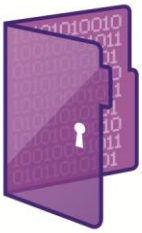
Office of the Access to Information and Privacy Commissioner
New Brunswick



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 : 2011-472-H-143
Affaires : 2011-535-H-167, 2011-537-H-168, 2011-548-H-171
Date : Le 13 septembre 2012

Enquête menée par la Commissaire

Atteinte à la vie privée – vol d'un ordinateur portable dans un hôpital

Contexte

1. Le Centre hospitalier universitaire Dr Georges L. Dumont de Moncton (ci-après « l'Hôpital ») héberge un centre de traitement spécialisé en néphrologie et en urologie (ci-après « le centre de traitement »), qui abrite aussi une clinique pour patients externes devant subir une épreuve urodynamique (ci-après « la clinique »).

2. Le lundi 29 août 2011 au matin, à son arrivée au centre de traitement et à son entrée dans la clinique, un employé s'est aperçu que l'ordinateur portable normalement situé dans la seule pièce qui constitue la clinique n'était pas là. Cet ordinateur était pourvu de logiciels spécialisés dont la clinique se servait pour établir des diagnostics. L'employé a averti les responsables de l'Hôpital.

3. L'Hôpital, le centre de traitement et la clinique relèvent tous du Réseau de santé Vitalité. L'Hôpital a informé sur-le-champ la directrice principale de la Protection des renseignements personnels du Réseau de santé Vitalité de ce qui s'est passé, et cette dernière s'est penchée sur l'incident. D'après les faits découverts décrits ci-après, le Réseau de santé Vitalité croyait que l'ordinateur portable manquant avait en fait été volé, puis a signalé le vol au détachement local de la Gendarmerie royale du Canada.

Avis d'atteinte à la protection de la vie privée

4. D'après la *Loi sur l'accès et la protection en matière de renseignements personnels sur la santé* (ci-après la « *Loi* »), on considère qu'il y a eu atteinte à la vie privée lorsque des renseignements personnels sur la santé ont été volés, perdus ou éliminés ou lorsqu'une personne non autorisée a eu accès à ces renseignements ou qu'ils lui ont été communiqués. En présence d'une de ces situations, la personne, le groupe ou l'organisation à qui ces renseignements personnels sur la santé avaient été confiés, que la *Loi* désigne sous le nom de dépositaire, est tenue de prendre des mesures. Le dépositaire est celui qui utilise des renseignements personnels sur la santé aux fins de prestation ou d'aide à la prestation de soins de santé. Ainsi, le Réseau de santé Vitalité, l'Hôpital, le centre de traitement et la clinique sont tous des dépositaires.

5. Dans la présente affaire, il y a eu atteinte à la vie privée des patients de la clinique lorsque l'ordinateur portable, qui n'était pas protégé par un mot de passe et qui contenait les données médicales des patients, donc des renseignements personnels sur leur santé, a été volé. Il n'est donc pas impossible que les renseignements confidentiels de ces patients puissent être vus par une personne non autorisée, c.-à-d. la ou les personnes qui ont volé l'ordinateur portable.

6. L'alinéa 49(1)*c)* de la *Loi* prévoit qu'un dépositaire qui découvre qu'une atteinte à la vie privée a eu lieu est tenu d'aviser le plus tôt possible toutes les personnes concernées que la confidentialité de leurs renseignements personnels sur la santé a été compromise. C'est ce que l'on appelle le processus de notification. La *Loi* exige aussi du dépositaire qu'il avise la Commissaire de cette atteinte à la vie privée le plus tôt possible. Dans le cadre de ce processus de notification, les personnes concernées doivent être informées de ce qui s'est produit et du moment où l'incident a eu lieu. Ces personnes doivent, en outre, être avisées de leur droit de déposer une plainte auprès du Commissariat en vertu du paragraphe 68(2) de la *Loi.* Si elles choisissent de se prévaloir de leur droit, la plainte permettra à la Commissaire d'enquêter sur l'atteinte à la vie privée et de formuler ses conclusions et ses recommandations connexes, le cas échéant, dans un rapport des conclusions.

7. Lorsque ce vol a été découvert, le Réseau de santé Vitalité a signalé l'atteinte à la vie privée à la Commissaire ainsi qu'au chef de la protection des renseignements personnels du ministère de la Santé. Ces événements ont eu lieu le 31 août 2011. Dans le présent rapport des conclusions, nous discutons des conclusions auxquelles nous sommes parvenus à l'issue de l'enquête que nous avons entreprise parallèlement à celle du Réseau de santé Vitalité.

8. Le Réseau de santé Vitalité a vérifié que l'ordinateur portable volé avait bel et bien servi à stocker des renseignements personnels sur la santé de plusieurs centaines de patients de la clinique. Parmi les données emmagasinées se trouvaient des renseignements personnels appartenant à ces patients et des renseignements sur leur santé. Ces patients appartenaient à trois groupes : des adultes, des enfants et des personnes maintenant décédées. Toutes ces personnes, leurs parents ou tuteurs ou encore les membres de leur famille (en fonction du type de patient) ont été avisés par une lettre postée au début d'octobre 2011. Cette lettre d'avis les informait que l'atteinte découlait du vol de l'ordinateur portable de la clinique et les avisait de leur droit de déposer une plainte auprès de la Commissaire à propos de cette atteinte.

9. Sur les centaines de patients avisés, nombre d'entre eux ont communiqué directement avec le Bureau de la vie privée du Réseau de santé Vitalité pour s'informer sur cet incident auprès des agents responsables. Cinq personnes nous ont transmis une plainte, demandé des

renseignements ou fait part de leurs préoccupations. Trois d'entre elles ont choisi de déposer une plainte officielle en vertu de la *Loi,* et ces plaintes sont résumées ci-dessous.

Plaintes déposées par des patients concernés

10. Après avoir été avisées de l'atteinte à la vie privée, trois personnes ont déposé une plainte auprès de notre bureau, et nous avons entrepris une enquête officielle sur cette affaire. Ces personnes cherchaient principalement les réponses aux questions suivantes :

> *Pourquoi l'ordinateur se situait-il dans un endroit accessible au public où il pouvait être volé?*
>
> *Pourquoi l'ordinateur n'était-il pas pourvu de plus de dispositifs de sécurité?*
>
> *La perte de renseignements personnels peut-elle mener à un vol d'identité et avoir une incidence sur les antécédents financiers de la personne concernée?*
>
> *Quelles mesures sont prises actuellement pour corriger cette atteinte et pour empêcher que des incidents semblables ne se produisent à l'avenir?*

11. Le présent rapport des conclusions de l'enquête de la Commissaire répond à ces questions et renferme une description de l'événement, les raisons pour lesquelles cette atteinte s'est produite et les recommandations émises quant aux mesures correctrices à prendre pour empêcher qu'un incident de la sorte ne se produise de nouveau dans l'avenir.

Pourquoi et comment cette atteinte s'est-elle produite?

12. En moyenne, ce sont entre 500 et 600 patients environ par jour qui se rendent au centre de traitement dans le but précis d'obtenir des services auprès de la clinique. La trentaine d'employés de la clinique travaille de 8 h 30 à 16 h 30 tous les jours, sauf la fin de semaine, la clinique étant alors fermée. Il faut aussi savoir que, bien que la clinique cesse ses activités à 16 h 30, le centre de traitement ne ferme ses portes au public qu'à 19 h.

13. La clinique ne compte qu'une seule pièce, soit celle où se trouvait l'ordinateur portable. La porte qui mène à cette pièce se verrouille automatiquement une fois fermée; les employés la laissent toutefois délibérément ouverte à la fin de leur quart de travail pour permettre au personnel de l'entretien ménager d'entrer dans la clinique. Une fois son travail terminé, le personnel de l'entretien ménager referme la porte, qui se verrouille alors automatiquement,

derrière lui. D'après ce que nous avons compris, l'entretien de la pièce est habituellement terminé à 18 h.

14. Le vendredi, le dernier employé sort de la clinique à 16 h 30, et la clinique demeure fermée jusqu'au lundi matin suivant. Le personnel de sécurité effectue une ronde de sécurité dans cette partie du centre vers 18 h tous les jours, même le vendredi, et vérifie alors que la porte de la clinique est bien verrouillée. Cette pièce demeure fermée à clé jusqu'à 7 h le lundi matin suivant, heure à laquelle le personnel de sécurité déverrouille la porte de la clinique (la porte de la pièce) pour permettre l'accès aux employés qui arrivent pour leur quart de travail. Les employés de la clinique arrivent habituellement entre 8 h et 8 h 15.

15. Nous pouvons donc conclure que la pièce où se trouvait l'ordinateur portable est laissée déverrouillée et sans surveillance entre 16 h 30 et 18 h chaque jour, sauf pour le laps de temps pendant lequel le personnel de l'entretien ménager vient y faire son tour, et pendant environ une heure chaque matin, soit entre 7 h et 8 h ou 8 h 15, heure d'arrivée du premier employé de la clinique. Avant la fin de semaine, la clinique est laissée déverrouillée et sans surveillance de 16 h 30 à 18 h le vendredi soir, sauf pour le laps de temps pendant lequel le personnel de l'entretien ménager vient y faire son tour, après quoi la clinique demeure fermée à clé de 18 h jusqu'aux environs de 7 h le lundi matin suivant, lorsque le personnel de sécurité vient déverrouiller la porte. La clinique demeure alors déverrouillée et sans surveillance pendant environ une heure, jusqu'à l'arrivée des employés vers 8 h ou 8 h 15. De ce que nous comprenons, la porte ne peut être déverrouillée que par le personnel de sécurité.

16. Dans la présente affaire d'atteinte à la vie privée, les faits montrent que le dernier employé a quitté la clinique à la fin de la journée du vendredi 26 août 2011 aux environs de 16 h 30. La porte a été laissée déverrouillée pour permettre au personnel de l'entretien ménager d'entrer dans la clinique. Nous savons que le personnel de sécurité a effectué sa ronde à 18 h ce soir-là, comme d'habitude, et a signalé que la porte de la clinique était fermée à clé. Elle est demeurée verrouillée jusqu'à 7 h 4 le lundi 29 août 2011, heure à laquelle le personnel de sécurité l'a déverrouillée pour permettre aux employés d'accéder à la clinique. Le premier employé, qui est arrivé sur les lieux environ une heure plus tard ce jour-là (tout juste après 8 h), s'est aperçu que l'ordinateur portable n'était pas là.

17. On ne sait pas bien à quel moment le vol a été perpétré, mais, d'après l'enquête, il a fallu que ce soit entre le vendredi soir et le lundi matin, pendant les périodes où la clinique a été laissée sans surveillance, car il n'y a aucune trace d'accès forcé. Les recherches menées n'ont pas permis de retrouver l'ordinateur portable manquant. Les caméras de sécurité situées dans la clinique n'ont capté aucune preuve susceptible d'aider à la présente enquête. Le Réseau

de santé Vitalité croit que, dans cette affaire, l'ordinateur portable a été volé et il a signalé le vol à la police. Hélas, la police ne possède aucune piste qui lui permettrait de récupérer l'ordinateur portable.

18. L'ordinateur en question est un ordinateur portable dans lequel était installé un logiciel spécialisé servant dans le cadre des épreuves spécialisées de la clinique. Il était attaché par un câble et un dispositif de verrouillage à un appareil de diagnostic, ces deux appareils étant placés sur un chariot mobile.

19. On n'a découvert qu'après le vol que le câble devant relier l'ordinateur portable à l'appareil de diagnostic – câble qui a été laissé derrière par le voleur avec une pièce du dispositif de verrouillage – était censé être attaché à l'ordinateur portable de manière à ce qu'il soit impossible de l'enlever, mais que le câble avait plutôt été attaché à un cadenas, ce qui a augmenté les chances que l'ordinateur portable soit volé. Une clé USB devant être utilisée en combinaison avec cet ordinateur portable a aussi été laissée sur place par le voleur.

20. Conformément à la politique du Réseau de santé Vitalité, les données enregistrées dans l'ordinateur portable devaient être chiffrées et on ne devait pouvoir y accéder qu'au moyen du logiciel de chiffrement installé sur une clé USB. De plus, d'après la procédure approuvée du Réseau de santé Vitalité au sujet du stockage de ce genre de données confidentielles, les employés ne doivent pas sauvegarder les données directement sur le disque dur de l'ordinateur, mais plutôt sur le système de réseau sécurisé (appelé MediTech), qui est géré par FacilicorpNB. Cette entreprise offre des services de soutien en matière de technologies de l'information au Réseau de santé Vitalité, entre autres acteurs du système de santé de la province. FacilicorpNB est chargée de l'installation de tout le matériel informatique du Réseau de santé Vitalité, mais l'utilisation qui est faite des ordinateurs, y compris la manière dont les données y sont placées ou stockées, demeure du ressort des établissements qui se servent du matériel comme les hôpitaux, les cliniques et leurs employés. Le stockage des données sur le système de réseau sécurisé permet de récupérer les données advenant une défaillance ou, comme dans le cas présent, le vol d'un ordinateur.

21. L'enquête réalisée dans le cadre de cette affaire a permis de savoir que les renseignements médicaux appartenant aux patients de la clinique avaient en fait été stockés directement sur le disque dur de l'ordinateur portable. À l'occasion, les renseignements étaient sauvegardés directement sur le bureau de l'ordinateur pour permettre au personnel d'y accéder rapidement. De plus, les données enregistrées dans l'ordinateur portable n'étaient pas chiffrées. En conséquence, n'importe qui peut accéder aux données sans avoir à utiliser la clé USB renfermant le logiciel de chiffrement.

22. Les renseignements médicaux ont donc été perdus lorsque l'ordinateur a été volé. Heureusement, le personnel de la clinique avait l'habitude de produire une version imprimable des renseignements diagnostiques des patients, de sorte qu'ils puissent être examinés et interprétés plus tard, et ces rapports papier étaient versés au dossier des patients. C'est l'unique raison pour laquelle les renseignements personnels sur la santé de ces patients n'ont pas été perdus complètement.

23. L'ordinateur portable en question renfermait des renseignements personnels sur la santé liés au diagnostic d'environ 550 patients de la clinique, y compris leur nom, leur sexe, leur date de naissance, le nom du médecin ayant prescrit l'épreuve et quelques notes au sujet du diagnostic du patient; par contre, ni l'adresse des patients, ni leur numéro d'assurance-maladie, ni leur numéro de téléphone n'y étaient enregistrés.

Quel est le niveau de sécurité acceptable pour les renseignements?

24. Les données confidentielles sont protégées par l'adoption de pratiques relatives aux renseignements personnels sur la santé qui comportent des garanties administratives, techniques et physiques raisonnables. Tandis que les garanties administratives (par exemple, politiques et procédures relatives à la confidentialité, formation pour le personnel sur les politiques et les procédures) verront à préserver l'exactitude et l'intégrité des renseignements, les garanties physiques et techniques, quant à elles, feront en sorte que les données confidentielles restent confidentielles et en sûreté :

Voici quelques exemples de garanties physiques :

- sécurité physique de l'immeuble;
- classeurs verrouillés;
- endroits d'entreposage verrouillés, dispositifs mobiles rangés de manière sécuritaire lorsqu'ils ne sont pas utilisés (éviter, par exemple, de les laisser sur un bureau sans surveillance);
- pratiques sécuritaires lorsque les employés s'éloignent du bureau ou de l'ordinateur le jour comme le soir (personnel de l'entretien ménager/qui a accès aux endroits?, etc.).

Voici quelques exemples de garanties techniques :

- contrôles d'accès destinés à veiller à ce que seuls les employés qui ont besoin des renseignements pour s'acquitter de leur travail y aient accès;
- mots de passe difficiles à deviner et chiffrement pour les ordinateurs, les réseaux sans fil et tous les appareils mobiles;
- déconnexion automatique et verrouillage de l'appareil lorsqu'il n'est pas utilisé.

25. En particulier, les dépositaires qui conservent des renseignements personnels sur la santé en format électronique doivent mettre en place des garanties supplémentaires comme l'exige la *Loi* et le règlement y afférent, qui mettent l'accent sur la protection accrue de tous les appareils et dispositifs mobiles (clés USB, ordinateurs portables, etc.). À cette fin, les dépositaires doivent s'assurer que ces appareils sont protégés par un mot de passe en tout temps, changer les mots de passe régulièrement et veiller à ce que les renseignements soient chiffrés de sorte qu'il ne soit pas possible d'y accéder advenant la perte ou le vol de l'appareil. Il ne faut jamais laisser les appareils électroniques mobiles sans surveillance, et il faut les ranger dans un endroit physique dont l'accès est limité aux personnes dûment autorisées.

26. Les appareils électroniques servant au stockage de renseignements personnels sur la santé, tels que les ordinateurs portables, devront avoir un niveau supplémentaire de protection. Il faut user 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* :

> **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, 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;
> […]

27. La *Loi* prescrit non seulement l'utilisation de garanties, mais définit aussi une façon pragmatique de les instaurer en fonction de deux normes (décrites aux paragraphes 50[1] et 50[2]), à savoir :

a) le caractère raisonnable;
b) le caractère approprié en fonction du degré de sensibilité des données.

28. 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.

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

30. Encore une fois, ce sont les circonstances propres à chaque cas qui détermineront les mesures de sécurité raisonnables nécessaires pour protéger les renseignements personnels sur la santé. À titre d'exemple, un disque dur d'ordinateur renfermant le nom des médecins censés participer à une enquête sur la santé n'exigera pas les mêmes mesures de sécurité qu'un disque dur d'ordinateur qui renferme les dossiers médicaux des patients de ces mêmes médecins. Comme mentionné précédemment, ces exigences supplémentaires se veulent un moyen de faire prendre conscience à tous du degré d'attention accru dont il faut faire preuve lorsqu'il est question de protéger des renseignements personnels sur la santé en format électronique. La protection par mot de passe et le chiffrement des données stockées sur un ordinateur sont devenues la norme, et ces mesures doivent aussi être appliquées aux systèmes de réseau sans fil, aux clés USB et aux autres appareils électroniques mobiles tels que les ordinateurs portables.

31. On peut aussi faire appel à des observations fondées sur le gros bon sens pour établir d'autres mesures de sécurité raisonnables. 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 qui donne lieu aux plus grandes préoccupations en matière de sécurité.

Pourquoi l'ordinateur se situait-il dans un endroit accessible au public où il pouvait être volé?

32. La principale préoccupation exprimée par les personnes concernées dans le cadre de cette atteinte à la vie privée concernait l'emplacement de l'ordinateur portable, plus précisément pourquoi un appareil portatif contenant des renseignements personnels et confidentiels sur la santé de centaines de patients était une proie si facile pour le voleur. Les agents de sécurité patrouillent régulièrement dans le secteur où se trouve la clinique, mais l'ordinateur portable a tout de même échappé aux mesures de sécurité.

33. Selon les faits obtenus, la clinique (la pièce) où se trouvait l'ordinateur a été laissée déverrouillée et sans surveillance pendant une courte période à partir de 16 h 30 le vendredi soir. La porte a alors été laissée déverrouillée pour que le personnel de l'entretien ménager vienne y faire son tour, la porte ayant ensuite été fermée à clé une fois le travail terminé. Nous ignorons à quelle heure précisément le personnel de l'entretien ménager a terminé son travail le vendredi soir en question. Nous savons cependant, à la lumière des faits signalés par la sécurité, que la porte était verrouillée à 18 h. Nous rappelons aussi que d'autres personnes circulent dans le centre de traitement, où se situe la clinique, même après le départ des employés, qui laissent la porte de la clinique déverrouillée, c'est-à-dire entre 16 h 30 et 19 h. De plus, le lundi matin en question, si l'ordinateur portable n'avait pas été volé le vendredi soir précédent avant le verrouillage de la porte, il aurait été laissé sans surveillance dans une pièce dont la porte n'était pas verrouillée pendant environ une heure entre le moment où on a déverrouillé la porte, soit à 7 h 4, et celui où le premier employé de la clinique est arrivé, aux alentours de 8 h.

34. Les employés de l'hôpital croyaient avoir verrouillé l'ordinateur au câble, mais il s'avère que le dispositif de verrouillage, destiné à le relier en permanence à l'unité mobile (matériel diagnostique), avait été retiré.

35. Il est essentiel d'adopter des méthodes plus sécuritaires en vue d'assurer la protection de l'ordinateur portable à tout moment où la pièce est laissée déverrouillée et sans surveillance. Comme mesure de sécurité, il serait raisonnable qu'un membre du personnel de la clinique ou du centre de traitement vienne jeter un coup d'œil à la pièce déverrouillée pendant les périodes où elle est accessible au public, mais qu'elle demeure sans surveillance, étant donné la nécessité de protéger l'ordinateur portable servant à recueillir des données confidentielles. L'ordinateur devrait au moins être verrouillé de façon sécuritaire, comme il était censé l'être. Bien qu'il puisse avoir semblé moins important de vérifier le dispositif de verrouillage que de servir des patients, sans oublier qu'il fallait donner accès au personnel de

l'entretien ménager, la responsabilité de protéger les données sauvegardées dans l'ordinateur ne devait pas être négligée pour autant.

36. L'incident montre encore plus clairement qu'il est primordial de ne pas stocker les données de nature confidentielle sur l'unité de disque dur d'un ordinateur portable. Cette seule action est une cause directe de l'atteinte à la vie privée. FacilicorpNB et le Réseau de santé Vitalité ont établi des règles contraignant le personnel de ne pas stocker des données sur les patients (leurs renseignements personnels par exemple) sur l'unité de disque dur de l'ordinateur. Les employés doivent plutôt prendre les mesures nécessaires pour veiller à ce que les données soient sauvegardées directement sur le réseau sécurisé du système MediTech. De nos jours, la *Loi* confirme la nécessité de ces règles : il faut protéger les données en tout temps.

Pourquoi l'ordinateur n'était-il pas pourvu de plus de dispositifs de sécurité?

37. Cette question est simple, mais elle est lourde de sens à la lumière des faits qui ont provoqué l'incident. On utilisait l'ordinateur portable volé pour sauvegarder des renseignements médicaux hautement confidentiels qui appartiennent à plusieurs centaines de patients. Il s'agit d'un usage qui n'était pas autorisé, d'autant plus que, sans chiffrement, les données étaient tout à fait accessibles à des utilisateurs non autorisés, y compris le ou les voleurs.

38. Les centaines de patients ayant profité des services de la clinique ont, en échange, confié leurs renseignements confidentiels à ceux qui y travaillaient. Par conséquent, la clinique, l'hôpital et le Réseau de santé Vitalité avaient le devoir de protéger les renseignements sur la santé de ces patients et de le faire en tout temps selon un degré de sécurité élevé, en vertu du paragraphe 50(1) de la *Loi*. Malheureusement, les dépositaires susmentionnées n'ont pas dûment protégé cette information.

39. Dans le présent cas, l'ordinateur portable n'était pas protégé par un mot de passe et les données n'étaient pas chiffrées, comme le voulaient les règles. Les données étaient emmagasinées sur l'unité de disque dur plutôt que sur le réseau sécurisé MediTech. À l'occasion, certaines données recueillies étaient sauvegardées directement sur le bureau de l'ordinateur afin de pouvoir y accéder rapidement. On nous avait assuré que tous les ordinateurs, qu'ils soient portables ou de bureau, dont se servait le personnel du Réseau de santé Vitalité comportaient des dispositifs de protection conformes à ce degré de sécurité, notamment la protection par un mot de passe pour prévenir un accès non autorisé. Nous n'avons cependant obtenu aucune explication à savoir pourquoi l'ordinateur n'était pas doté d'un mot de passe pour le protéger.

40. De plus, dans la plupart des cliniques du Réseau de santé Vitalité, les renseignements personnels sur la santé recueillis sont sauvegardés dans le système MediTech, dont l'exploitation relève de FacilicorpNB. Pour accéder à ce système, il faut deux mots de passe avant de pouvoir accéder aux données. Encore une fois, dans l'affaire qui nous a été confiée, les données confidentielles ont été enregistrées de façon arbitraire sur l'unité de disque dur de l'ordinateur portable, ce qui signifie que les renseignements personnels sur la santé ne bénéficiaient pas de la protection voulue. Dans la pratique, cette façon de faire pourrait fort bien avoir permis aux patients d'être servis plus rapidement; cependant, elle s'accompagnait du risque d'une atteinte à la vie privée quant aux renseignements personnels sur la santé des patients.

41. À nos yeux, l'utilisation de mots de passe et la sauvegarde de données dans le système exploité par FacilicorpNB sont des mesures de sécurité adéquates pour la protection des renseignements personnels sur la santé des patients recueillis à l'hôpital, au centre de traitement et à la clinique. Pareille information n'aurait pas dû être stockée sur l'unité de disque dur de l'ordinateur portable; elle aurait pu avoir été perdue à jamais si on n'avait pas imprimé de rapports papier que l'on a versés aux dossiers des patients.

42. Étant donné la nature confidentielle des renseignements personnels sur la santé et le volume de données en cause pour les centaines de dossiers électroniques de patients sauvegardés sur l'ordinateur portable, nous estimons qu'il est raisonnable d'exiger une norme des plus élevées relative aux garanties de sécurité dans cette affaire. Malheureusement, nous avons constaté des lacunes en matière de sécurité des données, notamment :

- la pièce où se trouvait l'ordinateur portable a régulièrement été laissée sans surveillance pendant de courtes périodes, dans une clinique très fréquentée et dans un centre de traitement que l'on sait accessible au public;
- l'ordinateur portable n'était pas verrouillé en permanence au matériel diagnostique, comme le voulaient les règles;
- on effectuait la sauvegarde des renseignements hautement confidentiels sur la santé des patients sur l'unité de disque dur de l'ordinateur, ce qui constitue une pratique non autorisée;
- la pratique approuvée, soit de sauvegarder les données (et d'en faire une copie de secours) sur le réseau sécurisé MediTech, n'a pas été suivie;
- aucun mot de passe de protection n'a été utilisé sur l'ordinateur portable stockent les renseignements personnels hautement confidentiels sur la santé des patients;

- on a négligé de chiffrer les renseignements personnels hautement confidentiels sur la santé des patients qui avaient été emmagasinés sur l'ordinateur portable.

43. Pour ces raisons, nous estimons que les mesures de sécurité adoptées collectivement et utilisées dans l'Hôpital, le centre de traitement, la clinique et le Réseau de santé Vitalité au moment de l'atteinte à la vie privée n'étaient pas conformes à ce qu'exigent les normes imposées aux dépositaires en ce qui a trait à la protection des renseignements personnels sur la santé en vertu de la *Loi* et que les mesures en vigueur à ce moment précis n'étaient donc pas conformes à la *Loi*. Nous en venons donc à la conclusion que les dépositaires ne se sont pas acquittés de leur obligation légale de protéger les renseignements personnels sur la santé des patients de l'Hôpital.

Quelles mesures sont prises actuellement pour corriger cette atteinte et pour empêcher que des incidents semblables ne se produisent à l'avenir?

44. Cette atteinte à la vie privée a donné lieu à un examen des mesures de sécurité que le Réseau de santé Vitalité entreprend pour assurer la protection des renseignements personnels sur la santé qui sont placés ou stockés dans des dispositifs électroniques, conformément à l'obligation qu'il a de le faire en vertu du paragraphe 20(2) de *Loi* :

> 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.

45. On nous a également avisés que le Réseau de santé Vitalité a passé en revue sa politique concernant l'utilisation d'ordinateurs portables et a examiné s'il est de mise que la clinique utilise un ordinateur portable comme elle le fait. Il a été déterminé que l'ordinateur en question, qui est relié à la machine diagnostique rangée sur le chariot, constitue le meilleur équipement pour effectuer les épreuves sur les patients en raison de sa mobilité. Cela dit, même si les unités mobiles comme celles-ci seront encore utilisées, le Réseau de santé Vitalité n'autorisera plus son personnel à utiliser les ordinateurs portables pour enregistrer les renseignements personnels sur la santé des patients.

46. De plus, comme conséquence directe de cette atteinte à la vie privée, le Réseau de santé Vitalité a recommandé à toutes les cliniques externes dont il est responsable de procéder à une évaluation des mesures de sécurité actuellement en place pour ce qui est de la protection des ordinateurs qui se trouvent dans des salles d'examen semblables pour veiller à ce que les

garanties de sécurité soient conformes à la *Loi*, dans le but particulier d'éviter des atteintes à la vie privée similaires à l'avenir.

47. Nous savons que de nouvelles mesures de sécurité ont été mises en œuvre, dont les suivantes, pour éviter d'autres atteintes à la vie privée semblables :

- le personnel ne peut utiliser le nouvel ordinateur portable acheté expressément pour la clinique qu'après avoir saisi un nom d'utilisateur et un mot de passe;
- on a fourni un nom d'utilisateur et un mot de passe uniquement aux professionnels de la santé qui doivent se servir de l'ordinateur pour faire subir les épreuves urodynamiques effectuées à la clinique;
- la carte d'accès qui permet à un employé d'utiliser l'ordinateur portable est maintenant entreposée en lieu sûr;
- le nouvel ordinateur portable est maintenant relié au matériel diagnostique mobile sur le chariot au moyen d'un câble de métal, ce qui rehausse le niveau de protection contre le vol; de plus, toute tentative de retrait l'ordinateur de façon illégale endommagera l'écran; il sera donc très difficile de le retirer ou de le voler;
- les renseignements recueillis sur les patients sont maintenant sauvegardés directement sur le réseau d'information sécurisé MediTech, qui est géré par FacilicorpNB, plutôt que sur l'unité de disque dur de l'ordinateur portable;
- FacilicorpNB préparera une copie de secours sécurisée des données des patients pour la clinique.

48. Nous savons que le personnel de l'entretien ménager du centre de traitement et de la clinique a accès aux pièces et aux bureaux où les renseignements personnels sur la santé des patients sont conservés, bien que les employés de ce service ne soient pas assujettis à la *Loi*. Le Réseau de santé Vitalité nous a assurés que le personnel de l'entretien ménager reçoit une formation qui met l'accent sur l'importance, dans un milieu hospitalier, de protéger le matériel qui contient des données confidentielles et qu'il s'agit de la même formation sur la protection des renseignements que celle que suivent les employés œuvrant dans le secteur des soins de santé.

49. Enfin, la Commissaire sera tenue au courant des différentes mesures entreprises en vue de veiller à ce que toutes les personnes concernées par cette affaire suivent les garanties de sécurité stipulées par la *Loi*. Cette mesure s'inscrit également dans l'évaluation qu'a faite le Réseau de santé Vitalité.

La perte de renseignements personnels peut-elle mener à un vol d'identité et avoir une incidence sur les antécédents financiers de la personne concernée?

50. Une autre grande préoccupation qui a été portée à notre attention concernait le risque de vol d'identité que constituait la perte des renseignements personnels sur la santé. Au nombre des renseignements perdus dans la présente affaire, mentionnons le nom des patients et d'autres renseignements d'ordre médical. Il convient toutefois de signaler que les données perdues ne comprennent pas le numéro d'assurance-maladie des patients, leur numéro de téléphone ni leur adresse.

51. Bien qu'il soit impossible d'établir avec un quelconque degré de certitude le risque encouru par 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. Il ne faut donc pas prendre cette perte de renseignements à la légère. Pour chaque renseignement d'identification supplémentaire dont l'intégrité est compromise, le risque de fraude et de vol d'identité augmente. Dans cette atteinte à la vie privée, nous pourrions estimer que le risque est moindre puisque les renseignements personnels perdus ne contenaient pas beaucoup de renseignements d'identification.

52. 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. Les enfants ou les personnes âgées de moins de 19 ans ne peuvent établir d'antécédents financiers ou de crédit parce qu'ils n'ont pas atteint l'âge voulu. La surveillance de leurs antécédents de crédit ne ferait donc pas partie des mesures de précaution découlant de la perte de leurs renseignements personnels.

53. 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 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 carte 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 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;
- 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).

Commentaires finaux de la Commissaire

54. Nos discussions avec les responsables du Réseau de santé Vitalité et du Centre hospitalier universitaire D^{r} Georges L. Dumont dans cette affaire d'atteinte à la vie privée ont permis de réunir tous les faits décrits dans le présent rapport. Des mesures ont immédiatement été prises afin de rassembler les données préliminaires; le Commissariat et les personnes touchées ont été avisés dans un délai raisonnable.

55. L'atteinte à la vie privée était de taille, en ce sens qu'elle touchait un grand nombre de patients d'une clinique, où toutes les données recueillies étaient stockées dans un seul ordinateur portable qui n'était pas doté de mesures de sécurité adéquates pour protéger les renseignements confidentiels. Ces détails ont mis en évidence, pour toutes les personnes concernées, à quel point il était facile de violer la vie privée d'une personne en l'absence de garanties de sécurité.

56. Nous avons aussi, dans le cadre de notre enquête, rencontré des responsables de FacilicorpNB et en avons appris davantage sur les responsabilités que cette dernière partage avec le Réseau de santé Vitalité pour ce qui est de l'installation et de l'utilisation du matériel utilisé pour la collecte, l'utilisation et le stockage des renseignements médicaux des patients ainsi que sur la responsabilité globale qui en découle. On nous a assurés que les deux organisations sont conscientes des obligations respectives qui leur incombent et de la nécessité de rester vigilants quant à l'adoption et au respect des politiques associées à la collecte et au stockage des renseignements personnels sur la santé, au degré de sécurité qui doit caractériser l'utilisation des dispositifs électroniques portables, notamment les

ordinateurs, et à la mise en application générale des mesures de sécurité appropriées en vue de protéger les renseignements des patients en tout temps.

57. Des mesures de précaution améliorées ont déjà été mises en place pour rehausser la protection des renseignements personnels sur la santé obtenus auprès des patients lorsque l'on doit avoir recours à une unité mobile spécialisée, comme celle utilisée dans cette affaire. Les données confidentielles recueillies de cette façon ne seront plus stockées directement sur l'unité de disque dur de l'ordinateur, mais plutôt sur le réseau sécurisé géré par FacilicorpNB. Nous avons bon espoir que les mesures correctives appliquées permettront d'assurer une meilleure protection des renseignements des patients à l'avenir.

58. Pour conclure, il est important de mentionner que 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 leur information privée sera utilisée 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.

RECOMMANDATIONS

59. À la lumière des conclusions exposées ci-dessus, la Commissaire convient des mesures entreprises par le Réseau de santé Vitalité dans le but d'éviter de futurs incidents d'atteinte à la vie privée semblables, à savoir :

- Le Réseau de santé Vitalité doit évaluer ses mesures de sécurité en vue d'assurer la protection des renseignements personnels sur la santé qui sont placés ou stockés dans des dispositifs électroniques, conformément aux obligations stipulées dans la *Loi*.
- Le Réseau de santé Vitalité doit passer en revue sa politique concernant l'utilisation d'ordinateurs portables et examiner s'il est de mise que la clinique utilise un ordinateur portable comme elle le fait.
- Toutes les cliniques externes qui relèvent du Réseau de santé Vitalité doivent examiner les mesures de sécurité actuelles pour ce qui est de la protection des ordinateurs qui se trouvent dans des salles d'examen semblables dans le but de veiller à ce que les garanties de sécurité soient conformes à la *Loi*.
- Le personnel ne peut utiliser le nouvel ordinateur portable acheté expressément pour la clinique qu'après avoir saisi un nom d'utilisateur et un mot de passe.

- Il faut attribuer un nom d'utilisateur et un mot de passe uniquement aux professionnels de la santé qui doivent se servir de l'ordinateur pour faire subir les épreuves urodynamiques effectuées à la clinique.
- La carte d'accès qui permet à un employé d'utiliser l'ordinateur portable doit être entreposée en lieu sûr.
- Le nouvel ordinateur portable doit être relié au matériel diagnostique mobile sur le chariot au moyen d'un câble de métal, comme il aurait dû l'être, pour qu'il soit très difficile de le retirer ou de le voler.
- Les renseignements recueillis sur les patients doivent être sauvegardés directement sur le réseau d'information sécurisé MediTech, qui est géré par FacilicorpNB, plutôt que sur l'unité de disque dur de l'ordinateur portable.
- Le Réseau de santé Vitalité doit s'assurer que la clinique prend les dispositions nécessaires auprès de FacilicorpNB pour obtenir une copie de secours des renseignements recueillis sur les patients.

60. Le Commissariat fera un suivi auprès du Réseau de santé Vitalité en décembre 2012 pour veiller à la mise en œuvre de ces mesures.

Émis à Fredericton (Nouveau-Brunswick), le 13 septembre 2012.

_____

Anne E. Bertrand, c.r.
Commissaire