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 de notification d'une atteinte à la protection de la vie privée : 2015-2513-H-710
Affaires : 2015-2587-H-729; 2015-2588-H-730; 2015-2589-H-731
Date : Le 28 janvier 2016

« Affaire concernant le vol d'un ordinateur portatif contenant des renseignements personnels sur la santé »

INTRODUCTION

1. Le présent rapport des conclusions de l'enquête de la Commissaire est établi en vertu de la *Loi sur l'accès et la protection en matière de renseignements personnels sur la santé*, L.N.-B., ch. P-7.05 (ci-après désignée comme « la *Loi* ») et fait suite à une enquête menée après que la Commissaire a été avisée d'une atteinte à la protection de la vie privée aux termes de l'article 49 de la *Loi.*

2. La Commissaire a amorcé son enquête après avoir été avisée le 16 juin 2015 par le Réseau de santé Horizon (« Horizon ») que cette atteinte à la vie privée avait eu lieu lorsqu'on a découvert que l'hôpital s'est fait voler un ordinateur portatif contenant les renseignements personnels sur la santé de 158 patients.

3. Au moment où nous avons été avisés de cette situation, Horizon n'avait pas encore informé les personnes dont les renseignements de patients étaient sauvegardés dans l'ordinateur portatif manquant. Nous en reparlerons plus loin dans le présent rapport.

4. Le présent rapport des conclusions portera sur les éléments suivants : le contexte de cette affaire et les faits mis au jour dans le cadre de l'enquête, les mesures prises pour limiter l'atteinte, le processus de notification, les mécanismes de sécurité exigés, les mesures correctives appliquées pour remédier à l'atteinte et nos conclusions. Ce rapport se termine par nos conclusions et recommandations en application de la *Loi*.

5. Nous traitons maintenant les éléments de ce rapport des conclusions.

ENQUÊTE

FAITS MIS EN ÉVIDENCE ET CONCERNANT L'INCIDENT

6. L'Hôpital Dr Everett Chalmers (« l'hôpital ») est doté d'un service d'inhalothérapie.

7. Le service d'inhalothérapie a pour fonction d'exécuter différents tests pour mesurer la capacité pulmonaire des patients. Un de ces tests est connu sous le nom de spirométrie.

8. L'entrée principale au service d'inhalothérapie n'est accessible qu'au personnel autorisé (qui compte de 19 à 21 membres). Pour entrer, ces membres du personnel doivent glisser leur carte d'accès.

9. Bien que l'entrée principale du service ne soit accessible qu'aux personnes autorisées et que sa porte demeure fermée, on nous a indiqué que l'entrée avait été laissée ouverte pendant le quart de travail de jour (de 8 h à 16 h). Cette pratique a été adoptée en raison du passage continuel d'inhalothérapeutes qui entrent et sortent en poussant du matériel roulant chaque jour. L'accès étant demeuré ouvert, les membres du personnel autorisé n'avaient pas besoin de glisser leur carte d'accès chaque fois qu'ils passaient par l'entrée principale du service.

10. Dans le service, une autre porte mène à l'extérieur, soit une sortie de secours qui demeure fermée et verrouillée en tout temps; pour des raisons évidentes, on peut l'ouvrir de l'intérieur en cas d'urgence.

11. Le personnel de ce service est constitué d'employés à plein temps, à temps partiel et occasionnels; il y a quelqu'un en poste jour et nuit. Les quarts de travail se déroulent le jour, le soir et la nuit, selon l'horaire suivant : de 8 h à 16 h, de 8 h à 20 h, et de 20 h à 8 h. Toutefois, les employés ne se trouvent pas toujours dans le service, en raison de leurs fonctions qui les obligent à se rendre dans d'autres secteurs de l'hôpital.

12. Nous soulignons que seul le personnel de jour a adopté la pratique de garder ouverte la porte d'entrée; ainsi, lorsqu'ils cèdent la place au quart de travail suivant, à 16 h, ils ferment la porte.

13. Le jeudi 11 juin 2015, le personnel du service trouvait la température des locaux très élevée pendant le jour, et ce, même si la porte était ouverte. Alors, pour rafraîchir les locaux, les membres du personnel qui quittent les lieux à 16 h ont décidé de laisser la porte ouverte au moment de leur départ. Ils ferment habituellement la porte d'entrée à 16 h, heure de leur départ.

14. Comme le veut leur quart de travail habituel, les membres du personnel étaient en poste jusqu'à 20 h ce soir-là et, encore une fois, comme la nature de leur travail les obligeait à aller et venir dans d'autres secteurs de l'hôpital, ils sont entrés et sortis du service entre 16 h et 24 h. Le 11 juin 2015, la seule différence est que, pendant ce quart de travail, la porte d'entrée au service a été laissée ouverte.

15. Pour bien rendre compte de cette atteinte, il est important de savoir de quelle façon le vol a été commis, en commençant par établir l'endroit où se trouvait l'ordinateur portatif, qui pouvait y avoir accès et comment il a été volé. Après quoi, nous analyserons les données qu'il contenait.

Ordinateur portatif volé

16. Le service utilisait trois ordinateurs pour faire ses tests. Un ordinateur de bureau se trouvait sur un bureau à l'intérieur du service, et deux ordinateurs portatifs étaient déposés chacun sur un chariot mobile (il y avait deux chariots mobiles en tout).

17. Le premier ordinateur portatif était fixé à son chariot mobile par un câble et un cadenas; par contre, le cadenas à combinaison n'était pas verrouillé. L'autre ordinateur portatif était fixé à son chariot mobile par un câble et un cadenas, et le cadenas à combinaison était verrouillé.

18. Un de ces ordinateurs portatifs a été volé, celui dont le cadenas n'était pas verrouillé. De plus, l'accès à cet ordinateur n'était pas chiffré ni protégé par un mot de passe.

19. En fait, nous avons découvert par la suite qu'aucun des ordinateurs (aucun des trois) n'avait un accès chiffré ou protégé par un mot de passe.

20. Nous comprenons que l'ordinateur volé contenait les renseignements personnels sur la santé des 158 patients qui avaient subi des tests de spirométrie depuis février 2015 (soit le type de test que réalise ce service). Plus précisément, les données recueillies et stockées sur l'ordinateur étaient les suivantes : le nom des patients, leur numéro d'assurance-maladie, leur date de naissance, le nom de leur médecin, leur poids et leur taille, les raisons de l'examen, une consultation médicale ou un diagnostic proposé, leurs antécédents respiratoires notables, les données brutes des tests et les médicaments pour troubles cardiaques ou respiratoires. Nous remarquons que le nom et le numéro de téléphone des patients n'étaient pas sauvegardés dans l'ordinateur.

21. Les ordinateurs portatifs servaient à faire les tests de spirométrie et d'autres tests respiratoires. Ils étaient installés sur des chariots mobiles pour permettre de réaliser ces tests soit au chevet du patient dans l'hôpital, soit au service d'électrocardiographie, ou encore au laboratoire de fonction pulmonaire pour les patients externes qui ont un rendez-vous. Le service d'électrocardiographie et les laboratoires de fonction pulmonaire sont tous deux situés tout près du service d'inhalothérapie, et le personnel du service (les inhalothérapeutes) déplacent le chariot mobile sur lequel se trouve l'ordinateur portatif, vers l'un ou l'autre de ces emplacements. Une fois les tests effectués, le chariot mobile est renvoyé au service.

22. Comme il est indiqué ci-dessus, le jour de l'incident, le personnel du service qui travaille pendant la journée a laissé ouverte la porte d'entrée après 16 h, dans l'espoir de rafraîchir les lieux pendant la soirée.

23. D'après l'enquête interne du Réseau de santé Horizon, il semblerait que l'ordinateur portatif soit disparu entre 16 h et 24 h, le soir du 11 juin 2015, soit pendant la période où la porte d'entrée du service est restée ouverte. C'est seulement après avoir constaté l'absence de l'ordinateur portatif sur son chariot, peu après minuit, que l'on a fermé la porte du service.

24. Nous savons que, d'après les habitudes du personnel, le service est laissé sans surveillance pendant des périodes indéterminées, ce qui signifie que c'était le cas ce soir-là, pendant les quarts de travail de la soirée et de la nuit (entre 16 h et 24 h, heure à laquelle la porte d'entrée a été fermée).

25. Peu après minuit, le membre du personnel a remarqué qu'un des deux ordinateurs portatifs n'était pas sur son chariot mobile. Présumant qu'il avait été envoyé à l'entretien, le membre du personnel n'a pas signalé l'absence de l'ordinateur au personnel de jour, lorsqu'il a terminé son quart de travail à 8 h. D'après les faits, il semble que le personnel des quarts de jour et de soir n'a pas remarqué non plus l'absence de l'ordinateur, puisque c'est seulement à la fin de l'après-midi ou au début de la soirée du 12 juin qu'un membre du personnel a remarqué qu'il ne se trouvait pas sur son chariot mobile.

26. Ne sachant pas si l'ordinateur portatif avait été envoyé à l'entretien ou volé, le membre du personnel a demandé au coordonnateur du service d'inhalothérapie s'il savait où il était. C'est seulement à ce moment que tous ont constaté que l'ordinateur n'avait pas été envoyé à l'entretien et qu'il était disparu.

27. Le coordonnateur du service d'inhalothérapie a ensuite demandé au membre du personnel de communiquer avec l'agent administratif et le bureau de la sécurité de l'hôpital, avant de remplir un rapport d'incident pour signaler à l'hôpital la disparition de l'ordinateur portatif.

28. Celui-ci n'a jamais été retrouvé, et le bureau de la sécurité a indiqué qu'il ne disposait d'aucune image vidéo montrant quelqu'un en possession de l'ordinateur dans le couloir pendant cette période. Nous constatons qu'il n'y a aucune caméra de surveillance à l'entrée du service. L'enquête d'Horizon n'a révélé aucune activité suspecte, sauf la

présence dans le secteur d'un patient qui a été interrogé par la suite et dont la chambre a été fouillée. Encore une fois, les recherches n'ont pas abouti.

Absence de mécanismes de sécurité pour protéger l'ordinateur

29. Dans le cadre de notre enquête, nous avons établi les raisons pour lesquelles l'ordinateur portatif n'était pas fixé à son chariot mobile au moyen d'un câble et d'un cadenas à combinaison, et n'était pas chiffré ni protégé par un mot de passe. Plus important encore, nous avons soulevé plusieurs questions sur le fait que le service était totalement accessible à tout venant, étant laissé sans surveillance avec la porte grande ouverte.

30. Nous soulignons que l'accès au service est censé être réservé uniquement au personnel autorisé, et que cette préoccupation dominante s'est concrétisée par l'obligation de glisser une carte d'accès approuvée pour pouvoir y entrer. Nous constatons donc que la principale cause de cette atteinte à la vie privée est la porte du service laissée ouverte en l'absence de surveillance par le personnel.

31. Nous pensons aussi qu'il était possible d'éviter l'incident en laissant simplement l'entrée fermée et accessible uniquement aux personnes autorisées. Autrement, comme ce fut le cas dans la présente affaire, un passant pouvait apercevoir l'ordinateur sur un chariot et saisir l'occasion de s'en emparer.

32. Il est encore plus troublant de constater qu'on n'a pas suivi la politique d'Horizon et de l'hôpital exigeant que les appareils médicaux soient fixés au moyen d'un câble et d'un cadenas, pendant l'utilisation des chariots mobiles.

33. Dans le passé, les deux ordinateurs portatifs du service étaient constamment fixés à leur chariot mobile au moyen d'un cadenas à combinaison. Or, au moment de l'incident, l'ordinateur en question semblait verrouillé alors qu'il ne l'était pas. Encore une fois, il est facile pour un individu de saisir l'occasion et de s'emparer d'un ordinateur lorsque le cadenas est déverrouillé.

34. Même après avoir reconnu qu'il s'agit d'une des causes de l'atteinte à la vie privée, Horizon a expliqué que cet oubli est survenu lorsque l'ordinateur en question a été acheté auprès de FacilicorpNB en février 2015, pour remplacer l'ancien modèle. L'ancien ordinateur avait été fixé au chariot mobile au moyen d'un câble et d'un cadenas à combinaison. Le service a également connu un changement de personnel, notamment

dans le cas des responsables de l'entretien des ordinateurs portatifs (soit la division de l'Ingénierie clinique de FacilicorpNB, comme il est décrit ci-dessous). Le roulement de personnel a eu pour conséquence que personne ne connaissait la combinaison du cadenas de l'ancien ordinateur portatif. Le cadenas a donc été coupé et remplacé par un nouveau.

35. De plus, le manque de communication entre le personnel du service et la division de l'Ingénierie clinique au moment de décider qui sera responsable d'attribuer une combinaison au nouveau cadenas a eu pour effet que l'on n'a jamais fixé convenablement le cadenas au chariot mobile.

36. C'est à la division des TI de FacilicorpNB qu'il incombe d'installer tout le matériel informatique utilisé par Horizon et de veiller à ce que les données et les renseignements soient sauvegardés et gérés en toute sécurité. Cela dit, l'utilisation qui est faite des ordinateurs, y compris la manière dont les données y sont placées ou stockées, demeure néanmoins la responsabilité d'Horizon ou de l'hôpital qui les utilise. Or, la division de l'Ingénierie clinique de FacilicorpNB inspecte et entretient les appareils médicaux thérapeutiques et les équipements de diagnostic spécialisé dont se servent les professionnels de la santé.

37. Lorsqu'Horizon utilise ces appareils pour sauvegarder des renseignements de nature délicate sur les patients, sa politique, tout comme celle de FacilicorpNB, prescrit de stocker ces données sur le système de réseau sécurisé, lequel permet de récupérer les données advenant une défaillance ou, comme dans le cas présent, le vol d'un ordinateur.

38. C'est en février 2015 qu'Horizon s'est procuré cet ordinateur portatif auprès de FacilicorpNB, pour remplacer un ancien modèle. Aussi, l'ordinateur a été acheté auprès de FacilicorpNB parce que le fournisseur du logiciel de test de spirométrie et du dispositif de diagnostic n'en a pas fourni, même s'il en fallait un pour utiliser cet outil médical. Ce logiciel et cet appareil ont été testés, sans grand succès. Il n'a donc pas été possible au moment du vol de chiffrer l'ordinateur portatif parce que le logiciel et les données étaient intégrés dans le même dispositif.

39. Par conséquent, l'ordinateur portatif a été acheté uniquement pour exploiter le logiciel qui permet de compiler les résultats des tests respiratoires.

40. Lorsque FacilicorpNB a fourni l'ordinateur portatif, on y a intégré un mot de passe. Toutefois, au moment de l'installation du logiciel de tests de spirométrie, on a supprimé la procédure de connexion parce que l'ordinateur (et ses données) n'allait pas être connecté au système de réseau sécurisé d'Horizon.

41. Horizon nous a indiqué que les anciennes techniques de chiffrement en place au moment de l'incident exigeaient l'emploi d'un mot de passe distinct de celui de la connexion pour permettre le chiffrement. Étant donné que certains appareils passaient par de multiples utilisateurs tout au long de la journée, notamment les ordinateurs portatifs et le dispositif permettant d'effectuer les tests de spirométrie, la nécessité d'un mot de passe distinct de celui de la connexion ne constituait pas une solution pratique pour différents milieux médicaux dans lesquels les différents appareils étaient partagés par de nombreux membres du personnel en rotation. Les régies régionales de la santé ne peuvent prendre le risque de voir leur personnel incapable d'accéder à des renseignements médicaux en raison d'un changement de mot de passe ou d'une omission de le communiquer.

DÉMARCHES ENTREPRISES POUR LIMITER L'ATTEINTE

42. Nous savons qu'après avoir découvert que l'ordinateur portatif était disparu ou avait été volé, des démarches ont été entreprises pour déterminer son emplacement et vérifier si la surveillance vidéo pouvait révéler des indices permettant de le retrouver, mais en vain.

43. Ainsi, Horizon a signalé le vol au service de police de Fredericton et aussi communiqué avec plusieurs bureaux locaux de prêteurs sur gages, mais encore une fois sans succès.

44. Lors d'une réunion tenue le 17 juin 2015, on a demandé à FacilicorpNB si la cybercaméra de l'ordinateur volé pouvait être activée à distance et fournir des indices de son emplacement, mais comme l'ordinateur portatif n'était pas connecté au réseau sécurisé d'Horizon, les cartes sans fil n'avaient pas été activées au départ.

45. Les données ont été volées, mais elles n'ont pas été perdues, parce que les résultats des tests des patients ont été récupérés sur les fichiers physiques en papier.

46. Par conséquent, cette atteinte a donné lieu à la communication de renseignements sur la santé de certains patients à des personnes non autorisées.

PROCESSUS DE NOTIFICATION

47. La *Loi* exige que les fournisseurs de soins de santé ou les dépositaires[1] aux termes de la *Loi* protègent en tout temps les renseignements personnels sur la santé de leurs patients et de leurs clients, 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. Dans la présente affaire, les dépositaires responsables sont l'hôpital et Horizon.

48. Lorsque des renseignements personnels sur la santé sont volés, perdus ou éliminés, ou lorsqu'une personne non autorisée y a accès, cela constitue une atteinte à la vie privée en vertu de la *Loi* et le dépositaire responsable, soit Horizon et l'hôpital dans la présente affaire, est tenu d'aviser les personnes concernées ainsi que la Commissaire, en application de l'alinéa 49(1)*c*) de la *Loi*.

49. Lorsqu'un appareil n'est pas chiffré, la personne qui l'a volé et qui n'est pas autorisée à les voir peut accéder aux données qu'il contient. Il est donc particulièrement important d'aviser les personnes concernées lorsque le vol de renseignements personnels pourrait mener à leur identification, et causer une menace à leur vie privée et leur identité.

50. Horizon a signalé l'atteinte à la Commissaire le 16 juin 2015. Après cela est venue la tâche d'aviser les personnes concernées. Le personnel du service a immédiatement commencé à comparer les patients qui avaient subi des tests de spirométrie depuis l'achat de l'ordinateur portatif, en février 2015, avec les personnes dont les renseignements y étaient sauvegardés. Le personnel a passé en revue les listes de patients, l'historique des visites et la charge de travail, ainsi que le dossier médical physique des patients dont les résultats des tests de spirométrie avaient été imprimés et insérés. Il a fallu y consacrer du temps et des efforts, en procédant par élimination, le service a été en mesure de confirmer que les renseignements perdus concernaient 158 patients.

51. Par des lettres envoyées le 13 juillet 2015, toutes ces personnes ont été avisées des faits suivants :
    - les détails de l'atteinte;

[1] Aux termes de la *Loi*, « dépositaire » désigne une personne, un groupe ou un établissement que la loi charge de recueillir, maintenir et utiliser des renseignements personnels sur la santé (comme ceux des patients dans la présente affaire), et de les protéger en tout temps conformément aux dispositions prévues par la *Loi*.

- les renseignements personnels sur la santé sauvegardés dans l'ordinateur;
- les conséquences du vol, qui étaient inconnues à ce moment;
- l'envoi de l'avis d'une atteinte au Commissariat à la protection de la vie privée;
- le signalement du vol au service de police de Fredericton;
- les coordonnées nécessaires pour se procurer un nouveau numéro d'assurance-maladie;
- les démarches entreprises par Horizon dans la foulée de ce grave incident, y compris la révision de ses processus internes;
- les coordonnées du chef de la protection de la vie privée d'Horizon;
- l'énoncé du droit des patients de communiquer* avec le Commissariat à la protection de la vie privée (avec les coordonnées d'un représentant).

**Nous soulignons qu'il faut aviser les patients de leur droit de se plaindre auprès du Commissariat à la protection de la vie privée, plutôt que de simplement communiquer avec le Commissariat.*

52. Sur les 158 patients avisés, 26 ont communiqué directement avec le Bureau de la vie privée du Réseau de santé d'Horizon pour s'informer sur cet incident. Le Commissariat a également reçu les demandes et plaintes de plusieurs personnes, et trois d'entre elles ont décidé de déposer une plainte officielle comme le leur permet le paragraphe 68(2) de la *Loi*.

> 68(2) Sans que soit limitée la portée de l'alinéa (1)*a*), la personne physique peut déposer auprès du Commissaire une plainte dans laquelle elle prétend que le dépositaire :
> *a*) a recueilli, utilisé ou communiqué les renseignements personnels sur la santé la concernant, en violation de la présente loi;
> *b*) a omis de protéger de façon sécuritaire les renseignements personnels sur la santé la concernant contrairement aux exigences de la présente loi.

53. Ces personnes s'inquiétaient toutes à l'idée que la perte de renseignements personnels sur la santé puisse entraîner un vol d'identité, parce que leur numéro d'assurance-maladie avait également été volé. Notre enquête sur cette plainte faisait partie du dossier de notification de l'atteinte que nous avions ouvert quand nous avons été avisés de l'incident.

La perte de renseignements personnels peut-elle mener à un vol d'identité?

54. On nous demande souvent d'évaluer le risque de vol d'identité dans le cadre d'incidents de cette nature.

55. Au nombre des renseignements perdus dans la présente affaire, mentionnons le nom des patients et d'autres renseignements d'ordre médical, dont leur numéro d'assurance-maladie. Heureusement, ni leur numéro de téléphone ni leur adresse ne figuraient parmi les données perdues.

56. Bien qu'il soit impossible d'établir avec un quelconque degré de certitude le risque que court une personne en ce qui a trait au vol d'identité lorsque l'intégrité de ses renseignements personnels a été compromise, 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.

57. 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 par lesquelles un imposteur adopte l'identité de quelqu'un d'autre pour avoir accès à ses biens. Il n'est pas possible d'assurer en même temps la surveillance du crédit et des renseignements personnels perdus.

58. Toute personne s'inquiétant du risque de vol d'identité fait preuve de prudence lorsqu'elle adopte des mesures simples, dans son horaire mensuel, afin de diminuer le risque que ses renseignements personnels se trouvent entre de mauvaises mains. En voici quelques-unes :

- 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 cartes de crédit afin de vérifier qu'ils ne contiennent aucun achat non autorisé;
- obtenir un rapport de crédit annuel (les grands bureaux de crédit en fournissent un gratuitement chaque année);
- se créer un nouveau mot de passe pour chaque compte en ligne et le changer fréquemment (un mot de passe est fiable s'il est difficile pour quiconque de le 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);
- lire 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 (nous suggérons

de consulter le site Web du Commissariat à la protection de la vie privée du Canada, au www.priv.gc.ca).

59. Dans certains cas particuliers, on peut conseiller aux patients exposés à un degré de risque plus élevé de s'adresser aux services de l'Assurance-maladie du ministère de la Santé pour demander une nouvelle carte d'assurance-maladie.

60. On a également invité les patients à surveiller leur compte en banque et, en cas de doute, d'aviser leur institution bancaire. De plus, Horizon a offert de rembourser toutes les demandes de vérification de crédit.

MESURES CORRECTIVES

61. Horizon a pris plusieurs mesures correctives pour prévenir la récurrence d'incidents similaires. Pour commencer, le service en question doit maintenant veiller à mettre en place les mesures de sécurité qui auraient dû s'appliquer dès le départ aux appareils électroniques contenant des renseignements personnels sur la santé. Ces mesures comptaient entre autres la possibilité de supprimer les données de patients sur les appareils mobiles.

62. Horizon a installé une protection par mot de passe sur tous les ordinateurs et appareils utilisés par ce service, fixé chaque ordinateur portatif à son chariot mobile respectif au moyen d'un dispositif de verrouillage, et exigé que la porte d'entrée reste fermée à clé 24 heures sur 24, 7 jours sur 7. Cette porte ne peut être ouverte qu'au moyen d'une carte magnétique. Ces mesures ont été prises dans les deux semaines suivant l'incident.

63. Une nouvelle politique en cours d'élaboration exigera que tous les appareils portatifs soient chiffrés et protégés par un mot de passe, quel que soit leur statut. Par contre, certains appareils n'offrent pas ces options. Dans ces cas, FacilicorpNB et les régies régionales de la santé devront établir des communications claires pour trouver d'autres garanties permettant d'assurer la confidentialité des renseignements personnels sur la santé.

64. Nous comprenons qu'à une plus grande échelle, on a instauré progressivement le chiffrement sur environ 2400 ordinateurs portatifs utilisés par le personnel de l'hôpital, ainsi que sur les appareils qu'utilisent les employés d'Horizon et de FacilicorpNB. Au moment de l'incident, environ 305 appareils étaient chiffrés; depuis l'incident toutefois, 98 % des 2400 ordinateurs portatifs ont été chiffrés et protégés par mot de passe.

65. D'autres mesures ont été prises, principalement pour la gestion et le maintien des mécanismes de sécurité et, selon nous, ces mesures devraient permettre d'éviter la récurrence de circonstances où personne ne connaît la combinaison du cadenas, la possibilité de chiffrer l'appareil, etc.

66. Encore une fois, en termes simples, nous estimons qu'au départ, il aurait été facile de prévenir le vol de l'ordinateur en gardant la porte fermée et en le fixant avec un cadenas verrouillé.

CONCLUSIONS DE LA COMMISSAIRE

67. L'atteinte à la vie privée était de taille, en ce sens qu'elle touchait un grand nombre de patients dont les renseignements personnels sur la santé ont été recueillis et sauvegardés dans un ordinateur portatif qui n'était pas doté de mesures de sécurité adéquates.

68. Cet incident montre sans ambiguïté la nécessité vitale de protéger les données confidentielles sur les appareils électroniques comme l'ordinateur portatif, surtout lorsqu'elles sont sauvegardées directement sur le disque dur de l'appareil plutôt que sur un réseau sécurisé.

69. Le logiciel de test de spirométrie n'était pas compatible avec le réseau sécurisé d'Horizon. Par conséquent, nous estimons qu'Horizon aurait dû prendre d'autres mesures pour s'assurer que l'ordinateur portatif serait protégé par chiffrement et par mot de passe.

70. Notre enquête a révélé qu'Horizon et le service d'inhalothérapie de l'hôpital ont failli à leur responsabilité de protéger les renseignements personnels sur la santé de leurs patients comme suit :

a) en laissant la porte d'entrée ouverte, pendant que la salle était sans surveillance pour une période de temps indéterminée;
b) en omettant de verrouiller l'ordinateur portable au chariot mobile, comme il se doit;
c) en permettant de stocker les renseignements de nature très délicate des patients sur un ordinateur portatif, sachant que celui-ci n'était pas protégé;
d) en omettant de protéger l'ordinateur par un mot de passe et les données par un chiffrement.

ABSENCE DE MESURES DE SÉCURITÉ

71. Comme il se doit, cette atteinte à la vie privée a donné lieu à un examen des mesures de sécurité qu'Horizon a mises en place pour protéger les renseignements personnels sur la santé sauvegardés sur les appareils électroniques.

72. En tant que dépositaire qui conserve des renseignements personnels sur la santé en format électronique, Horizon doit mettre en place les garanties supplémentaires prévues par la *Loi* et son *Règlement*, qui exigent une protection accrue de tous les appareils et dispositifs mobiles (clés USB, ordinateurs portatifs, etc.) afin de s'assurer que ces appareils bénéficient en tout temps d'une protection par mot de passe.

73. De plus, les appareils électroniques qui servent au stockage de renseignements personnels sur la santé, comme les ordinateurs portatifs, devront avoir un niveau supplémentaire de protection. Il faut utiliser d'extrême prudence lorsque l'on se sert de ces appareils et prendre des mesures de sécurité supplémentaires, aux termes du paragraphe 50(4) de la *Loi* et des paragraphes 20(1) et (2) du *Règlement* y afférent.

> 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.
>
> 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, telles 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;

> 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.

74. Même si la pratique de ne pas exiger un mot de passe pour se connecter à l'ordinateur volé pourrait avoir permis aux patients d'être servis plus rapidement, elle a eu pour effet nuisible de rendre vulnérables à une atteinte leurs renseignements personnels sur la santé.

75. Cela ne signifie pas que la protection par mot de passe et par chiffrement aurait prévenu le vol de l'ordinateur portatif, mais elle aurait réduit le risque d'accès non autorisé aux données confidentielles.

76. Pour toutes les raisons susmentionnées, nous estimons qu'au moment de l'incident, les mesures de sécurité adoptées et utilisées collectivement par l'hôpital et par Horizon n'étaient pas conformes aux normes imposées aux dépositaires en ce qui a trait à la protection des renseignements personnels sur la santé en vertu de la *Loi*.

77. Nous estimons également que les mesures en vigueur à cette époque n'étaient pas conformes à la *Loi*. Ainsi, Horizon et l'hôpital ne se sont pas acquittés de leur obligation légale de protéger les renseignements personnels sur la santé des patients de l'hôpital.

78. La *Loi* prescrit non seulement l'utilisation de mesures de sécurité, mais définit aussi une façon pragmatique de les mettre en œuvre en fonction de deux normes décrites ci-dessus : le caractère raisonnable et le niveau approprié au degré de confidentialité des données.

79. La première norme exige que les garanties soient raisonnables, ce qui signifie que les renseignements doivent être gardés en sécurité de manière raisonnable d'un point de vue objectif, et non d'après des choix subjectifs. En ce sens, les garanties de sécurité n'ont pas à être parfaites, mais elles doivent plutôt sembler raisonnables compte tenu des circonstances.

80. La deuxième norme exige que les mesures de sécurité soient établies en fonction du degré de sensibilité des renseignements que le dépositaire vise à protéger. Plus les renseignements sont sensibles, plus les mesures de sécurité doivent être importantes.

81. On peut aussi se fonder sur des observations relevant du gros bon sens pour établir d'autres mesures de sécurité raisonnables. Le simple verrouillage des portes et des

tiroirs constitue une mesure de sécurité efficace. Malheureusement, comme c'est arrivé dans la présente affaire, c'est souvent l'inattention aux pratiques quotidiennes qui cause le plus de risques en matière de sécurité.

82. Nous estimons à tout le moins que l'ordinateur portatif aurait dû être solidement verrouillé au chariot mobile, comme il est censé l'être, et que la porte d'entrée principale au service d'inhalothérapie ne devait pas être laissée ouverte en l'absence de toute surveillance dans le service.

83. Nous nous réjouissons de savoir que des mesures correctives ont été mises en place pour assurer une meilleure protection des renseignements des patients à l'avenir. Nous rappelons à tous, cependant, que des centaines de patients ayant profité des services d'inhalothérapie ont confié leurs renseignements confidentiels à ceux qui avaient le devoir de les protéger.

84. La *Loi* est conçue pour améliorer les soins de santé en veillant à ce que les patients se sentent à l'aise de communiquer les renseignements sur leur santé au personnel médical, sachant que leurs renseignements personnels seront utilisés de la façon la plus efficace et la plus sécuritaire possible. Cette confiance ne repose pas seulement sur les avantages de la technologie moderne qui soutiennent la prestation de soins de santé, mais aussi sur la notion que ceux qui utilisent cette technologie en feront usage en adoptant des méthodes sûres et raisonnables pour protéger leur vie privée.

85. N'oublions pas que cette affaire ne concerne pas seulement la facilité d'utilisation des appareils portatifs ou le fait de laisser une porte ouverte. Elle concerne aussi la protection des renseignements personnels d'une personne et, en cas de défaillance, ceux-ci tombent dans les mains d'individus qui ne devraient pas y avoir accès. C'est ce qui s'est passé dans la présente affaire.

86. Nous ajoutons néanmoins qu'Horizon et l'hôpital ont pris très au sérieux cette atteinte à la vie privée, ainsi que leur obligation d'adopter d'importantes mesures correctives pour s'assurer qu'il ne survienne pas d'incidents similaires dans l'avenir.

RECOMMANDATION

87. À la lumière des conclusions qui précèdent, la Commissaire recommande à Horizon et à l'hôpital de poursuivre leur mise en œuvre de toutes les mesures correctives qu'ils ont indiquées, dont certaines apparaissent dans le présent rapport des conclusions, jusqu'à

ce qu'elles les aient toutes mises en place, et à Horizon de fournir au Commissariat un rapport sur la situation ou sur l'achèvement de ces démarches au plus tard à la fin de juillet 2016.

Fait à Fredericton (Nouveau-Brunswick), ce 28 janvier 2016.

_____

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