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*

Dossier de notification d'atteintes à la vie privée: 2012-884-H-277

Dossiers de plaintes d'atteintes à la vie privée : 2013-1239-H-371, 2013-1240-H-372
2013-1264-H-379, 2013-1278-H-385

Date: Le 18 décembre 2014

*« Affaire concernant des accès non-autorisés aux dossiers de patients de fouinage »*

## INTRODUCTION et TOILE DE FOND

1. Ce rapport des conclusions de l'enquête de la Commissaire est émis en vertu de l'article 73 de la *Loi sur l'accès et la protection de renseignements personnels sur la santé* (ci-après, la « *Loi* ») conformément à une enquête effectuée en vertu de l'article 69 de la *Loi* sur les prétendus accès par deux employés qui n'étaient pas autorisés à accéder à des documents électroniques de multiples patients contenant leurs renseignements personnels sur la santé.

2. L'enquête fut entamée à la suite d'une notification faite le 4 juin 2012 auprès du Commissariat par le Réseau de santé Vitalité (ci-après, « Vitalité ») nous avisant que des multiples incidents d'atteintes à la vie privée impliquaient deux employés travaillant dans un hôpital en vertu du sous alinéa 49(1)c)(iv) de la *Loi* :

> 49(1) Le dépositaire est tenu
> …
> *c)* de notifier, la personne physique visée par les renseignements personnels sur la santé et le Commissaire, à la première occasion raisonnable et conformément aux règlements, que ces renseignements ont été :
> …
> (iv) communiqués par une personne non autorisée ou que celle-ci y a eût accès;

3. Comme la stipule la *Loi*, il y a violation de la vie privée lorsque des renseignements personnels sur la santé détenus par un dépositaire font l'objet d'un traitement inadéquat, que ce soit accidentellement ou intentionnellement. Selon l'article 49 de la *Loi* et à l'article 19 du *Règlement 2010-112*, ce serait le cas lorsque les renseignements sont :
   - volés;
   - perdus;
   - éliminés de manière non autorisée;
   - communiqués par une personne non autorisée ou que celle-ci y a eu accès.

   (Nous soulignons)

4. L'article 49 de la *Loi* et l'article 19 du *Règlement 2010-112* stipulent par ailleurs que, lorsque survient un incident de violation de la vie privée, les dépositaires sont tenus d'en aviser à la fois la Commissaire et les personnes visées par les renseignements, c'est-à-dire celles dont la vie privée a été violée. Cette notification doit se faire à la première occasion raisonnable.

5. Vitalité procéda à aviser les individus concernés, soient les personnes à qui appartiennent les renseignements personnels, que quelques mois plus tard après avoir mené son enquête approfondie. Nous élaborons davantage sur cette question plus tard dans ce rapport.

6. Certains des individus avisés des atteintes ont déposé des plaintes auprès de notre Commissariat en vertu du paragraphe 68(2) de la *Loi*, et ce, au début du mois de février 2013:

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

7. Le terme « dépositaire », tel que défini par la *Loi*, est utilisé pour signifier une personne, un groupe ou une institution qui s'est vu confié, par la *Loi*, la responsabilité de recueillir, d'utiliser et de communiquer les renseignements personnels de santé des individus (tels que les patients dans cette affaire), et de protéger ces renseignements en tout temps en conformité avec les règles énoncées dans la *Loi*.

8. Ce rapport des conclusions de l'enquête traite du rôle du Commissariat dans les enquêtes concernant les violations de la vie privée, les faits que l'on a découvert, les audits effectués qui ont mené à la découverte des bris, le niveau d'autorisation accordé aux employés de Vitalité pour accéder aux fichiers électronique des patients dans le système Meditech, l'autorisation accordée dans ce cas et ainsi de suite. Nous concluons avec des recommandations.

## Le rôle du Commissariat

9. Afin d'éviter toute confusion quant au travail de la Commissaire et son bureau, le Commissariat, il est utile en premier de préciser notre rôle et nos responsabilités dans le cadre des enquêtes que nous menons en vertu de la *Loi*. La Commissaire est chargée de fournir une surveillance indépendante de la bonne application des règles gouvernant l'accès aux renseignements détenus par le gouvernement et la protection de la vie privée, à la fois dans le secteur public et le secteur privé des soins de santé. La

protection de la vie privée dans le secteur des soins de santé est codifiée dans une loi en vigueur depuis le 1er septembre 2010, soit la *Loi sur l'accès et la protection en matière de renseignements personnels sur la santé*. La Commissaire est une agente de l'Assemblée législative, et à ce titre, ne fait pas partie du gouvernement ou du secteur des soins de santé et à cet égard, elle mène des enquêtes indépendantes.

10. Lorsqu'une atteinte à la vie privée est alléguée, ce qui signifie que des renseignements personnels sur la santé ont été traités de façon inappropriée, la Commissaire doit enquêter en aussi longtemps que la plainte ou la notification de l'atteinte est liée aux obligations énoncées par la *Loi*. Dans les situations où l'on suspecte que des dossiers de soins de santé n'auraient pas été protégés par ceux qui sont chargés d'en assurer ainsi, l'enquête de la Commissaire sert non seulement à résoudre la plainte afin de faire respecter la vie privée, mais aussi de trouver des moyens afin de mieux sauvegarder les renseignements.

11. La Commissaire n'est pas chargée de mener des enquêtes relatives à des infractions pénales, voyons plutôt à des enquêtes pour s'assurer de la conformité à la *Loi*. Par ailleurs, dans la présentation des résultats de ses enquêtes, la Commissaire ne rapporte pas sur la responsabilité civile ou pénale.

12. La Commissaire n'est pas non plus en mesure de prendre des décisions telles que celles prises à titre d'employeur. Lorsqu'un méfait est établi, la Commissaire ne recommandera pas que des mesures disciplinaires soient imposées; plutôt, la Commissaire recommandera que de telles mesures soient considérées, spécialement dans les circonstances où il s'agit d'une atteinte sérieuse.

13. À cet égard, lorsqu'une régie de la santé a signalé au Commissariat une violation qui implique l'un de ses employés, le Commissariat maintiendra une distance respectueuse du rôle de l'employeur qui est la régie, tout en lui demandant de se conformer à l'enquête de la Commissaire en recueillant les faits nécessaires afin de nous permettre d'enquêter l'affaire. Notre enquête est en parallèle à celle de la régie de la santé, tout en demeurons informés des mesures entreprises, du processus pour notifier les personnes concernées, pendant que nous vérifions les faits recueillis et adressons tous les aspects d'un cas d'atteinte à la vie privée conformément à notre rôle comme organisme de surveillance.

## CONTEXTE DE LA PRÉSENTE ENQUÊTE

### Les parties faisant l'objet de l'enquête

14. La *Loi* s'applique, en autre, au personnel des dépositaires, dénommés « mandataire » qui s'entend d'une personne ou d'un organisme qui représente les dépositaires ou qui agit pour leurs comptes en ce qui a trait à des renseignements personnels sur la santé pour les besoins des dépositaires et non pour ses propres besoins. La présente affaire implique deux dépositaires et deux mandataires, que voici.

***Réseau de santé Vitalité et l'Hôpital Georges-L.-Dumont (dépositaires)***

15. Le Réseau de santé Vitalité gère une série d'établissements francophones et bilingues et fournit des services de soins de santé à près de 250 000 personnes par l'entremise de plusieurs hôpitaux, établissements communautaires, centres de santé, deux centres de santé communautaires, centres de santé mentale, principaux bureaux de santé publique, et ainsi de suite. Les accès non autorisés aux documents électroniques des patients ont eu lieu à l'Hôpital universitaire Dr Georges-L.-Dumont (ci-après «l'Hôpital»). L'Hôpital fait partie de la Zone 1B au sein du réseau Vitalité qui dessert environ 87 000 habitants dans la région rejoignant Richibucto et Sackville et qui comprend la région du grand Moncton.

16. Vitalité et l'Hôpital sont tous deux considérés comme étant des « dépositaires » en vertu de la *Loi*. Pour cette raison, ils sont chargés, de plein droit par la *Loi*, de recueillir, utiliser et partager les renseignements personnels sur la santé des patients, et plus notable, de protéger ces renseignements en tout temps, en vue de protéger la vie privée des patients.

***Les employés A et B (mandataires)***

17. Vitalité a révélé que des accès non-autorisés aux documents électroniques de patients avaient été commis par deux de ses employés, soit un transcripteur médicale ci-après nommé « l'employé A » et un deuxième employé, secrétaire, ci-après nommé « l'employé B », tous deux affairés au bureau des psychiatres de l'Hôpital.

18. On remarque qu'il existe un bureau des psychiatres ainsi qu'une clinique de psychiatrie dans cet Hôpital, tous deux munis d'un personnel distinct. L'employé A - à l'emploi uniquement du bureau des psychiatres tandis que l'employé B - à l'emploi des deux, du bureau des psychiatres ainsi que de la clinique de psychiatrie.

19. De leur part, les employés A et B ne sont pas désignés comme dépositaires, mais plutôt comme « mandataires ». La *Loi* exige néanmoins que les mandataires recueillent, utilisent, partagent et protègent les renseignements personnels sur la santé des patients comme doit le faire leur employeur- dépositaire, et en tout temps, voir au respect de ces règles pour ne pas nuire à la *Loi*.

20. Dans cette affaire, l'employé A aurait visionné les renseignements personnels sur la santé de 99 patients, et ce sur une période de quelques mois (moins d'un an à partir de novembre 2011 jusqu'en mai 2012) sans en avoir l'autorisation de le faire. L'employé B est dit avoir visionné les renseignements personnels sur la santé de un patient sans en avoir l'autorisation et de l'avoir fait le 8 mai 2012.

21. Durant notre enquête, nous avons examiné les circonstances qui ont menées aux allégations quant aux incidents impliquant des accès non-autorisés aux documents électroniques des patients par les deux employés A et B. Nous avons examiné leur formation sur la confidentialité et la protection de la vie privée des patients, le niveau d'autorisation d'accès des deux employés en question, comment les dits employés ont accédé aux documents électroniques des patients dans le logiciel qui gère les documents électroniques de patients (Meditech), soit tous les faits pour nous permettre de déterminer si les accès étaient en effet justifiés ou non.

## Documents électroniques des patients – le système Meditech

22. L'un des aspects les plus fondamentaux et la règle par excellence de la *Loi* convient que les dossiers des patients sont accessibles uniquement avec le consentement du patient ou lorsqu'il existe des circonstances qui permettent légitimement l'accès sans consentement. Cette affaire met en évidence la facilité d'accès aux données personnelles dans des documents électroniques des patients que possède le personnel.

23. Cette facilité d'accès nécessite un niveau plus élevé de surveillance et de contrôle afin d'assurer que seuls ceux qui ont besoin d'accéder aux dossiers des patients le fassent et seulement lorsqu'ils doivent le faire.

24. Tenant compte de cette préoccupation, Vitalité a mis en place des mesures pour accorder et faire la surveillance des accès aux bases de données électroniques qui est accordé à l'ensemble de son personnel. Nous procédons tout d'abord en expliquant ce que l'on entend par un document électronique du patient.

***Le système Meditech***

25. Le document électronique du patient est un fichier informatique qui est créé lorsqu'une personne fréquente, pour la première fois, un établissement de soins de santé. Les renseignements personnels du patient sont alors entrés dans une base de données, notamment son nom, son adresse, son numéro d'assurance-maladie, la date de sa naissance, et ses renseignements sur les soins de santé comme les antécédents médicaux, les tests effectués et les résultats, le diagnostic, et d'autres. Ces renseignements, dénommés des *renseignements personnels sur la santé*, sont répertoriés dans un seul document électronique relatif à cette personne créé dans un système informatique spécialisé connu sous le nom de Meditech.

26. Ainsi, pour chaque personne qui se présente pour la première fois pour recevoir des soins de santé, la régie de soins de la santé crée un document électronique du patient, et le document électronique servira de répertoire de tous les renseignements personnels sur la santé de cette personne recueillis à ce moment-là. Si la personne se présente à nouveau par la suite pour recevoir des soins de santé, son document électronique est alors mis à jour avec les détails supplémentaires fournis à ce moment.

27. Depuis l'an 2006, les utilisateurs du système Meditech remarquent sur l'écran d'accueil des mises en garde par rapport à l'importance de la protection des renseignements personnels, notamment quatre messages distincts changés aux quatre mois. Ces messages se rapportent aux règles que l'accès à toute information est autorisé selon le principe du besoin de savoir, que l'accès à leur propre dossier ou celui d'un membre de la famille pour des raisons qui n'entrent pas dans l'exercice de leurs fonctions constitue une violation directe de la politique, que l'utilisation de toute autre nom d'utilisateur et mot de passe autres que ceux leur étant attribués ou leur partage avec d'autres constitue une violation directe de la politique, et que l'accès est vérifié régulièrement.

28. Ceux et celles qui ne respectent pas les politiques d'accès feront l'objet de mesures disciplinaires.

***Les pratiques de Vitalité pour la formation du personnel en matière de la protection des renseignements des patients contenus dans un document électronique***

29. Lorsque tout employé est embauché par Vitalité, l'individu est obligé de participer à une orientation générale qui comprend une sensibilisation du concept de confidentialité. Les employés doivent signer un formulaire reconnaissant leur devoir de maintenir la

confidentialité, et cette procédure est répétée annuellement. De plus, Vitalité a mis en place des politiques et des pratiques concernant la vie privée et la confidentialité pour assurer que tout son personnel suive la *Loi* et respecte la vie privée des patients en tout temps. Ce respect des règles inclut l'importance de garder les renseignements des patients confidentiels.

30. Vitalité maintient depuis longtemps une politique obligeant tous les employés de protéger les renseignements des patients. Seuls le personnel pouvait accéder et utiliser ces renseignements avec le consentement du patient ou lorsque cette tâche était permise par la loi, incluant :

- de ne pas discuter de renseignements concernant un patient dans les couloirs, cafétérias, ascenseurs, etc.
- de ne pas mentionner qu'un certain patient a fréquenté l'établissement de soins de santé,
- de ne pas discuter du dossier d'un patient avec d'autres employés qui n'ont pas besoin de connaître ces renseignements pour effectuer leur travail, et
- de ne pas accéder aux dossiers des patients lorsque que l'on ne donne pas de soins au patient.

31. Pour souligner l'importance des obligations énumérées ci-dessus, la dite politique établit également qu'un manquement à n'importe quelle de ces directives peut mener à des mesures disciplinaires ou même au congédiement. Ce respect de la vie privée du patient et de la confidentialité des renseignements du patient se poursuit aujourd'hui et est reflété dans les politiques et pratiques actuelles de Vitalité (CONFIDENTIALITÉ et ATTEINTE À LA VIE PRIVÉE) voulant assurer la conformité au principe de la vie privée des patients, y compris l'obligation de protéger les renseignements personnels sur la santé des patients en tout temps et les conséquences lorsque cette obligation n'est pas respectée.

32. En outre, Vitalité, à titre de dépositaire sous la *Loi*, a reconnu et a pris des mesures afin de rencontrer son obligation statutaire quant à la protection de la vie privée. De plus, l'Hôpital a également le devoir de s'assurer que le personnel suive de telles pratiques.

## LES FAITS RECUEILLIS

### La découverte des atteintes à la vie privée

33. Dans le cas présent, les atteintes à la vie privée des patients par l'employé A ont été portées à l'attention de Vitalité lorsqu'une patiente s'est plainte car elle pressentait que

l'employé A avait accédé de façon non-autorisée son dossier électronique vu qu'un ami en commun de la patiente et de l'employé A semblait être au courant de ses renseignements personnels mais la patiente ne les avait jamais été partagés avec ni l'ami en commun ni avec l'employé A. La patiente se disait d'être une ancienne amie de l'employé A avec qui elle a eu des conflits personnels. De plus, et au dire de la patiente, ses renseignements personnels sur la santé auraient été partagés par l'employé A à une autre amie commune à la patiente et l'employé A.

34. Vitalité a vérifié si l'employé A avait accédé au dossier de cette patiente et a découvert que c'était le cas, et ceci déclencha son enquête. Entre temps, l'employé A fut mis en arrêt de travail et cette suspension devait durer pendant toute la période de l'enquête.

35. En juin 2012, dans le *Formulaire de déclaration de violation de la vie privée* déposé auprès de notre bureau, Vitalité souligne le fait que son enquête interne est toujours en cours et que plus de détails seraient à venir. À partir de cette notification, nous avons entrepris notre propre enquête indépendante en vue de vérifier tous les faits déjà découverts et de déterminer l'ampleur des accès non autorisés présumés qui pouvaient avoir eu lieu dans cette affaire.

36. Lors de son enquête, Vitalité nous partage que l'employé A avait également aidé un autre employé de fouiner dans un dossier électronique d'un patient. En effet, Vitalité a poursuivi son enquête auprès de cet accès de la part de l'employé B et a confirmé que l'employé B aurait visionné, avec l'employé A et à partir de l'ordinateur de ce dernier, les renseignements personnels sur la santé d'un patient.

37. Notre enquête indépendante a donc porté sur les allégations des accès non autorisés aux dossiers électroniques des patients effectués par les deux employés A et B.

## Niveau d'autorisation pour accéder aux dossiers des patients

38. Les employés de Vitalité sont accordés un niveau d'autorisation conforme pour leur permettre d'accéder aux documents électroniques des patients pour effectuer les tâches de leur emploi. En guise de l'obligation de respecter la vie privée du patient, les employés ne sont autorisé d'accéder au dossier d'un patient que lorsque qu'ils ou elles sont demandé d'effectuer une tâche reliée à leur emploi ou de fournir un soin au patient qui lui requiert d'accéder aux renseignements personnels du patient.

39. Les activités du bureau des psychiatres et de la clinique de psychiatrie à l'Hôpital sont répertoriées à partir du système Meditech, donc les psychiatres et leur personnel utilisent le système Meditech pour accéder aux dossiers de leurs patients. Pour bien comprendre comment les atteintes à la vie privée se sont produites dans le présent cas, il est de mise d'expliquer comment le système informatique Meditech est utilisé à l'Hôpital, y compris bureau des psychiatres et de la clinique de psychiatrie.

40. Pour utiliser le système informatique Meditech, un employé reçoit d'abord un nom d'utilisateur et un mot de passe qui lui permettront d'accéder le réseau sécurisé de Vitalité (tel que fournit par FacilicorpNB, un organisme public qui fournit des services d'appui en informatique à Vitalité ainsi qu'à d'autres organismes au sein du système de santé de la province).

41. Le nom d'utilisateur et le mot de passe sont uniques à chaque employé. Cela permet FacilicorpNB, et de surcroît Vitalité, de mieux surveiller les accès au système Meditech effectués par les utilisateurs où les renseignements confidentiels personnels sur la santé du patient sont répertoriés.

42. En résumé, l'accès aux documents électroniques des patients est accompli comme suit: l'employé se connecte au réseau sécurisé à partir de son nom d'utilisateur et son mot de passe unique qui lui ont été attribués. Cela permet à l'employé d'entrer dans l'ensemble du réseau sécurisé informatique en commun. Par la suite, l'employé doit inscrire à nouveau son nom d'utilisateur et son mot de passe afin de se connecter au système Meditech où les documents électroniques des patients sont répertoriés. Une fois à l'intérieur du système Meditech, l'employé ne peut qu'accéder aux modules des dossiers électroniques des patients basé sur le niveau d'autorisation d'accès que l'employé a été accordé afin d'accomplir les tâches de son emploi. À ce stade, l'employé est en mesure d'accéder au dossier d'un patient spécifique par son nom.

43. Il n'est possible d'accéder les documents électroniques de certains patients qu'en effectuant une recherche avec l'intention de le faire, ainsi qu'en effectuant une recherche en se servant du nom de famille du patient en particulier, en entier ou en partie. L'employé peut accéder le dossier d'un patient par inadvertance, mais seulement dans le cas où l'employé a effectué une recherche pour un patient spécifique et a cliqué, par erreur, sur le nom d'un autre patient et accède au lieu au dossier de ce dernier. Lors de l'affichage et à la lecture du contenu du dossier repéré par inadvertance, l'erreur se révèle rapidement car l'employé voit l'identité complète du patient et à ce moment quitte le dossier électronique.

***Niveau d'autorisation d'accès accordé à l'employé A***

44. L'employé A fut embauché par Vitalité le 7 mai 2011 à titre de transcripteur médical au bureau des psychiatres de l'Hôpital. Vitalité nous a confirmé, qu'à son embauche, l'employé A a signé la Déclaration de confidentialité et de non divulgation et a complété le module de formation en ligne sur la protection de la vie privée et la confidentialité. On note que l'employé A n'était dans son poste que pendant un an à la date de la découverte des accès douteux, mais l'employé A était pleinement au courant de ses obligations statutaires et d'emploi de respecter la confidentialité des renseignements personnels sur la santé des patients en tout temps.

45. L'employé A fut accordé un nom d'utilisateur et un mot de passe qui lui était unique et qui lui permettait d'accéder au réseau sécurisé de Vitalité. De plus, cet employé reçu un mot de passe qui lui était unique pour lui permettre de se connecter au système Meditech et d'accéder aux documents électroniques des patients.

46. Donc, l'employé A avait le niveau d'autorisation d'accès nécessaire pour accomplir ses tâches de transcripteur médical, telles que dactylographier des expertises psychiatriques (exigées par les tribunaux ou les compagnies d'assurance) ainsi que des rapports médicaux dictés par les psychiatres. Les rapports ainsi transcrits étaient consignés au dossier des patients et acheminés dans aux médecins qui avaient demandé la consultation psychiatrique.

47. L'employé A avait accès aux modules suivant du système Meditech:
- l'admission pour enregistrer les visites de tous les patients (ce module n'est pas restreint par location, ce qui signifie que l'employé A peut voir toutes les différentes visites des patients peu importe l'unité de l'Hôpital),
- les archives qui permet de voir l'historique des visites des patients (ce module n'est pas restreint par location, ce qui signifie que l'employé A peut voir toutes les différentes visites des patients peu importe l'unité de l'Hôpital), et
- le module « Patient Care Inquiry » qui permet de consulter les rapports de transcription.

48. La «restriction à la location» signifie un accès seulement aux patients de l'unité où se trouve l'ordinateur. Par exemple, lorsqu'un employé travaille à partir d'un ordinateur de l'unité de néphrologie, il ou elle a seulement accès aux dossiers électroniques des patients de l'unité de néphrologie. Donc, une non-restriction à la location veut dire que

l'employé peut accéder aux documents électroniques de tous les patients dans Meditech, peu importe l'unité, quoique seulement pour accéder certaines modules.

***Niveau d'autorisation d'accès accordé à l'employé B***

49. L'employé B fut embauché par Vitalité le 1er mai 2006. À son embauche, ce dernier a signé la Déclaration de confidentialité et de non-divulgation et a complété la formation en ligne sur la protection de la vie privée et la confidentialité. De plus, Vitalité nous informe que le bureau des ressources humaines a fait relire et signer à nouveau la Déclaration de confidentialité et de non-divulgation lors de ses appréciations de rendement annuelles. Dès lors, nous pouvons conclure que l'employé B était pleinement au courant de ses obligations statutaires et d'emploi de respecter la confidentialité des renseignements personnels sur la santé des patients en tout temps.

50. Pour ce qui est du niveau d'autorisation d'accès de l'employé B, ce dernier accomplissait des tâches cléricales pour la clinique de psychiatrie et le bureau des psychiatres tels que l'entrée des résultats de tests, la gestion des rendez-vous, l'accueil des patients, la préparation des dossiers, etc. L'employé B occupait un poste nécessitant de travailler à plus d'un endroit dans l'Hôpital, donc l'employé B fut accordé deux comptes d'utilisateur du système Meditech, soit un compte comme réceptionniste en psychiatrie (sans restriction par location), et un compte comme réceptionniste aux soins infirmiers (avec restriction à la location).

51. Lors de l'utilisation de son compte utilisateur à la clinique de psychiatrie, l'employé B pouvait accéder dans Meditech :
- le module d'admission pour enregistrer les visites de tous les patients (ce module n'est pas restreint par location, ce qui signifie que l'employé B peut voir toutes les différentes visites des patients peu importe l'unité de l'Hôpital),
- le module « Medical Information System » qui lui permet de consulter l'adresse, le numéro de téléphone et de télécopieur des médecins,
- le module pour faire l'envoie et la réception des messages à l'interne dans Meditech, et
- le module « Scheduling » pour céduler les rendez-vous des patients avec les différents psychiatres.

***Surveillance des employés***

52. La surveillance du personnel est une mesure efficace de contrôle pour discerner si le personnel de Vitalité respecte leur obligation de conserver les renseignements personnels sur la santé confidentiels en tout temps en n'utilisant leur niveau d'autorisation aux dossiers électroniques de patients que lorsque nécessaire afin d'accomplir leurs tâches.

53. Nous nous sommes informés auprès de Vitalité du niveau de surveillance exercé auprès des employés A et B en question, et on nous a indiqué que la gestionnaire, à la fois responsable du service de psychiatrie et du bureau des psychiatres, fait une surveillance indirecte et les interactions avec les employés sont plutôt en fonction de problématiques qui sont porté à son attention. Douze psychiatres qui œuvrent dans ce secteur abordent auprès de la gestionnaire les problématiques opérationnelles au besoin. Nul n'avait souligné de problème concernant les employés A et B avant la découverte des incidents qui nous concerne.

54. Puisque la surveillance des employés ne peut pas toujours être suffisante, un autre moyen de déceler si le personnel respecte son niveau d'autorisation aux documents électroniques des patients est de mener des audits aléatoires (ou des audits sur demande dans le cas où l'on suspecte des accès non-autorisés).

## Procédure d'audits pour dépister les accès douteux aux documents électroniques des patients

55. Un employé reçoit la permission d'accéder à des dossiers de patients lorsque l'on lui demande d'accomplir une tâche dans le cadre de son travail ou avec le consentement du patient. Donc, un accès au dossier du patient est jugé non-autorisé lorsque l'employé a extrait ou a lu des renseignements personnels sur la santé de patients à l'extérieur de tels paramètres de son travail.

56. Afin de déterminer si les accès effectués par le personnel sont autorisés ou non, Vitalité peut entreprendre des audits aléatoires. Un audit génère une liste énumérant les accès par l'utilisateur pour une période d'un mois et permet une vérification à savoir si les accès sont autorisés.

57. Le comité formé pour effectuer ces audits est connu sous le nom de *Comité de sécurité et accès à l'information électronique* et est chargé d'examiner et de surveiller l'accès aux

systèmes électroniques contenant des renseignements personnels sur la santé en vue d'assurer que les utilisateurs s'en servent et les communiquent que de façon appropriée.

58. Si l'audit démontre que l'accès est douteux, le Comité procédera à la préparation d'un rapport d'incident au bureau approprié pour déclencher un suivi (à l'agent de la vie privée ou à un gestionnaire de l'unité), soit une enquête. On peut demander au Comité de procéder à une vérification plus approfondie des accès de l'employé visé et dans plusieurs cas, un second audit reprend une période de six mois. Cet audit plus étendu est effectué en premier en faisant une demande spécifique à FacilicorpNB qui à son tour identifiera les documents nécessaires qui démontrent tous les accès réalisés par l'employé au cours de la période de six mois. Ces documents sont ensuite soumis au Bureau du Chef régional de la protection de la vie privée aux fins d'examen. Les résultats de l'audit de six mois sont passés en revue de la même façon afin de découvrir s'il y a eu d'autres accès douteux.

59. Si des accès douteux supplémentaires sont découverts, le Bureau du Chef régional de la protection de la vie privée effectue une révision de ces accès et où un ou plusieurs accès sont jugés non autorisés, les résultats de cette étape suffiront à entraîner une enquête plus approfondie et une notification à la Commissaire.

60. À titre d'exemple, si un employé a accédé au dossier d'un patient pendant que l'employé n'exerçait pas les tâches de son travail au moment où l'accès ait eu lieu, on lui exigera de s'expliquer auprès des responsables compétents afin de déceler si l'accès était autorisé ou non. En autres mots, l'employé devra expliquer si l'accès était accidentel ou s'il avait reçu la permission du patient d'accéder au dossier.

***Accès douteux et aveux de la part de l'employé A***

61. Dans cette affaire, après avoir reçu une plainte de la part d'une patiente alléguant un accès non-autorisé à son dossier électronique, Vitalité a effectué un audit pour une période d'un mois au dossier de la patiente afin de découvrir s'il y avait des accès douteux. Le résultat de l'audit a révélé trois accès douteux de la part de l'employé A. Un audit plus approfondie a alors été effectué de tous les accès de l'employé A pour une période rétrospective de 6 mois afin de déceler si l'employé A avait accédé de façon non autorisée des dossiers électroniques d'autres patients. Les résultats ont révélés plusieurs accès douteux qui dans la majorité des cas, étaient à des dossiers des patients connus par l'employé A.

62. Suite à ces résultats, Vitalité entrepris d'effectuer un audit depuis l'embauche de l'employé A, soit en mai 2011. Les résultats de cet audit démontrent que l'employé A aurait accédé à 99 dossiers électroniques de patients de façon non-autorisée entre le mois de novembre 2011 et de mai 2012. De plus, l'audit démontre que l'employé A aurait tenté de visionner les dossiers électroniques de trois individus en effectuant une recherche d'après leurs noms, mais qu'aucun résultat n'a été affiché puisque ces individus n'avaient jamais fréquenté l'Hôpital à titre de patients.

63. Ayant les résultats des audits en main, Vitalité a tenu quelques rencontres avec l'employé A et lui a demandé de partager ses motifs quant aux accès, et aussi de dévoiler si l'employé A avait partagé les renseignements personnels sur la santé des patients avec d'autres gens. Selon la preuve obtenue, l'employé A admis avoir effectué une recherche à partir des noms de patients et patientes connues, mais ne pas se souvenir des raisons pourquoi l'avoir fait à des dossiers de patients ou patientes dont les noms lui étaient inconnus. L'employé A dit avoir agi ainsi par simple curiosité et ne pas croire avoir divulgué les renseignements personnels vus à d'autres personnes; n'étant pas certain de ce fait, l'employé A aurait ajouté que si une telle divulgation avait eu lieu, l'employé affirmait l'avoir fait sans malice et par accident.

64. Vitalité a tenté de découvrir si l'employé A avait en effet partagé les renseignements personnels sur la santé des patients, et plus précisément ceux de la patiente qui s'était plainte à cet égard, mais l'employé A n'a pas avoué avoir partagé les renseignements personnels sur la santé de la patiente en question.

65. Selon une appréciation raisonnable des faits, nous jugeons que l'employé A aurait communiqué les renseignements personnels de la patiente qui s'est plainte. La patiente pressentait que l'employé A avait accédé de façon non-autorisée son dossier électronique vu qu'un ami en commun semblait être au courant de ses renseignements personnels sur la santé mais la patiente ne les avait jamais été partagés. L'employé A avait en effet accédé au dossier de la patiente sans en être autorisé, et il est raisonnable de tirer la conclusion que l'employé A partagea cette information avec l'ami en commun.

66. Les faits ne sont pas réfutés. L'employé A a admis avoir agi sans autorisation et de façon délibérée par simple curiosité en accédant à 99 dossiers électroniques de patients, en ayant tenté d'accéder à trois dossiers électroniques de patients sans succès, ainsi que d'avoir communiqué les renseignements personnels d'au moins une patiente. Donc,

l'employé A a admis avoir accédé et avoir lu des renseignements personnels sur la santé de près d'une centaine de patients, sans autorisation et de façon délibérée. De plus, nous doutons sérieusement de la sincérité de ses explications lorsque cet employé déclare ne pas avoir eu l'intention de partager les renseignements personnels des personnes dont la vie privée cet employé avait outragé. L'employé A a volontairement communiqué des renseignements personnels sur la santé d'une patiente, sans égard à ses obligations statutaires ni à celles de son emploi, et sans égard envers la protection de la vie privée de cette patiente contrairement à la *Loi* et en violation des sous-alinéas 76(1)(a) et (b), ainsi qu'au paragraphe 76(2) de la *Loi* qui stipule comme suit:

> 76(1) Il est interdit :
>
> (a) de recueillir, d'utiliser ou de communiquer des renseignements personnels sur la santé en violation délibérée de la présente loi,
>
> (b) de tenter d'obtenir ou d'obtenir des renseignements personnels sur la santé, ou de tenter d'avoir accès ou d'avoir accès à des renseignements personnels en violation délibérée de la présente loi, …
>
> 76(2) Commet une infraction l'employé d'un dépositaire ou d'un gestionnaire de l'information qui, 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 présente loi,
>
> 76(5) Quiconque contrevient au paragraphe (1), (2), (3) ou (4) commet une infraction punissable en vertu de la partie II de la Loi sur la procédure applicable aux infractions provinciales à titre d'infraction de la classe F.

***Accès douteux et aveux de la part de l'employé B***

67. C'est lors des plusieurs rencontres avec l'employé A que Vitalité a découvert que l'employé B aurait également accédé de façon non-autorisée le dossier d'un patient, étant le dossier électronique de l'enfant d'une autre personne.

68. Les responsables de Vitalité se sont donc entretenus avec l'employé B afin de connaître la raison de l'accès non-autorisé des documents électroniques. L'employé B dit avoir eu un conflit personnel avec une certaine personne et l'employé B voulait savoir l'heure à laquelle cette personne devait se présenter pour un rendez-vous à la clinique d'obstétrique, une clinique qui est à proximité de la clinique de psychiatrie à l'Hôpital. L'employé B demanda alors à l'employé A d'accéder le dossier électronique de l'enfant de cette personne pour éviter d'être à son poste de travail et éviter la personne à

l'heure de son rendez-vous. L'employé B avait accès aux horaires des autres cliniques, y inclut la clinique d'obstétrique, mais aurait tout de même demandé à l'employé A d'accéder le dossier afin que l'employé B puisse visionner le dossier et connaître l'heure du rendez-vous de la personne.

69. Suite à cette découverte, Vitalité a effectué un audit du dossier du patient en question et a déterminé que l'employé B, par l'entremise de l'employé A et l'ordinateur de ce dernier, avait accédé au dossier électronique du patient le 8 mai 2012. Selon la politique de Vitalité, des audits additionnels pour une période de trois mois ont été effectués (soit entre le 7 mai et 16 août 2012) afin de déceler si l'employé B avait accédé de façon non-autorisée des dossiers électroniques de d'autres patients. Les résultats de ces audits ont démontré que ce n'était pas le cas, et que les autres accès de cet employé étaient justifiés. Dès lors, Vitalité n'a pas entrepris d'audits additionnels concernant cet employé.

70. Selon notre appréciation de ces faits non-contestés, nous jugeons que l'employé B a enfreint la *Loi* dans le cadre de son travail car l'employé B a admis avoir accédé et avoir obtenu des renseignements personnels sur la santé d'un patient, sans autorisation et de façon délibérée, et ce en contravention de l'alinéa 76(1)(b) de la *Loi* :

> 76(1) Il est interdit :
> …
> (b) de tenter d'obtenir ou d'obtenir des renseignements personnels sur la santé, ou de tenter d'avoir accès ou d'avoir accès à des renseignements personnels en violation délibérée de la présente loi, …

***Les employés A et B travaillent-ils toujours pour le Réseau de santé Vitalité?***

71. Comme mentionné plus haut, l'employé A fut mis en arrêt de travail pendant la durée de l'enquête de Vitalité. Nous pouvons rapporter que l'employé A a démissionné de son poste le 26 juillet 2012 et l'employé A n'est plus à l'emploi dans aucun établissement du Réseau de santé Vitalité.

72. Pour ce qui en est de l'employé B, cette personne est toujours au service de Vitalité. Toutefois, suite à la découverte de l'atteinte à la vie privée d'un patient, l'employé B fut soumis à des mesures disciplinaires en fonction de la Politique sur les atteintes à la vie privée de Vitalité. Vitalité a jugé que l'incident d'atteinte à la vie privée était une atteinte intentionnelle mais non malveillante quoique tout de même une infraction des politiques de Vitalité et de la *Loi*. Les mesures disciplinaires imposées à l'employé B ont

compris : une discussion au sujet des politiques sur la confidentialité et des procédures pertinentes sur l'accès aux dossiers et le respect de la vie privée, une formation à nouveau sur la protection de la vie privée et des conséquences du non-respect, et un réengagement en signant à nouveau une Déclaration de confidentialité et de non-divulgation de Vitalité.

## PROCESSUS DE NOTIFICATION D'ATTEINTE À LA VIE PRIVÉE

73. L'objectif principal de la *Loi* est de protéger la vie privée des personnes dont les renseignements personnels sur la santé ont été confiés à un dépositaire. En outre, les personnes affectées par une atteinte à la vie privée ont le droit de savoir que leurs renseignements personnels sur la santé ont été compromis.

74. L'objectif de la *Loi* n'est non plus de dissimuler la conduite du dépositaire (ou son personnel) ni à cacher son identité en cas d'atteinte à la vie privée. Au contraire, le processus de notification en vertu de la *Loi* exige, pour cette raison, que les dépositaires Vitalité et l'Hôpital en question soient nommés.

75. Conformément à l'article 49 de la *Loi* et ses règlements, les personnes concernées doivent être informées de ce qui s'est produit et de quand l'incident a eu lieu, y compris:

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 and le lieu de la violation de la vie privée;
e) La date à laquelle le dépositaire a pris connaissance de la violation de la vie privée.

76. Par ailleurs, toute personne touchée par une atteinte à la vie privée doit être formellement informée de son droit de déposer une plainte auprès du Commissariat. Le dépositaire ne sera pas autorisé à s'abstenir de répondre aux questions qui en découlent, y compris de fournir des explications concernant la cause de l'atteinte et la personne – et du nom de l'employé - responsable.

**Notification des atteintes à la vie privée dans ce cas**

77. Comme indiqué précédemment, lorsque les nombreux accès douteux ont été découverts en juin 2012, Vitalité en a avisé le Commissariat peu de temps après. Cependant, Vitalité ne pouvait pas procéder à notifier les patients concernés avant d'avoir vérifié et confirmé que les accès étaient effectivement non autorisés et que l'employé A avait eu l'occasion de fournir des explications dans chacun des cas d'accès douteux. De plus, c'était pendant l'enquête des accès douteux de la part de l'employé A qu'un accès douteux de l'employé B a été découvert. Après tout le travail pour vérifier les accès douteux, Vitalité pouvait procéder à en informer toutes les personnes concernées, selon leur obligation statutaire en vertu de l'article 49 de la *Loi*.

78. À notre avis, il était nécessaire pour Vitalité de procéder ainsi avant de procéder à la notification de près de cent patients. Nous avons convenu que Vitalité pouvait procéder dans un seul envoi afin que le Bureau du Chef régional de la Protection de la vie privée de Vitalité, avec des arrangements en place, soit en mesure de répondre à tous les appels des personnes concernées. Pour ces raisons, nous constatons que le délai de notification dans la présente affaire était raisonnable compte tenu des circonstances.

79. Vitalité a avisé par lettres toutes les personnes touchées par les atteintes à la vie privée au début du mois de février 2013. Chaque lettre informait la personne de la découverte de l'atteinte à la vie privée, que les renseignements accédés pouvaient avoir inclus, d'après le dossier du patient, des données démographiques, telles que le nom, l'adresse postale, le numéro de téléphone, l'état civil du patient, ainsi que des renseignements personnels sur la santé tels que les noms des médecins traitants, numéro de chambre, renseignements d'assurance privée, numéro de dossier, le numéro d'assurance-maladie, nom de mère, date de congé et raison des visites. Vitalité invitait ces gens de poser des questions au sujet du cas ou de partager leurs inquiétudes s'ils désiraient de le faire et de leur droit de déposer une plainte auprès de la Commissaire au sujet de l'atteinte.

80. Plusieurs des personnes concernées ont également contacté notre bureau pour partager leurs préoccupations et pour solliciter plus d'information concernant cette affaire. Parmi ces personnes, quatre d'entre eux ont exercé leur droit de déposer une plainte officielle en vertu de la *Loi* et le résumé de leurs plaintes soulevait les questions suivantes:

- Qui est l'employé ayant commis l'atteinte?
- Quels renseignements personnels sur la santé furent accédés?

- Une longue période de temps s'est écoulée avant la découverte de l'atteinte. Quelle est la raison pour cela?
- Comment et pourquoi l'atteinte s'est-elle produite?
- L'atteinte à la vie privée pourrait-elle entraîner un vol d'identité?

81. Nous avons refilé à Vitalité les questions à savoir l'identité des employés A et B qui avaient accédé à leurs dossiers, car rien n'empêche d'en informer les individus concernés qui en font la demande auprès du dépositaire, étant Vitalité. Nous ne prescrivons pas d'annoncer au public le nom d'un 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. De plus, Vitalité pouvait répondre plus précisément sur quels renseignements personnels sur la santé furent accédés dans le cas particulier des patients concernés. Comme constaté plus haut dans ce rapport, nous avons répondu aux autres questions soulevées par les personnes concernées. Maintenant, nous adressons la question de vol d'identité.

***Est-ce que les accès non autorisés pourraient mener au vol d'identité***

82. Une autre inquiétude portée à notre attention était le risqué de vol d'identité en raison des accès non autorisés commis par ces employés aux renseignements personnels sur la santé des patients concernés. Il appert de répéter que nous avons vérifié les faits de ce cas et nous n'avons pas découvert des faits à l'appui que les employés A et B accédaient les dossiers des patients et leurs renseignements personnels en vue de s'en servir pour voler leur identité ou de vendre leur identités à des tiers.

83. 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.

84. 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.

85. 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*).

## CONCLUSIONS DE L'ENQUÊTE

86. La *Loi* visent à améliorer le système de soins de santé global au Nouveau-Brunswick, à faire en sorte que les personnes physiques se sentent à l'aise de communiquer leurs renseignements personnels, sachant que ceux-ci demeureront confidentiels et que leur sécurité sera assurée, et en sorte que les fournisseurs de soins de santé soient mieux outillés pour dispenser des soins par l'utilisation de renseignements plus exacts, à jour et complets sur leurs patients.

87. Cette confiance repose non seulement sur les avantages contribuant à la prestation des soins de santé, comme la création de systèmes informatiques renfermant les dossiers médicaux de milliers de personnes alors facilement accessibles, mais aussi sur la

prémisse selon laquelle seules les personnes autorisées à accéder à ces systèmes les utiliseront dans l'exercice de leurs fonctions, et seulement lorsqu'elles ont l'autorisation de le faire, plutôt que pour satisfaire un besoin personnel.

88. Avec plus d'importance, la *Loi* codifie les mesures entourant les renseignements des patients qui garantiront la responsabilisation des personnes qui les ont en main. À cet égard, elle établit des règles très claires relativement au traitement des renseignements personnels sur la santé, de leur collecte, leur utilisation et leur communication, et à leur conservation et leur entreposage, toutes centrées sur un seul et même principe élémentaire : assurer en tout temps la protection et la sécurité des renseignements afin de protéger la vie privée des personnes physiques concernées.

89. La présente affaire concerne les accès non-autorisés à 99 documents électroniques de patients effectués de façon délibérée de la part de l'employé A, y compris la communication de certains renseignements personnels sur la santé d'une patiente. Cette affaire concerne aussi un accès non-autorisé de la part de l'employé B. Les employés en question avaient l'autorisation nécessaire pour accéder aux dossiers électroniques des patients de l'Hôpital sur le système Meditech pour accomplir les tâches de leurs postes. Par contre, les faits sont sans équivoque que ces employés n'avaient pas ni la permission ni aucune justification, donc n'était pas en droit, d'accéder les dossiers électroniques des patients répertoriés dans le système Meditech en question dans cette affaire.

90. L'employé A, entre novembre 2011 et mai 2012, a accédé à 99 dossiers et a communiqué certains renseignements confidentiels dans un cas à un ami en commun avec la patiente. Nous avons douté sérieusement de la sincérité de ses explications d'avoir agi ainsi. Il faut dire que 99 accès non-autorisés dans une courte période de six mois fait preuve d'insouciance envers la *Loi* et de la vie privée de ces patients.

91. Pour ce qui de l'employé B, le fait que ce dernier n'ait accédé qu'à un seul dossier de façon non-autorisée ne minimise pas le sérieux de l'affaire; accéder à des dossiers électroniques de patients pour satisfaire sa curiosité est en contravention de la *Loi*.

92. Les dépositaires Vitalité et l'Hôpital sont tenus, en vertu de l'article 50 de la *Loi*, de protéger les renseignements personnels sur la santé par l'adoption de pratiques comportant des garanties obligatoires conçues de manière à assurer la confidentialité, la sécurité et l'intégrité de l'information et elles sont décrites de manière plus détaillée à l'article 20 du *Règlement du Nouveau-Brunswick 2010-112* de la *Loi* telles que de:

- ✓ limiter l'accès aux renseignements personnels sur la santé et leur utilisation aux personnes explicitement autorisées;
- ✓ protéger les renseignements personnels sur la santé au cours de leur collecte, de leur utilisation, de leur communication.

93. Lorsque l'une ou l'autre de ces règles ou garanties n'est pas appliquée, suivie ou respectée, les dépositaires et leurs personnels risquent fort de commettre ce que l'on appelle une *violation de la vie privée*. Faire une surveillance plus accrue aurait peut-être décelé les accès non-autorisés de l'employé A; toutefois, l'engagement personnel de suivre les règles selon une bonne formation de respecter la confidentialité et la vie privée des patients et des bonnes directives et pratiques comme l'impose Vitalité à l'embauche de son personnel et au cours de la période d'emploi aurait dû suffire.

94. Malheureusement, cette affaire remet en évidence la facilité d'accès aux données personnelles que possèdent le personnel pour naviguer avec aisance dans les dossiers des patients sans crainte ni remords de conscience ou de représailles, comme l'a démontré l'employé A, responsable de près d'une centaine atteintes à la vie privée de patients dans cette affaire.

95. Fouiner dans les dossiers médicaux tend rapidement à devenir l'un des actes les plus signalés et reprochés par le public parmi ceux posés par des employés ayant comme fonction de travail le traitement des renseignements personnels sur la santé, et ce, non seulement au Nouveau-Brunswick.

96. À Terre-Neuve-et-Labrador, deux employés ont été accusés d'infraction en vertu de la *Personal Health Information Act* à la suite de deux enquêtes distinctes menées par le Commissaire à l'information et à la protection de la vie privée, qui avait reçu des plaintes selon lesquelles les deux personnes en question auraient accédé de façon irrégulière aux renseignements médicaux personnels de nombreux patients. Quelques mois passés, ces deux employés ont comparu devant la Cour provinciale de Terre-Neuve-et-Labrador où ils ont été imposés une amende, soit 1 000$ pour l'un employé et 5 000$ pour l'autre. Ces amendes devraient signaler à tous l'importance que la *Loi* rattache à la confidentialité des renseignements personnels sur la santé, étant des plus précieux, et que la violation de cette confidentialité ne sera pas tolérée par la société.

97. Dans la dernière année, nous avons émis des recommandations auprès du Réseau de santé Vitalité sur le besoin d'augmenter la fréquence des audits aléatoires afin de déceler les accès non-autorisée plus rapidement (voir les Rapports de conclusions 2012-

743-H-236 publié le 5 juin 2013 et 2014-1294-H-393 publié le 31 juillet 2014). Nous répétons ces recommandations pour encourager le Réseau de santé Vitalité de mettre en œuvre un processus et d'allouer les ressources nécessaires à la réalisation plus fréquente et régulière de vérifications aléatoires des accès aux bases de données de patients existantes de Meditech.

98. Ceci étant dit, nous sommes heureux de signaler la décision de Vitalité d'avoir accepté nos recommandations antérieures et que Vitalité explore en ce moment des options pour assurer une telle surveillance plus accrue des accès aux documents électroniques des patients.

## RECOMMANDATIONS

99. Vu les conclusions élaborées dans ce rapport, la Commissaire présente les recommandations suivantes à Vitalité :

**Recommandation n° 1 :** La Commissaire recommande que le Réseau de santé Vitalité poursuive ses efforts de mettre en œuvre une surveillance plus accrue des accès aux documents électroniques des patients, soit d'allouer les ressources nécessaires à la réalisation plus fréquente et régulière de vérifications aléatoires des accès aux bases de données de patients existantes de Meditech. Ces vérifications aléatoires plus fréquentes et régulières doivent viser tous les fournisseurs de soins de santé et leur personnel employé par Vitalité.

Le Réseau devra fournir à la Commissaire une mise à jour sur l'état de la mise en œuvre de la **Recommandation n° 1** au plus tard le 27 février 2015.

**Recommandation n° 2 :** Compte tenu de l'ampleur des actes d'accès non conformes à la *Loi* reprochés à l'employé A, en vertu du paragraphe 76(1) et (2) de la *Loi* et puisqu'on souhaite montrer que l'accès non autorisé aux et la communication des renseignements personnels sur la santé ne sera pas toléré au Nouveau-Brunswick, la Commissaire recommande vivement que le Réseau de santé Vitalité envisage la possibilité de porter des accusations contre l'employé A en vertu de la *Loi sur la procédure applicable aux infractions provinciales*.

**<u>Recommandation n° 3</u> :** Vu l'acte de violation de la vie privée commis par l'employé B et ses aveux, et compte tenu des mesures disciplinaires qui lui fut imposées par Vitalité en raison de cette méconduite, la Commissaire recommande que l'employé B soit soumis à une surveillance (par des audits aléatoires) de ses accès aux documents électroniques des patients dans Meditech pendant une période de trois mois à compter de la date de ce Rapport.

100. Le Commissariat fera le suivi auprès du Réseau de santé Vitalité au cours des prochaines semaines et des prochains mois au sujet de la mise en œuvre des présentes recommandations.

FAIT à Fredericton (Nouveau-Brunswick), ce _____ décembre 2014.

_____
Anne E. Bertrand, c.r.
Commissaire