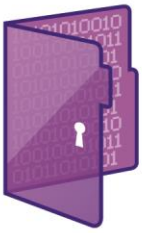
Office of the Access to Information and Privacy Commissioner
New Brunswick



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 vie privée: 2012-743-H-236

Affaires: 2012-816-H-255, 2012-818-H-257, 2012-819-H-258, 2012-821-H-260, 2012-823-H-261, 2012-826-H-262, 2012-829-H-264, 2012-831-H-265, 2012-873-H-273

Date: Le 5 juin 2013

Enquête menée par la Commissaire

Atteintes à la vie privée – accès non autorisés

Introduction

1. Ce présent rapport des conclusions de l'enquête de la Commissaire est émis suite aux dépôts de plusieurs plaintes auprès du Commissariat à l'accès à l'information et à la protection de la vie privée. Les plaignants prétendent que l'Hôpital et Centre de santé communautaire de Lamèque (ci-après «l'Hôpital et Centre de santé communautaire») et le Réseau de santé Vitalité ont omis de protéger de façon sécuritaire les renseignements personnels sur la santé les concernant contrairement aux exigences de la *Loi sur l'accès et la protection de renseignements personnels sur la santé* (ci-après, la « *Loi* »).

2. Dans le présent rapport des conclusions, nous discutons des constatations auxquelles nous sommes parvenus à l'issue de l'enquête que nous avons entreprise parallèlement à celle du Réseau de santé Vitalité dans le but d'émettre des recommandations relativement à cette affaire.

3. D'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 tenu 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.

4. Dans le présent cas, l'Hôpital et Centre de santé communautaire ainsi que le Réseau de santé Vitalité sont tous deux des dépositaires, soit des organismes œuvrant dans le système des soins de santé, et à qui plus particulièrement est décernée la responsabilité de protéger les renseignements personnels sur la santé des patients dans cette affaire. À ce dire, ces deux dépositaires doivent répondre aux allégations dans les présents cas d'atteinte à la vie privée.

Contexte

5. Les cas d'atteinte à la vie privée seraient survenus lorsqu'un des employés de l'Hôpital et Centre de santé communautaire a accédé, de façon non autorisé, les dossiers électroniques qui contenaient des renseignements personnels sur la santé concernant plus de 150 patients étant des collègues de travail, des membres de sa famille, et d'autres gens de sa communauté. Les renseignements personnels sur la santé en jeux comprenaient :
    - les noms des patients,
    - leurs données démographiques,
    - les dates de leurs visites à l'Hôpital et Centre de santé communautaire, et
    - les raisons de ces visites.

6. Il y a aussi des faits portant à croire que certains de ces renseignements personnels sur la santé auraient été communiqués par l'employé en question en violation de la *Loi*.

7. Avant de débuter avec nos constatations relativement à ces cas d'atteinte, nous croyons qu'il est de mise de décrire qui sont les dépositaires dans cette affaire, ainsi que de leurs responsabilités et enfin, par quels moyens les atteintes se sont produites.

8. Le Réseau de santé Vitalité est une organisation francophone qui gère un ensemble d'établissements et de programmes francophones et bilingues. Les établissements et les programmes ont une identité propre qui se reflète par un lien solide avec la communauté. Le Réseau de santé Vitalité a son siège social à Bathurst et offre des soins et des services de santé à près de 250 000 personnes. Son équipe est formée de plus de 7 600 employés, de près de 470 médecins, dont 227 spécialistes, et de 1 200 bénévoles. Le Réseau de santé Vitalité compte plusieurs hôpitaux, établissements communautaires, centres de santé, deux centres de santé communautaires, sans en dire pour des centres de santé mentale, bureaux principaux de santé publique, et bien d'autres.

9. Sous le regroupement du Réseau de santé Vitalité, l'Hôpital et Centre de santé communautaire est un établissement singulier, conçu pour abriter non seulement certains services cliniques que l'on retrouve dans un centre hospitalier, mais aussi ceux qui répondent à plusieurs besoins de santé d'une communauté.

10. Entres autres, l'Hôpital et Centre de santé communautaire offre des services interdisciplinaires, soit ceux que l'on retrouve dans une clinique sans rendez-vous, un bureau de médecins, pour des sessions de physiothérapie, et ainsi de suite. Ces services

sont regroupés sous un même toit : les services d'accueil et d'admission, les services des cliniques de conditions chroniques, thérapeutiques, l'unité de médecine familiale et l'unité de médecine, le service d'imagerie médicale, le laboratoire, le service alimentaire, et bien d'autres.

11. L'Hôpital et Centre de santé communautaire est donc une importante composante de la communauté et il jouit de très bons rapports avec les citoyens et citoyennes qu'il dessert. Son succès lui permettant d'offrir une telle multitude de services en soins de santé n'est possible, on nous avise et comme nous l'avons observé, qu'avec un personnel attentif et compétent.

12. Il va donc sans dire qu'à la découverte des présents cas d'atteinte à la vie privée des patients, le bureau de la directrice principale sur la protection de la vie privée du Réseau de santé Vitalité et l'Hôpital et Centre de santé communautaire et son personnel sont demeurés stupéfaits. Comment pouvait-il qu'une pareille chose puisse avoir eu lieu dans un établissement si adroit et qui insiste sur la mission principale de protéger la vie privée de ses patients.

13. En effet, les deux dépositaires reconnaissent solidement et ne reculent pas devant leur obligation statutaire de protéger les renseignements personnels sur la santé des patients dont ils desservent en tout temps conformément aux dispositions connexes de la *Loi*. De multiples mesures sécuritaires prescrites par la *Loi* les exigent d'adopter des pratiques fondées sur les normes relatives à la sécurité de la technologie de l'information reconnues dans le monde et des pratiques qui comportent des garanties administratives pour protéger cette information en format électronique (l'article 50).

14. Donc, il en revient au Réseau de santé Vitalité et à l'Hôpital et Centre de santé communautaire de monter un recueil des dossiers électroniques des patients dans des systèmes informatisés de haute qualité et sécuritaires, et vu la facilité pour accéder à ces réseaux électroniques, ils doivent davantage s'assurer que leur personnel ne s'en servent que lorsqu'ils sont en droit de le faire.

15. C'est pourquoi nous nous sommes penchées sur la question à savoir quelles étaient les circonstances qui ont permis à un employé de perpétrer de telles violations de la *Loi*. Ni la direction ni le personnel de l'Hôpital et Centre de santé communautaire n'a soupçonné que l'employé en question accédait aux dossiers électroniques des patients (et le personnel compte parmi la liste des patients de cet établissement) sans en avoir la permission.

16. Nous avons enquêté cette étrange conduite en examinant les tâches assignées à cet employé à l'époque, son niveau d'autorisation pour accéder aux fichiers électroniques des patients, la surveillance de son travail, et les mesures de sécurité au sein de cet établissement.

L'employé en question

17. Dans le présent cas, l'employé responsable des atteintes à la vie privée occupait deux postes à l'Hôpital et Centre de santé communautaire à titre d'employé occasionnel. Cet employé gagnait un seul salaire mais répondait à la direction de deux gestionnaires : pour remplir les tâches de commis aux admissions, à l'inscription et à l'établissement des calendriers au service de réception des patients, et pour effectuer les tâches en tant que soutien administratif auprès de l'unité de médecine familiale (étant un bureau de médecins).

18. À son poste de commis aux admissions, cet employé devait accomplir les diverses tâches de traitement des admissions, soit tout ce qui est requis pour faire l'enregistrement des patients dans un hôpital. Cet employé s'occupait aussi des transferts et congés des patients, y inclut les patients de la clinique sans rendez-vous. Pour accomplir ces tâches, l'employé avait à imprimer et préparer les dossiers, bracelets, cartes d'hôpital et les formulaires par types d'admissions, de manœuvrer dans le système de rendez-vous central retrouvé au réseau informatisé Meditech.

19. La surveillance de cet employé lorsque dans son poste de commis aux admissions était réalisée par un gestionnaire. Selon notre enquête sur les faits, ce gestionnaire n'a jamais décelé aucun indice lui portant à croire ou à pressentir que l'employé en question accédait aux dossiers électroniques des patients sans en avoir la permission. En effet, le gestionnaire rapporte que l'employé en question donnait un bon rendement au travail et s'entendait bien avec le personnel.

20. Dans son poste de soutien administratif à l'unité de médecine familiale, cet employé remplissait les diverses tâches requises d'un bureau de médecins. Toutefois, une tâche particulière à ce poste lui exigeait de faire la numérisation des notes et des rapports provenant de l'extérieur de l'unité pour enfin les répertorier dans les dossiers électroniques des patients de cette unité.

21. Encore une fois, on nous a avisés que la surveillance de cet employé n'a jamais provoqué de la part de la gestion une crainte que l'employé accédait aux dossiers électroniques des patients sans en avoir la permission. Tout comme dans son poste de commis aux admissions, l'employé en question donnait un bon rendement et était bien perçu par le personnel de l'unité de médecine familiale.

Deux systèmes informatisés

22. Lors de notre enquête sur la conduite illicite de l'employé en question dans cette affaire, nous nous sommes dirigés sur l'examen des systèmes informatisés utilisés par le personnel de cet établissement. En effet, le personnel de l'Hôpital et Centre de santé communautaire utilise deux systèmes informatisés, soit Meditech et un autre ayant connu par son nom de logiciel Purkinje. Le système Meditech permet de passer à l'enregistrement des patients en y inscrivant des données démographiques, à la gestion des rendez-vous des patients, ainsi qu'à toutes les autres fonctions reliées à la facturation. Le système informatisé connu sous le nom de Purkinje est utilisé, en autres, par l'unité de médecine familiale, soit le personnel de soutien aux médecins. Dans ce système, l'on peut transcrire et y repérer les notes des médecins suivant les visites des patients. L'Hôpital et Centre de santé communautaire compte également des médecins, mais dans le cas des patients hospitalisés, le personnel se sert du réseau informatisé Meditech.

23. Selon les modules utilisés du système informatisé Meditech par l'Hôpital et Centre de santé communautaire, les employés ne peuvent pas y faire la numérisation des notes ou des rapports des médecins. Donc, l'on peut décerner assez facilement selon l'apparence du document s'il fut créé en se servant du système Meditech ou bien à l'aide du logiciel Purkinje dans cet établissement.

24. C'est pourquoi qu'en tant que soutien administratif à l'unité de médecine familiale, l'employé en question effectuait ses tâches à l'aide du système informatisé Purkinje, y compris pour enregistrer les patients à leurs rendez-vous, pour faire la numérisation des rapports médicaux de ces patients, et toutes autres tâches connexes à ce poste nécessitant l'accès aux dossiers électroniques des patients.

Découverte des atteintes à la vie privée

25. Au début de son relais de travail le matin du 29 février 2012 (au lendemain du relais de travail du soir du 28 février), un employé du service d'accueil, admissions et centre de rendez-vous découvre un document numérisé sur l'imprimante. À première vue,

l'employé constate que le document contient des renseignements personnels sur la santé d'un patient et juge curieux cette découverte car ce n'est pas un document créé dans le système informatisé Meditech par les employés au service d'admissions. L'employé a alors averti le superviseur du service d'admissions de la découverte de ce document.

26. De sa part, le superviseur du service d'admissions s'informe auprès des superviseurs des cliniques de l'Hôpital et Centre de santé communautaire qui utilisent des documents numérisés pour accomplir leur travail dans le but de savoir si un membre de leur personnel aurait imprimé le document retrouvé sur l'imprimante à l'accueil par erreur.

27. Il est à noter que les imprimantes sont regroupées dans un réseau de plusieurs imprimantes pour desservir tout l'établissement. Puisque la protection de la confidentialité des renseignements appartenant aux patients prédomine dans cet établissement, lorsqu'un employé fait une erreur en imprimant un document dans un bureau qui n'est pas sous sa surveillance mais dans un autre endroit au sein de l'Hôpital et Centre de santé communautaire, un rapport d'incident doit être rempli pour expliquer pourquoi une telle erreur s'est produite. Dans ce cas-ci, les superviseurs des cliniques lui ont avisé que ce n'était pas le cas.

28. Ne pouvant pas décerner l'origine du document retrouvé dans l'imprimante de son secteur, le superviseur du service d'admissions a donc communiqué avec le bureau de soutien en matière de technologies de l'information afin de retracer qui avait fait la commande pour imprimer le document (donc, de quel ordinateur et quel employé qui s'en était servi pendant le relais de travail du 28 février).

29. Le premier audit effectué est limité au relais de travail du 28 février 2012. On y découvre que l'employé en question s'était servi du niveau d'autorisation d'accès accordée à son embauche dans le cadre de son travail à l'unité de médecine familiale pour accéder au dossier électronique d'où provenait le document numérisé. Il n'y a pas d'indication que l'employé avait la permission d'accéder à ce dossier électronique. Plus inquiétant, l'audit mène à la découverte que l'employé en question avait accédé non seulement au dossier qui n'était pas relié à son travail comme commis aux admissions, mais aussi à 33 autres dossiers qui provenaient du système informatisé Purkinje sans que cet employé possède la permission de le faire au moment où les accès avaient été effectués.

30. À la découverte de ces faits, le superviseur du service d'admissions s'interroge à savoir si l'employé en question accomplissait du travail de rattrapage normalement faisant partie de son poste à l'unité de médecine familiale (la numérisation des notes et rapports des

médecins en se servant du système Purkinje). En d'autres mots, est-ce que durant son relai de travail de soir la veille, cet employé effectuait des tâches pour l'unité de médecine familiale lorsque cet employé était en fonction dans son second poste au service d'admissions? Le gestionnaire de l'unité de médecine familiale lui confirme que ce n'est pas le cas.

31. Ces faits ont soulevés des doutes chez les dirigeants de l'Hôpital et Centre de santé communautaire sur la légitimité de ces accès par cet employé. L'établissement a donc communiqué avec le bureau de la directrice principale de l'information et de la protection des renseignements personnels du Réseau de santé Vitalité le 1er mars 2012 et l'on décide d'effectuer un audit de six mois des accès effectués par cet employé afin de déterminer quel en était le cas. De plus, les accès électroniques de cet employé lui sont retirés immédiatement et l'employé est suspendu de ses fonctions pendant l'enquête. Cet audit révèle que l'employé en question avait également fait des accès non-autorisés pendant cette période.

32. Le gestionnaire rencontre cet employé le 2 mars afin de savoir pourquoi le document numérisé avait été imprimé lors de son relais de travail au service d'admissions. L'employé ne donne pas de réponse satisfaisante et nie avoir commis des accès non-autorisés. Face aux résultats du premier audit (du 28 février) qui lui démontrent que des accès non-autorisés avaient été effectués, l'employé modifie son témoignage et cette réaction de la part de l'employé éveille des soupçons chez le gestionnaire.

33. Donc, on s'engage de mener un troisième audit sans tarder, soit le 13 mars, pour soutirer l'état des accès effectués par cet employé à partir de la date de son embauche (une période de temps approximative de trois ans). Ce troisième examen révèle que l'employé en question avait accédé plus de 150 dossiers électroniques contenants des renseignements personnels sur la santé de plusieurs patients, y compris les dossiers des collègues de travail à titre de patients et ceux des membres de sa famille et de ses amis lorsque l'employé n'était guère en droit de le faire.

Processus de notification de l'atteinte

34. Conformément à la *Loi*, un dépositaire, tel que l'Hôpital et Centre de santé communautaire ou le Réseau de santé Vitalité, qui découvre qu'une atteinte à la vie privée a eu lieu est tenu d'en aviser le plus tôt possible la Commissaire. Le dépositaire doit aussi notifier toutes les personnes concernées que la confidentialité de leurs

renseignements personnels sur la santé a été compromise. Ce processus de notification est prévu à l'alinéa 49(1)*c)* de la *Loi* et est obligatoire dans la plupart des cas.

35. 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. La *Loi* et ses règlements ordonnent au dépositaire de fournir, dans un tel avis, les détails suivants :
    a) Le nom du dépositaire;
    b) 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;
    c) Une description de la nature de la violation de la vie privée;
    d) La date et le lieu de la violation de la vie privée; et
    e) La date à laquelle le dépositaire a pris connaissance de la violation de la vie privée.

36. De plus, les personnes concernées doivent être avisées de leur droit de déposer une plainte auprès de la Commissaire. Le dépositaire ne peut renoncer à son obligation d'émettre un avis que dans des cas spécifiques et limités, qui n'existaient pas dans les présents incidents.

37. Toutefois, dans le présent contexte du processus de notification, des questions furent soulevées par le Réseau de santé Vitalité à savoir si, dans certains cas, l'on puisse dispenser d'effectuer une notification. À titre d'exemples, devrait-on notifier si:
    - l'avis, de par son contenu, aurait l'effet d'exposer le nom du membre du personnel du dépositaire, ou même, pourrait identifier ceux et celles qui ont aussi été les victimes des atteintes?
    - dans le cas des atteintes produites dans une petite communauté où le dépositaire et son personnel et les personnes concernées se connaissent tous, l'avis aux membres de la communauté pourrait exposer le nom de l'employé responsable, ou encore permettre à certains de facilement déceler qui sont les autres victimes touchées par les atteintes?
    - cela risquerait d'exposer l'employé responsable de l'atteinte à la communauté et donc qui pourrait lui attirer des ennuis?

38. À notre avis, ce sont des inquiétudes valables mais non celles qui puissent mener un dépositaire à écarter sa responsabilité statutaire de notifier tous ceux et celles qui ont été touchés par une atteinte à la vie privée. L'objet principal de la *Loi* est de protéger la vie privée de l'individu à qui appartiennent les renseignements personnels sur la santé

lorsque ceux-ci sont confiés à un dépositaire. La *Loi* oblige aussi le dépositaire d'être transparent dans ses pratiques relatives au traitement des renseignements personnels sur la santé qui lui ont été confiés et l'oblige d'assurer son observation en tout temps. De plus, le dépositaire est responsable pour les gestes commis par ses employés relatifs aux renseignements personnels sur la santé qui lui ont été confiés, et les personnes atteintes d'une violation de la vie privée ont le droit de savoir que leurs renseignements personnels sur la santé ont été compromis.

39. La *Loi* n'est pas conçue pour dissimuler la conduite du dépositaire (ou de son personnel) qui l'a mené à manquer à son obligation légale, ni pour cacher son identité dans des cas d'atteinte à la vie privée. Au contraire, c'est pourquoi le processus de notification sous la *Loi* exige que l'on nomme le dépositaire en question. Tout individu victime d'une atteinte à la vie privée a le droit de se plaindre auprès de la Commissaire et le dépositaire ne pourra pas éviter de répondre aux questions qui en découleront, y compris d'expliquer comment la violation s'est produite et qui en est responsable.

40. Nous reconnaissons que le processus de notification est sûrement ardu dans la plupart des cas, mais nous sommes convaincus que la notification entraînera des effets bénéfiques pour tous:
    - de responsabiliser le dépositaire envers ces obligations statutaires;
    - de rassurer l'individu qui en est victime qu'une telle conduite ne se répétera pas au futur; et,
    - d'inciter le dépositaire à restaurer la confiance de l'individu sûrement ébranlée en raison de la violation de sa vie privée.

Notification dans les présent cas

41. Nous soulignons le fait que le processus de notification dans les présents cas a été mené par le Réseau de santé Vitalité. Lorsque les multiples cas d'accès non autorisé ont été découverts, le Réseau de santé Vitalité a signalé ces incidents d'atteinte à la vie privée à la Commissaire le 8 mars 2012. Il va sans dire que le Réseau de santé Vitalité ainsi que l'Hôpital et Centre de santé communautaire voulaient notifier sans tarder les gens de la communauté de ce qu'ils avaient découvert.

42. Plus imminent pour les deux dépositaires, on voulait rassurer la communauté qu'une telle conduite de la part des employés était une rareté, qu'un telle conduite ne serait tolérée, et qu'une telle conduite ne reflétait aucunement à quel point l'établissement et

tout le personnel prenaient à cœur la protection de leurs renseignements personnels sur la santé.

43. Vu ses obligations sous la *Loi*, rien dans les présent cas n'empêchait le Réseau de santé Vitalité de notifier les personnes touchées par l'accès non autorisé à leur dossier médical :
    - de la raison pour laquelle un tel incident s'était produit; et
    - de par sa nature et ses explications, l'avis pourrait conduire à l'identification d'autres personnes concernées ou encore, d'exposer l'identité de l'employé responsable.

44. Le Réseau de santé Vitalité entreprit la notification aux personnes concernées par envois de lettres en avril 2012. Chaque lettre de notification informait de l'atteinte à la vie privée par l'accès non autorisé aux renseignements personnels sur la santé, et ce, par un employé de l'Hôpital et Centre de santé communautaire. De plus, l'avis informait ces individus de leur droit de déposer une plainte auprès de la Commissaire relativement à cette atteinte.

45. Sur les centaines de personnes avisées, plusieurs ont fait appel directement à l'Hôpital et Centre de santé communautaire pour en savoir plus long et le personnel devait faire face à plusieurs interrogations sur cet incident. Ces personnes ont été référées à la directrice principale de la protection de la vie privée du Réseau de santé Vitalité pour recevoir ces explications et plus de 50 d'entre eux ont communiqué avec ce bureau.

46. Plusieurs des personnes victimes de ces atteintes ont communiqué avec la directrice principale de la protection de la vie privée du Réseau de santé Vitalité pour connaître l'identité de l'employé responsable. Conformément à la *Loi* et à nos conseils sur cette question que nous avons partagés avec le Réseau de santé Vitalité, l'identité de l'employé en question n'a été donnée qu'aux personnes concernées.

47. Environ 30 de ces personnes ont demandé à l'Hôpital et Centre de santé communautaire de leur fournir une copie de leurs renseignements personnels sur la santé que l'employé en question avait vu sans leur consentement.

48. Plusieurs de ces personnes ont également communiqué avec nous afin de nous faire part de leurs préoccupations et de nous demander des renseignements; neuf parmi ces gens nous ont transmis une plainte en vertu de la *Loi,* et celles-ci sont résumées par leurs

questions ci-dessous, à savoir :

- l'identité de l'employé responsable pour avoir commis cette violation;
- la raison et la façon que l'atteinte s'est produite;
- si l'employé en question est toujours à l'emploi du Réseau de santé Vitalité; et,
- si l'atteinte à leur vie privée peut mener à un vol d'identité.

Identité de la personne qui a causé l'atteinte

49. Manquer à la charge de protéger la vie privée d'un individu ne constitue pas une infraction. Toutefois, l'acte de recueillir, d'utiliser ou de communiquer des renseignements personnels sur la santé en violation délibérée de la *Loi* constitue une infraction en vertu de l'article 76.

50. Si l'employé d'un dépositaire accède et communique volontairement des renseignements personnels sur la santé lorsque l'employé n'était pas autorisé de le faire, cette conduite constitue une infraction en vertu du paragraphe 76(2). Une infraction est punissable en vertu de la Partie II de la *Loi sur la procédure applicable aux infractions provinciale*s et les procédures relatives à une infraction sont lancées par le dépôt d'une dénonciation auprès d'un juge de la cour provinciale.

51. Ayant débattu la question du devoir du dépositaire de notifier des cas d'atteinte à la vie privée, même s'il s'agit de violation de la vie privée de plusieurs membres d'une petite communauté, nous soulignons le fait que la protection de l'identité de l'employé responsable de l'atteinte n'est pas une considération pertinente dans la décision du dépositaire d'émettre ou non un avis aux individus concernés par l'atteinte à la vie privée. Non plus peut-on empêcher d'ainsi en informer les individus concernés qui en font la demande auprès du dépositaire.

52. Nous ne prescrivons pas d'annoncer au public le nom de l'employé responsable d'une atteinte à la vie privée. Cependant, il n'y a rien dans la *Loi* qui prévient de notifier l'individu atteint par une telle violation du nom de l'employé lorsque l'individu en fait la demande.

Comment l'employé a commis ces atteintes et pourquoi?

Autorisation d'accès et permission de s'en servir

53. Afin de bien saisir la façon dont l'employé à perpétré les multiples cas de violation de la vie privée, nous jugeons bon d'expliquer le fonctionnement des systèmes informatisés utilisés à l'Hôpital et Centre de santé communautaire.

54. Les renseignements personnels sur la santé des patients sont répertoriés dans des documents électroniques créés dans les systèmes informatisés Meditech et Purkinje. Les données confidentielles recueillies par le personnel sont protégées sur la notion magistrale de maintenir la confidentialité des renseignements personnels sur la santé en tout temps.

55. Le Réseau de santé Vitalité et la directrice de l'Hôpital et Centre de santé communautaire nous a informé qu'ils prennent à cœur l'importance de la confidentialité dans leur milieu de travail. La notion de confidentialité prend naissance à l'entrevue des candidats pour un poste dans l'établissement. Les candidats sont jugés sur leurs réactions et réponses de mises en situation axées sur l'importance de maintenir la confidentialité. Cette confidentialité engendre la vie privée des patients, des collègues de travail et de l'établissement.

56. À l'embauche d'un nouvel employé, ce dernier participe à une orientation générale qui comprend une session sur la sensibilisation au sujet de la confidentialité. Cette session est obligatoire. Par ailleurs, chaque employé est tenu de signer le formulaire de reconnaissance de leur obligation envers l'importance de la confidentialité, et cet acte est répété à chaque évaluation annuelle sur le rendement de l'employé.

57. Avant de donner l'autorisation pour accéder aux données qui contient les renseignements personnels sur la santé des patients répertoriés sur les systèmes Meditech et Purkinje, le gestionnaire doit en premier préciser, et ce à l'embauche, le niveau d'autorisation que sera accordé le nouvel employé. C'est-à-dire, on passera à déterminer le niveau d'accès qui lui est nécessaire pour permettre à ce nouvel employé d'accomplir les tâches de son poste.

58. Le niveau d'accès est accordé en fonction de mots de passe. Les mots de passe sont décernés selon les consignes données établies par le gestionnaire. Le Réseau de santé Vitalité avise FacilicorpNB du nom du nouvel employé ainsi que de son niveau

d'autorisation d'accès aux systèmes et obtient les mots de passe qui ont été créés pour le nouvel employé. Facilicorp NB est un organisme public qui offre des services de soutien en matière de technologies de l'information au Réseau de santé Vitalité, parmi d'autres dans le système de santé de la province. Quoique Facilicorp NB effectue l'installation et le maintien de tout le matériel informatique dans les établissements du Réseau de santé Vitalité, y compris le réseau sécurisé et les systèmes informatisés, il en revient aux établissements mêmes de donner les directives à leur personnel pour se servir de ces outils de travail lorsqu'il traite des données, soit les renseignements personnels sur la santé de leurs clients ou patients.

59. Enfin, pour accéder au système informatisé Meditech ou celui de Purkinje, un employé requiert son numéro d'utilisateur (qu'il reçoit lors de son embauche) et deux mots de passe. Le premier mot de passe accorder permet à l'employé d'accéder au réseau sécurisé du Réseau de santé Vitalité, soit le réseau sécurisé sous la gérance de FacilicorpNB. Un deuxième mot de passe est assigné au nouvel employé pour lui permettre d'accéder au système informatisé Meditech ou celui de Purkinje. Dans le cas où l'employé a des tâches qui lui nécessite de travailler dans les deux systèmes informatisés, l'employé se sert du pareil deuxième mot de passe pour accéder à l'un ou l'autre des systèmes informatisés.

60. Donc, le nouvel employé de l'Hôpital et Centre de santé communautaire reçoit une autorisation pour accéder au système sécurisé du Réseau de santé Vitalité, en plus d'un deuxième mot de passe pour accéder au système informatique Meditech et/ou celui de Purkinje. Toutefois, ce sont les tâches du poste (ou des postes) de l'employé qui gouverneront à quel moment cet employé pourra se servir de cette autorisation, c'est-à-dire, à quel moment dans son travail l'employé aura la permission de se servir de son autorisation d'accéder aux dossiers des patients dans les systèmes informatisés Meditech ou Purkinje.

61. Un employé d'une clinique médicale qui reçoit à son embauche l'autorisation d'avoir accès aux dossiers médicaux de tous les patients de la clinique de médecine familiale n'a pas la permission d'accéder à tous les dossiers des patients de la clinique et à tous les jours. L'employé possède en tout temps l'autorisation d'accéder à ces données, mais il ou elle ne possède pas en tout temps la permission de le faire.

62. L'employé ne reçoit la permission de le faire que lorsque l'on lui demande d'accomplir une tâche ou de rendre service à un patient qui nécessitera l'accès aux renseignements personnels de ce patient.

63. Donc, à titre d'exemple, l'employé d'une clinique médicale a la permission d'accéder au dossier du patient LeGrand :
    - lorsqu'il doit vérifier le prochain rendez-vous de ce patient pour lui donner cette date; ou encore,
    - lorsque le médecin lui demande d'envoyer un rapport médical concernant le patient LeGrand à une autre clinique. À ce moment unique, l'employé a la permission d'accéder au dossier du patient LeGrand pour recueillir le rapport. Toutefois, lorsque l'employé a accompli cette tâche précise, l'employé n'a plus la permission d'accéder au dossier du patient LeGrand, sauf si on lui demande d'effectuer un autre service ou autre tâche relativement à ce patient.

Autorisation accordée à l'employé en question

64. À l'embauche de l'employé en question, l'Hôpital et Centre de santé communautaire lui a accordé le niveau d'autorisation d'accès aux systèmes informatisés que l'on jugeait nécessaire afin de lui permettre d'effectuer les tâches de ses deux postes. Puisque l'employé devait accéder système informatisé Meditech pour faire son travail de commis aux admissions, et que l'employé devait également accéder au système informatisé Purkinje en tant que soutien administratif à la clinique de l'unité de médecine familial, on lui a accordé son premier mot de passe pour utiliser le réseau sécurisé, et un deuxième mot de passe pour utiliser les systèmes Meditech et Purkinje.

65. Le niveau d'autorisation d'accès du système Meditech qui lui fut accordé était en fonction de l'enregistrement des patients et faire la gestion de leurs rendez-vous. Par contre, le niveau d'autorisation d'accès accordé à cet employé pour accéder au système Purkinje était beaucoup plus étendu, étant donné la panoplie des tâches à titre de soutien administratif à l'unité de médecine familiale. L'employé en question avait donc l'autorisation d'accéder à tous les antécédents médicaux des patients, ainsi qu'aux données concernant les épisodes de soin, les médicaments courants et passés, les résultats de laboratoire, et bien d'autres contenus des dossiers des patients.

66. De plus, l'employé en question n'avait pas à travailler dans l'unité de médecine familiale pour accéder au système Purkinje car cet accès était possible à partir de l'ordinateur mis à sa disposition au service d'admission lorsque l'employé travaillait à ce poste. L'employé en question pouvait donc accéder les dossiers des patients retrouvés dans le système Purkinje de son ordinateur au service d'admission. C'est de cette façon qu'un document

créé dans le système informatisé Purkinje s'est retrouvé sur l'imprimante au service d'admissions qui a mené à la découverte des atteintes dans cette affaire.

67. Face aux résultats de tous les audits menés dans cette affaire, l'employé en question a admis avoir accédé aux dossiers sans en avoir la permission mais a nié avoir utilisé ou partagé les renseignements y retrouvés. L'employé en question déclare avoir agi ainsi pour satisfaire sa curiosité. Il paraîtrait que cet employé éprouvait des problèmes dans sa vie personnelle et pour s'en apaiser, s'informait des problèmes des autres en inspectant leurs données démographiques : les dates et les raisons de leurs visites.

L'employé en question n'avait pas la permission

68. Il est reconnu que l'employé en question avait l'autorisation nécessaire pour accéder aux dossiers électroniques des patients de l'Hôpital et Centre de santé communautaire sur les systèmes Meditech et Purkinje pour accomplir les tâches de ses deux postes. Par contre, les faits sont sans équivoque que cet employé n'avait pas la permission et donc n'était pas en droit d'accéder les dossiers électroniques des 150 patients répertoriés dans le système Purkinje, y compris des collègues, et membres de sa famille au moment où les dits accès ont été commis.

69. En effet, l'employé en question n'avait pas le droit d'effectuer lors des dernières années les accès qui ont été révélés par les audits menés par le Réseau de santé Vitalité dans cette affaire.

70. De plus, il est incontestable que cet employé a enfreint la *Loi* en utilisant les dits renseignements confidentiels, soit avoir passé à leur impression sur une imprimante de l'Hôpital et Centre de santé communautaire. Nous avons également appris que durant la même période de temps où l'employé est accusé d'avoir commis des atteintes à la vie privée de plusieurs dans sa communauté, l'une des personnes concernées fut interrogée par une autre personne sur un élément particulier de sa santé physique qui n'aurait pu avoir été connu que si on avait lu ou communiqué ses renseignements personnels retrouvés dans son dossier médical.

71. Pour ces raisons, nous doutons sérieusement de la sincérité de ses explications lorsque cet employé déclare ne pas avoir eu l'intention d'utiliser ou de partager les renseignements personnels des personnes que cet employé avait outragées. Non plus sommes-nous en mesure d'accepter les explications offertes que cet employé ait ainsi

violé la vie privée de tellement de personnes, à plusieurs reprises pendant au moins 36 mois uniquement pour combler sa curiosité.

72. À notre avis, cet employé a fait preuve de violations au terme de la *Loi* des plus graves. L'employé en question a perpétré volontairement des accès non-autorisées par la *Loi* et ce de façon continue, sans égard à ses obligations statutaires ni à celles de son emploi, et sans égard envers la protection de la vie privée des gens que cet employé connaît.

Est-ce que l'employé responsable travaille toujours pour le Réseau de santé Vitalité?

73. Lorsque l'Hôpital et Centre de santé communautaire et le Réseau de santé Vitalité ont pris connaissance de ces cas d'atteintes à la vie privée, le Réseau de santé Vitalité a immédiatement retiré l'accès à tous les systèmes informatisés de cet employé. De plus, cet employé fut mis en arrêt de travail pendant la durée de l'enquête menée par le Réseau de santé Vitalité. Suite à la découverte de l'étendue des atteintes, cet employé fut enlevé de ses deux postes et on nous avise que l'employé en question n'est plus à l'emploi dans aucun établissement du Réseau de santé Vitalité.

L'accès non autorisé aux renseignements personnels peut-il mener à un vol d'identité?

74. Une autre préoccupation qui a été portée à notre attention concernait le risque de vol d'identité que constituait l'accès non autorisé aux renseignements personnels sur la santé.

75. Dans les présent cas d'atteintes à la vie privée, l'employé responsable ne semble pas avoir été motivé par un désir de voler l'identité des individus lésés. Comme nous l'avons indiqué plus haut, nous n'acceptons pas que son «fouinage» dans les dossiers médicaux de toutes ces personnes n'était uniquement pour combler sa curiosité ou satisfaire à un besoin personnel. Ayant dit ceci, il n'y a rien qui nous porte à croire que cet employé voulait extraire l'identité de ces personnes à des fins frauduleuses.

76. Toutefois, on ne peut présumer que le risque de vol d'identité est nul lorsque l'intégrité de ses renseignements personnels a été compromise. Pour cette raison, nous offrons des conseils à cet égard.

77. 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.

78. 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 sous la touche *Le vol d'identité et vous,* puis *Document d'orientation*).

Mesures pour corriger ces cas d'atteintes et pour empêcher que des incidents semblables ne se produisent à l'avenir

79. Certes que cette affaire ne va pas prévenir l'octroi des autorisations nécessaires pour permettre au personnel d'accéder les dossiers électroniques des patients afin d'effectuer les tâches de leur travail. Toutefois, ces cas d'atteintes à la vie privée donnent lieu à un examen des mesures de sécurité que le Réseau de santé Vitalité et l'Hôpital et Centre de santé communautaire pour assurer la protection des renseignements personnels sur la santé répertoriés dans des dossiers électroniques sous leur égide.

80. Cet examen est indispensable pour rencontrer l'obligation des dits dépositaires prévue au 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.

81. De plus, et compte tenu de l'étendu des mauvais gestes de la part de l'employé en question inaperçus nonobstant une surveillance régulière, l'examen des garanties sécuritaires entourant l'autorisation accordée et la permission de s'en servir s'avère essentiel.

82. À cet égard, le Réseau de santé Vitalité et la directrice de l'Hôpital et Centre de santé communautaire continue à faire valoir l'importance de la confidentialité dans le milieu de travail. Tel qu'indiqué plus haut, un nouvel employé participe à une sensibilisation obligatoire sur la confidentialité et est tenu de signer le formulaire de reconnaissance de leur obligation envers l'importance de la confidentialité à chaque année pendant son évaluation de rendement. Le personnel peut aussi recevoir de la formation additionnelle au sujet de la confidentialité par l'entremise de sessions de sensibilisation offertes par le Réseau de santé Vitalité. Ces sessions sont offertes dans toutes les zones du Réseau et des présentations *Powerpoint* sont rendus disponibles sur les répertoires partagés de chaque zone et donc accessibles aux employés en tout temps.

83. Les sessions de sensibilisation visant à informer les employés sur l'importance de la confidentialité des renseignements personnels sur la santé des patients souligne la gravité que représente une atteinte à la vie privée, et plus précisément, de la dissimilitude entre une atteinte causée par erreur et une atteinte délibérée. Également, on éduque les employés que de *volontairement* violer la *Loi* entraîne des conséquences dépendamment des circonstances entourant l'incident : soit, l'employé peut recevoir un simple

avertissement de la part du gestionnaire, subir une suspension de ses tâches ou une discipline plus sévère, et même faire face à une dénonciation pour avoir commis une infraction en vertu de la *Loi*.

84. Bien que le Réseau de santé Vitalité nous a indiqué que les sessions de sensibilisation sont offertes à tous les nouveaux employés, nous avons appris que cette formation n'est pas obligatoire pour les employés déjà à l'emploi. Le module qui se veut éduquer les employés sur l'importance de la confidentialité et de la vie privée des patients n'a seulement qu'été offert aux employés de la Zone 1 du Réseau de santé Vitalité. Malheureusement, on nous avise que jusqu'à présent, seul 2700 des 7000 employés du Réseau de santé Vitalité ont participé à ces sessions de formation. Le Réseau de santé Vitalité s'engage à offrir cette session aux employés dans les autres zones et pour faciliter leur participation, cette formation sera offerte en personne et en ligne.

85. Nous pouvons constater qu'en date de ce Rapport, le personnel de l'Hôpital et Centre de santé communautaire a déjà reçu cette formation. De plus, la Directrice de l'Hôpital et Centre de santé communautaire nous a rassurés, et nous n'avons aucun doute, qu'elle prend toutes les occasions possibles pour faire le rappel avec son personnel de l'importance de la confidentialité en milieu de travail et après les heures de bureau.

86. Le devoir de protéger les renseignements personnels des patients en tout temps à l'Hôpital et Centre de santé communautaire est aujourd'hui estampillé partout dans leurs services. Afin de sensibiliser d'avantage le personnel de l'importance de leur obligation envers la confidentialité des renseignements personnels sur la santé, la Directrice de l'Hôpital et Centre de santé communautaire nous a fait part qu'elle a tenu plusieurs rencontres avec son personnel afin de les informer de la situation et des répercussions possibles advenant une défaillance à leur obligation. Nous précisons qu'aucun des noms des personnes concernées n'ait été divulgué pendant ces rencontres.

87. La grande majorité des employés ont participé à ces rencontres et ont pu partager entre eux leurs préoccupations sans en dire de l'impact ces atteintes à la vie privée avait eu sur eux et leurs proches. Personne ne s'était rendu compte que l'employé en question perpétrait de telles violations, mais tous ont vécu la honte qui en a découlé.

88. Sans avoir été demandé de le faire, les membres du personnel se sont portés volontiers sur-le-champ de signer le formulaire portant sur la confidentialité des renseignements personnels sur la santé, un geste signifiant une intention claire que la mauvaise conduite de l'employé en question ne reflétait aucunement leur moralité et honnêteté.

89. Cet établissement, toute comme la communauté dont il dessert, a souffert pendant ce triste épisode et n'espère que de rebâtir la précieuse confiance des citoyens et citoyennes qui régnait auparavant. À notre avis et selon nos observations, nous sommes convaincus que l'Hôpital et Centre de santé communautaire jouira de cette confiance encore une fois à l'avenir compte tenu de toutes les nouvelles mesures pour assurer la protection des données en leur milieu.

90. À titre de conséquence directe des présents cas d'atteintes à la vie privée, le Réseau de santé Vitalité nous a également fait part qu'il passe présentement en revue la politique concernant l'exercice des audits qu'il mène pour surveiller le respect de la part des employés de la vie privée des patients. Aujourd'hui, l'on compte sur FacilicorpNB pour effectuer des vérifications sur demande et au hasard. Les rapports des vérifications sont par la suite acheminés au Chef de la protection des renseignements personnels du Réseau de santé Vitalité pour leur validation et suivis. Le Réseau de santé Vitalité nous informe que suite à une demande d'exécution d'audits, FacilicorpNB est disposé à produire les rapports d'audits indiquant soit la date, l'utilisateur, le dossier du patient qui fut accédé ainsi que le type d'accès commis.

91. Le Réseau de santé Vitalité passe à l'essai de politiques concernant les accès aux données et ce travail a pour but de créer des paramètres d'exécution des audits au hasard, des audits qui pourraient découvrir les accès non autorisés plus rapidement et de prévenir des cas d'atteinte à la vie privée de l'envergure dont les dépositaires - et les membres de la communauté - ont dû faire face dans cette affaire.

92. C'est pour cette raison que nous suggérons au Réseau de santé Vitalité de continuer ses efforts dans cette bonne marche, mais plus impératif, qu'il passe à mener des audits au hasard dans le but de déceler plus rapidement les cas d'accès non autorisés. À cet égard, et afin de prévenir davantage que l'on n'accède pas aux dossiers des patients sans en avoir la permission, le Réseau de santé Vitalité a déjà sensibilisé ses employés de son intention d'effectuer des audits au hasard.

93. La Commissaire s'assurera d'être tenue au courant des différentes mesures entreprises en vue de veiller à ce qu'elles soient mises en application pour veiller à la confidentialité et à la sécurité des renseignements personnels sur la santé des patients desservis par l'Hôpital et Centre de santé communautaire et le Réseau de santé Vitalité.

Commentaires finaux de la Commissaire

94. Cette enquête a révélé des cas d'atteintes de grande sévérité de par le fait que la violation s'étendait à la vie privée d'un très grand nombre de gens, commises au cours de plusieurs années, par un seul employé d'un établissement de santé d'une petite communauté où l'employé et ses victimes y habitent ensemble et se connaissent.

95. L'Hôpital et Centre de santé communautaire et le Réseau de santé Vitalité nous ont assuré qu'ils demeurent conscients des obligations qui leur incombent et de la nécessité de rester vigilant quant à l'adoption et au respect des politiques associées à l'accès des renseignements personnels sur la santé, et la mise en application générale des mesures de sécurité appropriées en vue de protéger les renseignements personnels sur la santé des patients en tout temps.

96. Des mesures de précaution améliorées sont en cours pour rehausser la protection des renseignements personnels sur la santé obtenus auprès des patients. Des audits ne seront plus exécutés seulement lorsqu'une atteinte à la vie privée est découverte ou soupçonnée, mais plutôt au hasard afin d'identifier les atteintes plus rapidement. De plus, les sessions de sensibilisation obligatoires pour tous les employés aideront à éduquer les employés de l'importance de la confidentialité des renseignements personnels sur la santé des patients.

97. Nous avons bon espoir que les mesures correctives appliquées permettront d'assurer une meilleure protection des renseignements des patients à l'avenir.

98. 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 leurs renseignements personnels sur leur santé aux personnels hospitalier et médical, sachant que leur renseignements confidentiels seront utilisés de façon la plus efficace et la plus sécuritaire possible. Cette confiance ne repose pas uniquement sur les avantages qui soutiennent la prestation de soins de santé telle la création des systèmes informatisés où les dossiers médicaux de milliers de gens sont répertoriés et permet une facilité d'accès, mais aussi sur la notion que seuls ceux et celles qui ont l'autorisation d'accès aux systèmes s'en serviront pour effectuer leur travail seulement lorsqu'ils ont la permission de le faire et non pas pour satisfaire un besoin personnel.

99. Une politique visant à sensibiliser ses employés sur leur obligation de protéger la vie privée des gens lorsque le dépositaire traite de leurs renseignements personnels sur la santé des citoyens dans leur communauté avec une mise en garde que le non-respect de cette obligation peut entraîner des répercussions, représente à notre avis une pratique essentielle dans la démarche de rencontrer ses obligations statutaires en vertu de la *Loi.*

100. Quoiqu'il soit de mise d'instaurer une politique visant la protection des données précieuses, elle n'en vaut rien si l'on ne peut en assurer sa conformité. À notre avis, c'est plutôt l'adoption de bonnes pratiques qui engendrera de meilleurs résultats, y compris une sensibilisation soutenue envers les employés sur leur obligation de maintenir la confidentialité des renseignements personnels.

101. Une pratique visant à encourager ses employés d'avouer leurs erreurs commises à l'endroit du traitement des dits renseignements confidentiels est éclairée dans le contexte des erreurs de violation de la vie privée commises de façon non délibérée. Le dépositaire voulant soutenir cette pratique en assurant que nul employé ne sera blâmé même s'il y a preuve de violation délibérée de la *Loi* représente, à notre avis, un défaut sérieux de ses obligations statutaires.

102. Cette affaire met en évidence la facilité d'accès aux données personnelles que possèdent les employés une fois autorisés de la faire à leur embauche. Pourvoir naviguer avec aisance dans les dossiers médicaux sans crainte ni remords de conscience ou de représailles, comme l'a démontré l'employé responsable en causant des centaines d'atteintes, est l'unique raison pour laquelle nous soutenons les efforts du Réseau de santé Vitalité d'entamer une surveillance beaucoup plus vigilante des accès effectués sur les systèmes informatisés par le biais d'audits effectués au hasard.

103. À notre avis, il est sûrement possible de prévenir l'occurrence de pareille violation de la vie privée en adoptant une pratique qui verra à modifier ou enlever l'autorisation d'accès qui est accordé à l'employé à son embauche dans les cas où ce dernier ou cette dernière change de poste ou encore ses tâches ont été accomplies et l'employé n'a plus besoin d'accéder à certains données - à certains systèmes informatisés – pour continuer son travail.

104. Mais ces efforts seuls ne serviront pas de force de dissuasion pour prévenir ceux et celles d'intenter de causer de pareilles violations dans le futur. Il faut dissuader tous ceux et celles chargés de protéger les renseignements privés qui leur sont confiés qui sont indifférents au respect de la vie privée des personnes à qui appartiennent ces renseignements.

105. C'est pourquoi nous portons réflexion sur des mesures plus sévères à l'endroit de cet employé, c'est-à-dire, sur la question de dénonciation à son encontre pour avoir commis ces multiples infractions de la *Loi*. Tel qu'indiqué plus haut dans ce rapport, tout employé d'un dépositaire commet une infraction si, sans l'autorisation de son employeur, communique volontairement des renseignements personnels sur la santé dans des circonstances où l'employeur ne serait pas autorisé à les communiquer sous le régime de la *Loi.*

106. Dans le présent cas, il n'y a aucun doute que l'employé responsable a enfreint la *Loi*, et a commis des infractions à plusieurs reprises. L'employé a admis avoir accédé aux renseignements personnels sur la santé de plus de 150 patients sans en avoir la permission, donc de façon délibérée. Bien que l'employé en question a présenté des explications de souffrir de problèmes personnels, rien n'excuse ses actes à notre avis. Il faut aussi rappeler que nous avons raison de croire que cet employé aurait communiqué les renseignements personnels sur la santé de certains patients à d'autres gens dans la communauté sans l'autorisation de son employeur, et ce en violation de la *Loi*.

107. Nous jugeons les faits entourant cette affaire suffisamment sérieux et qui atteignent le seuil de violation de la vie privée que nous devons agir pour démontrer à tous que l'accès non autorisé aux renseignements personnels sur la santé ne sera pas toléré.

Recommandations

108. À la lumière des conclusions exposées ci-dessus, la Commissaire recommande que les mesures considérées par le Réseau de santé Vitalité dans le but d'éviter de futurs incidents d'atteinte à la vie privée semblables soient mises en œuvre comme suit :

    a) Que chaque employé du Réseau de santé Vitalité, qui a reçu à son embauche une autorisation pour accéder aux systèmes où sont répertoriés les dossiers contenants les renseignements personnels sur la santé afin d'accomplir les tâches de son poste, reçoive une formation adéquate et complète sur la

question de la confidentialité et la protection de la vie privée de ces personnes à qui appartiennent les renseignements;

b) Que la formation indiquée au paragraphe a) ci-dessus adresse en particulier la question à savoir quand l'employé pourra se servir de cette autorisation pour accéder aux dossiers des patients, c'est-à-dire, à quel moment dans son travail l'employé en aura la permission légitime d'y avoir accès;

c) Que la formation indiquée au paragraphe a) ci-dessus soit offerte en premier aux employés déjà en fonction;

d) Que la formation indiquée au paragraphe a) ci-dessus soit offerte aux employés lors des séances de formation continue ne dépassant pas une période de trois ans depuis la dernière formation;

e) Que le Réseau de santé Vitalité informe la Commissaire d'un échéancier durant lequel le Réseau de santé Vitalité prévoit pourvoir entreprendre et accomplir la formation indiquée au paragraphe a) et précisée aux paragraphes b), c) et d) ci-dessus;

f) Que le Réseau de santé Vitalité inclue dans les descriptions de tâches de tout poste l'obligation de l'employé de respecter la confidentialité des renseignements personnels sur la santé en tout temps.

g) Que le Réseau de santé Vitalité adopte sans tarder une nouvelle pratique ce qui concerne l'exercice des audits au hasard des accès aux systèmes informatisés utilisés dans son réseau, y compris Meditech et Purkinje;

h) Que le Réseau de santé Vitalité adopte sans tarder une nouvelle pratique qui veillera à suspendre sur-le-champ l'autorisation d'accès de tout employé qui fait preuve de violation délibérée de la *Loi* et qui inclut d'en aviser la Commissaire à la première occasion raisonnable;

i) Que le Réseau de santé Vitalité adopte sans tarder une nouvelle pratique de passer en révision l'accès accordé aux employés qui n'ont plus besoin d'accéder à un système informatisé en particulier puisqu'ils ont complété ou ont cessé d'effectuer les tâches nécessitant cet accès, et ce, pour les employés dans tous ses établissements, y compris l'Hôpital et Centre de santé communautaire; et,

j) Que la direction de l'Hôpital et Centre de santé communautaire continue ses démarches pour sensibiliser son personnel de leur obligation de maintenir la confidentialité des renseignements personnels en tout temps.

109. Notre Commissariat fera un suivi auprès du Réseau de santé Vitalité et l'Hôpital et Centre de santé communautaire lors du mois de septembre 2013 pour veiller à la mise en œuvre de ces mesures.

110. Enfin, la Commissaire fait part de son intention d'entreprendre des démarches sur la question de dénonciations à l'encontre de l'employé responsable pour avoir commis ces multiples infractions de la *Loi*.

Émis à Fredericton (Nouveau-Brunswick), le 5 juin 2013.

_____

Anne E. Bertrand, c.r.
Commissaire