Office of the Access to Information and Privacy Commissioner
New Brunswick

Commissariat à l'accès à l'information et à la protection de la vie privée
Nouveau-Brunswick

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 : 2014-2214-H-640
Date : Le 26 août 2016

Dossier concernant le vol, dans un hôpital, d'un ordinateur portatif sur lequel étaient stockés des renseignements personnels sur la santé non chiffrés

INTRODUCTION et CONTEXTE

1. Le présent rapport des conclusions de l'enquête de la commissaire est présenté en vertu du paragraphe 73(1) de la *Loi sur l'accès et la protection en matière de renseignements personnels sur la santé* (« la *Loi* ») et fait suite à un incident de violation de la vie privée signalé au Commissariat le 17 décembre 2014. La violation est survenue lorsqu'un ordinateur portatif contenant des renseignements personnels sur la santé a été volé à l'Hôpital de Moncton; bien qu'il ait été protégé par mot de passe, ses données n'étaient pas chiffrées.

2. Trois dépositaires assujettis à la *Loi* se trouvent concernés par l'affaire – le Réseau de santé Horizon, le Réseau de santé Vitalité et FacilicorpNB – puisque la violation est survenue à un hôpital relevant d'Horizon, l'ordinateur portatif appartenait à un employé de FacilicorpNB et les personnes visées par les renseignements qui se trouvaient sur l'ordinateur étaient des patients du Réseau Vitalité.

3. En juin ou juillet 2013, les hôpitaux de Bathurst et de Campbellton (Réseau Vitalité) ont conclu avec l'Hôpital de Moncton (Réseau Horizon) une entente en vertu de laquelle les examens radiologiques effectués à Bathurst et à Campbellton seraient envoyés à l'Hôpital de Moncton pour y être étudiés par des radiologistes. Ces derniers prépareraient ensuite des rapports à renvoyer à Bathurst ou à Campbellton. Le processus en question a été adopté en raison du nombre insuffisant de radiologistes qui auraient eu le temps de lire les examens et de préparer des rapports dans ces régions.

4. Un employé de FacilicorpNB travaillant en ingénierie clinique a été sollicité pour apporter une aide technique. FacilicorpNB est l'organisme gouvernemental qui épaule les régies régionales de la santé – ainsi que d'autres entités – avec leurs besoins en matière de technologie de l'information.

5. L'employé a configuré une imprimante de sorte que les rapports dictés par les radiologistes de Moncton puissent être imprimés en format PDF directement à Bathurst ou à Campbellton suivant les besoins. Aux fins de contrôle de la qualité, il a aussi fait en sorte que des copies des rapports lui soient acheminées par courriel, afin qu'il puisse vérifier que le nombre d'examens envoyés correspondait bien au nombre de rapports renvoyés à ces hôpitaux.

6. L'employé conservait les rapports pendant quelques jours dans l'éventualité où ils devraient être renvoyés aux hôpitaux, puis les supprimait. Il les gardait dans des dossiers créés sur son ordinateur portatif (un pour Bathurst et un autre pour Campbellton). Une copie de sauvegarde électronique des rapports était créée sur un dispositif mobile distinct (clé USB).

ENQUÊTE SUR LA VIOLATION DE LA VIE PRIVÉE

Faits établis quant aux causes de la violation

7. Il est peu courant que des rapports contenant les renseignements sensibles de patients soient enregistrés sur un ordinateur portatif, mais dans le cas qui nous intéresse, cette pratique a été adoptée en raison de la pénurie de radiologistes que l'on connaissait alors.

8. Lorsque l'ordinateur portatif a été volé, l'employé avait déjà supprimé 58 rapports dans le dossier de Bathurst, mais n'a pu dire avec certitude si les 78 rapports contenus dans le dossier de Campbellton avaient aussi été supprimés. Les responsables ont présumé que les copies des rapports envoyés à Campbellton se trouvaient toujours sur l'ordinateur au moment du vol, ce qui constituait une violation de la vie privée des patients dont les renseignements figuraient dans les 78 rapports. Fort heureusement, de ces 78 rapports, 6 seulement contenaient les noms de patients, mais tous les rapports contenaient des renseignements personnels sur la santé tels que :

- la date et l'heure de la visite et le numéro d'unité de l'hôpital;
- les antécédents cliniques des patients;
- les résultats et impressions du radiologiste.

9. L'employé de FacilicorpNB travaillait dans un bureau situé au service d'imagerie médicale de l'Hôpital de Moncton. De petites dimensions, ce bureau est situé à côté des salles de rayons X. Bien qu'il y ait une caméra vidéo dans le couloir menant au bureau, cette dernière ne transmet que des images en temps réel et ne permet pas l'enregistrement. Il s'est ainsi avéré impossible de visionner les images pour déterminer comment et par qui l'ordinateur portatif avait été pris. L'examen des vidéos de surveillance d'autres caméras n'a pas révélé d'ordinateur portatif en la possession de qui que ce soit.

10. Notre enquête a permis de déterminer que vers 9 h 40, l'employé, sur le point de quitter le bureau pour prendre une pause, a fermé sa session sur l'ordinateur portatif comme il le faisait habituellement lorsqu'il laissait l'appareil sans surveillance. Le bureau avait une porte munie d'une serrure que l'employé aurait donc pu fermer et verrouiller; la cause efficiente du vol ayant mené à la violation de la vie privée est cependant que l'employé a volontairement laissé la porte du bureau ouverte. Il était en fait habituel pour lui de ne pas fermer systématiquement sa porte durant sa journée de travail, parce que ses tâches exigeaient qu'il entre et sorte fréquemment de son bureau.

11. En revenant au bureau vers 10 h, après une pause de 20 minutes, l'employé a immédiatement remarqué que l'ordinateur portatif ainsi qu'un casque d'écoute et un cordon d'alimentation avaient disparu.

12. Étant donné que l'employé avait l'habitude de ne pas fermer à clé la porte de son bureau, nous concluons que ce n'était qu'une question de temps avant que l'ordinateur portatif soit volé. L'appareil n'était pas attaché au moyen de câbles de verrouillage et était laissé bien en vue, à un endroit auquel le public pouvait clairement accéder. Pire encore: les données sur l'ordinateur portatif n'étaient pas chiffrées pour en assurer la protection.

13. Un autre des facteurs ayant contribué à la violation est que les trois dépositaires concernés avaient permis à l'employé à continuer de garder ouvertes des portes qui pouvaient être verrouillées lorsqu'il sortait de la pièce ou du bureau, sachant pourtant très bien qu'un appareil portatif contenant les renseignements de patients s'y trouvait, et lui avaient permis de garder les renseignements de patients sur un ordinateur portatif sans qu'ils soient chiffrés.

Obligation statutaire de protéger les renseignements des patients en tout temps

14. La *Loi* établit des règles claires sans ambiguïté pour les dépositaires en ce qui concerne la collecte, l'utilisation, la communication, la conservation et la destruction sécuritaire des renseignements personnels sur la santé, règles destinées à assurer la confidentialité des renseignements et à protéger la vie privée des personnes physiques auxquelles ils se rapportent.

15. La *Loi* impose par ailleurs des garanties claires, de nature administrative, technique et physique, qui visent à assurer en tout temps la confidentialité et la protection des renseignements des patients.

16. D'autres vols d'ordinateurs portatifs dans des hôpitaux du Nouveau-Brunswick – sept, au total – nous avaient déjà été signalés auparavant. Nous y reviendrons plus loin dans le présent rapport.

17. Bien que le vol constitue une préoccupation, l'enjeu principal, ici, en ce qui concerne la protection des renseignements des patients doit demeurer les fonctionnalités de sécurité (telles que les mots de passe et le chiffrement) desquelles doivent être doté chaque ordinateur portatif pour éviter que des voleurs ou d'autres personnes qui ne devraient jamais voir ces renseignements privés puissent accéder aux données.

18. Horizon, Vitalité et FacilicorpNB sont tous des dépositaires à part entière au sens de la *Loi* et, puisqu'ils sont également responsables de protéger les renseignements personnels sur la santé par ces garanties, le fait qu'elles n'aient pas été en place dans la présente affaire les rend conjointement responsables de ce qui, à nos yeux, était sans aucun doute une violation de la vie privée évitable.

Obligations des dépositaires d'intervenir lorsque survient une violation de la vie privée

19. Lorsque survient une violation de la vie privée, les personnes responsables doivent en déterminer la cause, maîtriser l'incident pour en limiter les conséquences, aviser à la fois, à la première occasion raisonnable, la Commissaire et les personnes physiques dont les renseignements ont été compromis et mettre en œuvre des mesures correctives pour éviter des incidents similaires.

20. Lorsqu'ils avisent les personnes physiques touchées par une violation de la vie privée, ces responsables doivent, en vertu du *Règlement 2010-112 :*

- nommer le dépositaire responsable;
- fournir le nom et les coordonnées de la personne désignée par le dépositaire pour répondre aux demandes de renseignements concernant les pratiques relatives aux renseignements qu'a adoptées le dépositaire;
- décrire la nature de la violation de la vie privée;
- donner la date et le lieu de la violation de la vie privée;

- indiquer la date à la laquelle le dépositaire a pris connaissance de la violation de la vie privée.

Notification des personnes concernées par la violation et de la Commissaire

21. Six des rapports qui se trouvaient sur l'ordinateur portatif volé contenaient le nom de patients, et deux identifiaient un même patient. Cinq personnes auraient donc pu être identifiées à partir des rapports radiologiques lorsque le voleur y accéderait. Ces cinq personnes, des patients du réseau Vitalité, ont été informées de l'incident par le Réseau.

22. Quant aux 73 autres personnes dont les renseignements avaient aussi été rendus accessibles à l'auteur du vol de l'ordinateur portatif, Horizon, Vitalité et FacilicorpNB sont parvenus à déterminer que ces patients ne pourraient, étant donné la nature de l'information contenue dans les rapports, être identifiés sans leur nom. Ils ont donc décidé de ne pas les aviser.

23. Nous avons examiné les renseignements des patients en question et concluons que, bien que l'identification soit dans les faits envisageable grâce aux dates et heures des visites à l'hôpital, au numéro d'unité et aux antécédents des patients, il faudrait beaucoup d'efforts pour obtenir ces données et déchiffrer les renseignements hospitaliers correspondants. En l'absence de preuves donnant à penser que le voleur aurait pu être un employé de l'hôpital, nous convenons qu'il n'était pas nécessaire, en vertu de l'article 49 de la *Loi*, d'aviser les 73 personnes physiques restantes.

24. La violation de la vie privée touchait trois dépositaires distincts et, bien qu'ils aient joué différents rôles, tous trois étaient tenus de se conformer aux exigences de la *Loi*, y compris à l'obligation d'aviser le Commissariat.

25. La notification en vertu de la *Loi* vise à procurer un résultat important : faire en sorte que le dépositaire à l'origine de la violation endosse la responsabilité de celle-ci et réponde des actions ayant ou n'ayant pas été posées.

26. Cette responsabilisation mènera par ailleurs le dépositaire à adopter des mesures correctives pour s'assurer que les conditions ayant donné lieu à la violation sont ajustées, améliorées ou éliminées, de sorte qu'elle ne se reproduise pas. Autrement, les patients se demanderaient :

À quoi bon?

27. La mise en œuvre de mesures correctives sera obligatoire pour tous les dépositaires touchés par une violation de la vie privée, et les autres mesures à prendre advenant une telle violation, comme la maîtrise de l'incident et la notification des personnes physiques concernées dépendront de la mesure dans laquelle le dépositaire y a contribué.

28. Dans la présente affaire, les personnes physiques concernées étaient des patients de Vitalité; il était donc logique que Vitalité se charge de les aviser.

29. Nous comprenons que les trois dépositaires touchés ont eu des discussions quant à la meilleure approche à adopter face à la situation, et qu'il a été convenu qu'un seul formulaire de notification de violation de la vie privée serait envoyé à la Commissaire. Nous avons été avisés de la violation par Horizon et par Vitalité.

30. Bien que l'adoption d'une approche d'équipe pour gérer la violation ait été, dans la présente affaire, appropriée, tous les dépositaires responsables doivent respecter leurs obligations et, dans cette perspective, FacilicorpNB aurait aussi dû prendre part à la notification de la Commissaire effectuée par Horizon et Vitalité en vertu de l'article 49.

31. Rappelons que la notification en vertu de la *Loi* est obligatoire et a pour objectif de rendre le dépositaire à l'origine de la violation *responsable* des actions posées ou au contraire, des actions qui n'ont pas été posées, et de *faire en sorte qu'il en réponde*. Nous recommanderons que les prochaines fois, FacilicorpNB respecte ses obligations en vertu de l'article 49 et avise la Commissaire.

Maîtrise des conséquences de la violation de la vie privée

32. Après avoir découvert la violation de la vie privée, l'employé a immédiatement informé la sécurité de l'hôpital, et un rapport de vol a été rempli par le gestionnaire des services de sécurité et présenté à la police. Cette dernière a demandé le numéro de série de l'ordinateur portatif et ouvert une enquête sur l'affaire. FacilicorpNB n'a pas fourni cette information à la police, mais nous ignorons toujours pourquoi exactement cela ne lui a pas été possible.

33. Heureusement, la clé USB qui contenait la copie de sauvegarde des données n'a pas été volée. Les données n'ont donc pas été perdues. L'ordinateur n'a jamais été récupéré.

34. Les responsables d'Horizon, de Vitalité et de FacilicorpNB ont aussi été mis au courant de l'incident. Ils ont organisé une réunion pour déterminer les premières mesures à adopter et examiner les images captées par les caméras qui, nous le savons maintenant, n'ont rien révélé.

35. L'employé au cœur de l'affaire a indiqué aux responsables que l'ordinateur portatif pourrait être branché à un ordinateur de bureau pour accéder aux dossiers (contenant les rapports de Campbellton et de Bathurst) sur un disque SharePoint. Pour avoir accès aux rapports, cependant, il faudrait que le voleur trouve le mot de passe et le nom d'utilisateur, et le lien ne fonctionnerait que s'il se trouvait dans les locaux de l'hôpital. Ne connaissant pas l'identité du voleur, l'employé a communiqué avec les deux établissements et demandé que les fichiers soient déplacés ou supprimés, de sorte qu'il ne soit plus possible d'y accéder par l'intermédiaire du lien sur l'ordinateur volé, ce qui a été fait.

Mesures correctives adoptées par suite de cet incident

36. Horizon, Vitalité et FacilicorpNB ont convenu de mettre en place les mesures suivantes :

- le nouvel ordinateur portatif de l'employé a été protégé par mot de passe et ses données, chiffrées;
- la clé USB utilisée par l'employé pour stocker une copie de sauvegarde électronique des données sera aussi protégée par mot de passe et son contenu, chiffré;
- l'employé s'est vu conseiller, à l'avenir, de fermer la porte du bureau chaque fois qu'il en sort, le gardant fermé à clé en tout temps lorsqu'il ne s'y trouve pas;
- un nouveau comité composé de membres du personnel d'Horizon, de Vitalité et de FacilicorpNB a été constitué en octobre 2015 pour établir des politiques et une gouvernance relativement aux appareils contenant des renseignements personnels sur la santé (statuer sur un certain nombre de facteurs parmi lesquels le chiffrement, les mots de passe, la sécurité physique des appareils, la déclaration des incidents, etc.);

- une nouvelle politique exigera que tous les appareils portatifs soient protégés par mots de passe et par chiffrement et, lorsque ce n'est pas possible, que FacilicorpNB et les régies de la santé communiquent entre elles pour cerner d'autres garanties destinées à assurer la protection des renseignements personnels sur la santé;

    - un formulaire de dérogation spécial devra être signé par le vice-président de la régie de la santé pour qu'une exception à la politique puisse être accordée;

    - la politique fera également en sorte que, si la régie de la santé se procure tout appareil sans passer par ses services des technologies de l'information et sans que le personnel ne soit mis au courant, il lui incombe de s'assurer que l'appareil est sécurisé.

        - *Ces deux facteurs n'étaient pas en place avant que l'incident survienne.*

37. L'employé à l'origine de la violation dont il est question aux présentes avait reçu, en 2010, une formation sur la protection de la vie privée dispensée par l'agent de la Protection de la vie privée de FacilicorpNB. Il avait aussi suivi, avant 2010, d'autres formations liées à la vie privée offertes par les hôpitaux, et signe chaque année une déclaration d'entente concernant la confidentialité, comme le prévoit la politique de confidentialité conjointe de FacilicorpNB et des régies régionales de la santé.

38. Bien que la formation soit censée être donnée annuellement, tout ce qu'on nous a signalé est que l'employé en question avait signé la déclaration chaque année et que sa dernière formation remontait à 2010. Dans le cas présent, l'employé n'a pas été réprimandé.

39. À notre avis, il y a eu dans cette affaire un manque de bon sens : ne pas fermer une porte en sachant très bien qu'un ordinateur portatif non sécurisé contenant des renseignements de patients non chiffrés demeurait bien en vue et accessible.

40. Jamais, par ailleurs, on n'aurait dû tolérer que des rapports sur les patients puissent être traités au moyen d'un ordinateur portatif sur lequel les données n'étaient pas chiffrées. Un portatif contenant les renseignements de patients devrait toujours être sécurisé.

41. Bien que nous soyons toujours d'avis que cette affaire aurait clairement pu être évitée, les mesures correctives que nous venons d'énumérer devraient éviter qu'une telle situation se reproduise, afin de restaurer la confiance de la part des patients à qui Horizon, Vitalité et FacilicorpNB sont imputables, en tant que dépositaires, en vertu de la *Loi*.

Mesures correctives d'un cas précédemment signalé d'ordinateur portatif volé dans un hôpital

42. En 2015, un ordinateur portatif contenant les données de 158 patients a été volé à l'Hôpital régional D^r^ Everett Chalmers à Fredericton, plus précisément au service d'inhalothérapie. Nous avions conclu que dans cette affaire, le réseau Horizon et l'Hôpital avaient failli à leur responsabilité de protéger les renseignements personnels de leurs patients en laissant ouverte la porte d'une pièce où l'ordinateur portatif n'était pas attaché par des câbles à un chariot mobile, et contenait des données sur les patients particulièrement sensibles qui n'étaient ni protégées par mot de passe ni chiffrées (rapport des conclusions 2015-2513-H-710).

43. Au cours de notre enquête de cette affaire, Horizon a resserré son examen des mesures de sécurité pour s'assurer que celles qui devaient être mises en place relativement aux appareils électroniques contenant des renseignements personnels sur la santé l'étaient bel et bien. Ces mesures comprenaient la possibilité de supprimer les données de patients d'appareils mobiles. Horizon a également installé la protection par mot de passe sur tous les ordinateurs et les appareils utilisés par ce service de l'Hôpital régional D^r^ Everett Chalmers, fixé, au moyen d'un dispositif de verrouillage, les ordinateurs portatifs à leur chariot mobile respectif et exigé que la porte d'entrée demeure fermée à clé 24 heures sur 24, 7 jours sur 7.

44. Horizon était aussi en train d'élaborer une politique en vertu de laquelle tous les appareils portatifs devraient avoir des mots de passe et toutes leurs données devraient être chiffrées, quel que soit leur état; dans certains cas, advenant que certains appareils ne puissent être protégés par mot de passe ou que leurs données ne puissent être chiffrées, FacilicorpNB et les régies régionales de la santé devraient trouver d'autres garanties qui permettent d'assurer la confidentialité des renseignements personnels sur la santé pour ces appareils.

45. À l'époque, soit au moment où la violation de la vie privée est survenue, en 2015, seul le contenu de quelque 300 appareils était chiffré; le chiffrement a ensuite été déployé progressivement pour en venir à inclure, tandis que nous concluions l'enquête, environ 2400 ordinateurs portatifs utilisés par le personnel de l'hôpital ainsi que l'équipement utilisé par les employés d'Horizon et de FacilicorpNB.

46. Le présent rapport des conclusions contient donc des recommandations à l'endroit d'Horizon, de FacilicorpNB et de Vitalité pour le maintien de ces mesures correctives.

RECOMMANDATIONS

47. Se fondant sur tout ce qui précède, la Commissaire recommande, conformément à l'alinéa 63 *f*) de la *Loi*, que les trois dépositaires, FacilicorpNB, le Réseau de santé Vitalité et le Réseau de santé Horizon mettent en œuvre, conjointement et sans délai :

(a) des lignes directrices écrites d'application obligatoire en vertu desquelles, avant d'être remis aux membres du personnel, tous les appareils électroniques portatifs destinés au stockage de renseignements personnels sur la santé doivent être protégés par mots de passe et toutes leurs données, chiffrées, sans exception;

(b) des lignes directrices écrites d'application obligatoire voulant que tous les appareils électroniques portatifs remis aux fins de stockage de renseignements personnels sur la santé soient gardés sous clé dans un bureau ou un espace de rangement lui-même fermé à clé lorsqu'ils ne sont pas utilisés ou sont laissés sans surveillance pour quelque durée que ce soit, sans exception;

(c) que les données de tous les appareils électroniques portatifs remis aux fins de stockage de renseignements personnels puissent, à distance, être rendues illisibles, dans la mesure où les coûts associés à cette capacité le permettent.

48. De plus, la Commissaire recommande en vertu de l'alinéa 63 *f*) de la *Loi* que les trois dépositaires, FacilicorpNB, le Réseau de santé Vitalité et le Réseau de santé Horizon informent tous les membres de leur personnel de ces lignes directrices obligatoires par un avis stipulant qu'en cas de non-application, même par manque de diligence, des mesures disciplinaires seront adoptées.

49. Enfin, la Commissaire recommande que FacilicorpNB, le Réseau de santé Vitalité et le Réseau de santé Horizon adoptent ou améliorent les mesures correctives adoptées et mises en œuvre dans l'affaire de l'ordinateur portatif volé à l'Hôpital régional D^{r} Everett Chalmers, précédemment mentionnée (2015-2513-H-710), et qu'ils présentent à la Commissaire un rapport conjoint de leurs progrès dans l'application de toutes ces recommandations d'ici le 28 octobre 2016 au plus tard.

Fait à Fredericton (Nouveau-Brunswick), ce 26 août 2016.

_____
Anne E. Bertrand, c.r.
Commissaire à l'accès à l'information et à la protection de la vie privée