointe administrative de la Docteure Sanderson a emménagé dans un nouveau bureau, qui se situe juste à côté de celui de la Docteure Sanderson et est loin de l'ancienne aire de travail passante qui était accessible autant aux patients qu'aux autres employés. L'adjointe administrative dispose donc maintenant de son propre espace de travail et d'un espace pour ranger les dossiers des patients. Des dispositions devaient être prises pour lui fournir un tiroir ou une armoire qui se ferme à clé où elle pourra ranger les dossiers des patients dont elle se sert quotidiennement.

Ce nouveau bureau devrait être un endroit où les renseignements personnels sur la santé sont en sûreté. En effet, le bureau n'est pourvu que d'une seule porte, qui est verrouillée chaque fois que l'adjointe administrative quitte son poste de travail.

Perte de renseignements personnels et vol d'identité

Dans la présente affaire, l'une des principales inquiétudes qui ont été portées à notre attention concernait le risque de vol d'identité. La perte des renseignements personnels sur la santé des patients de la Docteure Sanderson pourrait mener à un vol d'identité. Parmi les renseignements perdus dans la présente affaire, il y avait le nom des patients, leur date de naissance, leur numéro d'assurance-maladie, leur adresse, etc. Il est impossible d'établir avec un quelconque degré de certitude le risque encouru par une personne lorsque l'intégrité de ses renseignements personnels a été compromise, mais on ne peut présumer que ce risque est nul et, par conséquent, cette perte de renseignements ne doit pas être prise à la légère. Pour chaque renseignement d'identification supplémentaire dont l'intégrité est compromise, le risque de fraude et de vol d'identité augmente.

Les voleurs d'identité ont de nombreuses façons de mettre la main sur des renseignements personnels, et l'exploitation de données tirées de bases de données perdues ou volées

appartenant à des organismes privés ou publics en est une. Il n'y a pas de définition universelle de ce qui constitue un « vol d'identité », mais cette expression sert à désigner de nombreux concepts, de la falsification d'un chèque à l'utilisation d'une carte de crédit volée, et même les fraudes sophistiquées dans lesquelles un imposteur adopte l'identité de quelqu'un d'autre pour avoir accès à ses biens.

Afin de diminuer grandement les risques que les renseignements personnels de tout un chacun se trouvent en de mauvaises mains, il suffit d'intégrer des mesures simples à son horaire mensuel, par exemple :

- surveiller le moment où son relevé de carte de crédit est censé arriver et téléphoner à la société émettrice de la carte de crédit s'il accuse un retard;
- passer en revue tous ses relevés bancaires et de carte de crédit afin de vérifier qu'ils ne contiennent aucun achat non autorisé;
- vérifier son rapport de solvabilité chaque année – les grands bureaux de crédit en fournissent un gratuitement chaque année;
- se créer un nouveau mot de passe pour chaque compte en ligne sur son ordinateur et le changer fréquemment – un bon mot de passe est difficile pour quiconque à deviner;
- rester vigilant et sur ses gardes lorsque l'on reçoit des courriels de banques, d'agences gouvernementales ou de sociétés émettrices de cartes de crédit qui demandent de fournir des renseignements personnels en ligne – les vraies banques et les vraies agences ne le font jamais et, pourtant, des fraudeurs copient souvent de vrais logos pour donner à leurs messages frauduleux un aspect plus authentique;
- consulter le site Web du Commissariat à la protection de la vie privée du Canada (www.priv.gc.ca), qui offre d'autres renseignements et trucs utiles sur la façon de signaler et de corriger les torts découlant d'un vol d'identité ou de fraudes connexes.

Les coordonnées d'organismes offrant des services de surveillance du crédit ont été remises aux personnes touchées par la présente affaire d'atteinte à la vie privée. Ces organismes de surveillance ont souligné que les enfants dont les renseignements personnels ont été perdus dans cette atteinte sont très jeunes et ne possèdent donc pas encore d'antécédents financiers ou de crédit qui exigeraient ce genre de surveillance.

Nouvelle carte et nouveau numéro d'assurance-maladie

Dans la présente affaire d'atteinte à la vie privée où des renseignements personnels comme le numéro d'assurance-maladie des patients ont été perdus, il n'est pas nécessaire de se procurer un nouveau numéro d'assurance-maladie. Selon les faits recueillis, bien que la clé USB en question soit introuvable depuis novembre 2010 (ou avant), le Réseau de santé Horizon n'a

reçu aucun signalement d'une mauvaise utilisation des renseignements personnels sur la santé qu'elle contenait.

Actuellement, les fonctionnaires de l'Assurance-maladie sont d'avis que cette situation ne constitue qu'un risque minimal de vol d'identité. À cet égard, l'Assurance-maladie a donc suivi sa règle générale, soit celle de ne pas renouveler automatiquement le numéro d'assurance-maladie des personnes touchées par la présente affaire. Néanmoins, lorsque les personnes touchées ont été avisées de l'atteinte, les coordonnées des services de l'Assurance-maladie leur ont été communiquées et on leur a permis de demander une nouvelle carte d'assurance-maladie.

Commentaires finaux de la Commissaire

Nous avons travaillé avec la Docteure Sanderson, ses employés ainsi que son employeur, le Réseau de santé Horizon, en lien avec cette atteinte à la vie privée. Nous sommes confiants d'avoir mis au jour tous les faits entourant cet incident et comprenons les conséquences de cette affaire sur toutes les parties concernées, y compris la Docteure Sanderson et ses employés.

La Docteure Sanderson aurait dû porter une attention immédiate à la situation lorsqu'elle a été avisée une première fois que la clé USB avait disparu. Il faut toutefois reconnaître qu'elle s'est rendu compte de toutes les ramifications de ses actions, et nous croyons que les conséquences ont eu une très grande incidence sur sa pratique actuelle et future. La question du temps qu'il a fallu pour aviser les personnes touchées et notre bureau de cette atteinte a été réglée, et les règles sur la notification des atteintes à la vie privée ont été revues avec la Docteure Sanderson.

Comme indiqué précédemment dans le présent rapport sur les conclusions, de nouvelles mesures ont déjà été mises en place afin de mettre fin aux anciennes méthodes non sécuritaires de stockage des renseignements personnels de nature sensible, comme le stockage de dossiers médicaux des patients sur des supports électroniques amovibles, sauf en cas d'absolue nécessité. Dans ces cas exceptionnels, les données contenues sur une clé USB doivent être chiffrées, et celle-ci doit être mise sous clé.

De plus, les politiques et pratiques du Réseau de santé Horizon en matière de stockage de données issues des dossiers de santé en format électronique ont fait l'objet d'un examen approfondi continuel depuis l'incident.

Nous sommes convaincus que les mesures correctrices proposées, une fois étudiées en détail et approuvées, seront mises en œuvre. Notre bureau assurera le suivi de ces mesures.

Il est important de mentionner que, dans cette affaire, l'intégrité des professionnels de la santé chargés de soigner des patients et de protéger leurs renseignements personnels n'a été aucunement remise en question. Nous reconnaissons que ceux qui œuvrent dans le domaine des soins de santé prennent très au sérieux leur devoir de protéger les renseignements personnels sur la santé; cependant, cet incident a montré que des atteintes pouvaient survenir facilement lorsque ceux qui devraient protéger les renseignements personnels s'en remettent à la facilité de la routine pour accomplir leur travail.

Des habitudes ordinaires en viennent à prendre une si grande place dans notre vie professionnelle que nous ne nous rendons pas compte qu'elles nous empêchent de remplir notre devoir de protéger les renseignements. C'est là que réside le problème. Il est important de garder à l'esprit notre devoir de protéger en tout temps les renseignements personnels sur la santé. Nous ne respectons pas ce devoir lorsque nous adoptons des méthodes pratiques mais moins sécuritaires de gestion des renseignements de nature sensible appartenant à des tiers. Une baisse de la vigilance, de la prudence et de la conscience mène invariablement à un relâchement des garanties de sécurité, ce qui donne lieu à une protection moindre qui, quoique non intentionnelle, est néanmoins tangible. C'est à ce moment que les atteintes à la vie privée deviennent possibles et, malheureusement, se produisent.

Toutes les personnes touchées par l'atteinte à la vie privée dont il est question ici ont ressenti une grande déception. C'est peut-être en raison de la cause fondamentale évidente de l'incident en soi : un petit appareil portatif, une clé USB, contenant autant de renseignements précieux n'a clairement pas été mis en sûreté. Les expériences difficiles vécues par tous ceux qui sont concernés et touchés par cette atteinte à la vie privée laisseront une forte impression sur eux. Des leçons ont été retenues de cet incident, notamment une conscience accrue de la facilité avec laquelle des données peuvent être perdues et des vies peuvent être touchées et un respect ravivé quant à la nécessité de faire preuve de vigilance constante en matière de protection des renseignements personnels sur la santé. Ces leçons aideront à rebâtir des liens de confiance avec les personnes dont la vie a été touchée. La mise en œuvre de mesures correctrices garantira que ce type d'incident ne se répétera pas.

À cet égard, nous croyons fermement que la Docteure Sanderson et ses employés ont appris une leçon importante des suites de cette atteinte à la vie privée, une expérience qui n'était pas intentionnelle, nous le savons, mais qui s'est néanmoins produite sous leur surveillance. Nous espérons que le présent rapport des conclusions et que les recommandations qui

l'accompagnent répondront en grande partie aux questions des personnes touchées par cette atteinte à la vie privée ainsi qu'à celles du grand public qui continuera, jour après jour, de confier des renseignements privés aux professionnels de la santé.

RECOMMANDATIONS

Compte tenu des conclusions exposées ci-dessus, la Commissaire émet les recommandations suivantes :

1. que la Docteure Sanderson revoie les obligations des dépositaires aux termes de la *Loi* et s'assure que ses pratiques actuelles en matière de protection des renseignements respectent ces obligations;

2. que la Docteure Sanderson revoie les politiques du Réseau de santé Horizon au sujet de l'utilisation et du stockage sécuritaires des renseignements personnels sur la santé;

3. que la Docteure Sanderson revoie avec ses employés les pratiques en matière de protection des renseignements qu'ils appliquent de même que la politique du Réseau de santé Horizon sur l'utilisation et le stockage sécuritaires des renseignements personnels sur la santé;

4. que la Docteure Sanderson revoie les exigences de la *Loi* au sujet de la notification des atteintes ainsi que la politique du Réseau de santé Horizon quant aux étapes à suivre pour signaler une atteinte à la vie privée;

5. que le Réseau de santé Horizon poursuive ses efforts pour parachever sa politique sur les pratiques de sécurité en matière d''utilisation et de rangement de clés USB contenant des renseignements personnels sur la santé et pour procéder à sa mise en œuvre, et que le Réseau de santé Horizon en informe la Commissaire lorsque ce sera fait;

6. que le Réseau de santé Horizon émette un avis à l'intention de tous ses médecins salariés et de leurs employés leur rappelant leur obligation de protéger les renseignements personnels sur la santé en tout temps, conformément à la *Loi;*

7. que le Réseau de santé Horizon émette un avis à l'intention de tous ses médecins salariés et de leurs employés leur rappelant leur obligation de suivre la politique du Réseau de santé Horizon sur le signalement des atteintes à la vie privée conformément à la *Loi*.

Publié à Fredericton (Nouveau-Brunswick), ce 9 février 2012.

_____

Anne E. Bertrand, c.r.
Commissaire