Rapport des conclusions en vertu de la *Loi sur le droit à l'information et la protection de la vie privée*

par

L'honorable Alexandre Deschênes, C.R.

Délégué de l'ombud de la province du Nouveau-Brunswick

Le 10 mai 2023

Citation : EM/ANB Inc. (Re), 2023 NBOMBUD 1

A. Introduction

1. L'enquête dont il est question aux présentes fait suite à une atteinte à la vie privée signalée par Ambulance Nouveau-Brunswick (EM/ANB Inc., ci-après désignée comme ANB) à l'ombud du Nouveau-Brunswick le 7 février 2022. En vertu de l'alinéa 4.2(4)*d*) du *Règlement 2010-111* (ci-après, le *Règlement*) adopté sous le régime de la *Loi sur le droit à l'information et la protection de la vie privée* (sauf indication contraire, la *Loi*), ANB avait l'obligation légale de signaler l'atteinte. L'ombud a déterminé qu'une enquête formelle s'imposait, et en a informé ANB le 8 juillet 2022. En août 2022, l'ombud m'a désigné en vertu de l'article 9 de la *Loi sur l'ombud* pour agir en son nom dans le cadre de l'enquête, car elle estimait qu'elle se trouvait en situation de conflit d'intérêts dans cette affaire.

B. Contexte

2. Sept ans avant l'atteinte signalée, ANB avait chargé ses propres employés des technologies de l'information (unité des TI) de concevoir un site intranet fonctionnant à partir d'une plateforme SharePoint. Des employés comme les travailleurs paramédicaux, munis de leur identifiant unique et de leur mot de passe, s'y connecteraient et y déposeraient des rapports d'incident internes/externes sur les opérations, ainsi que des rapports d'incident liés à la sécurité des patients. Les rapports déposés par le personnel d'ANB ne seraient fournis qu'à sept membres désignés de la direction et du personnel d'ANB. Une caractéristique essentielle de ce système de rapports d'incidents ferait en sorte que les employés non désignés ne puissent avoir accès aux rapports déposés par d'autres employés. Les rapports déposés par les travailleurs paramédicaux dans leur propre espace pouvaient concerner des incidents allant d'accidents ou de problèmes mécaniques avec une ambulance (rapports d'incidents opérationnels) à tout incident lié aux soins aux patients ou susceptible d'influer sur ceux-ci, comme une chute ou une erreur de médication (rapports d'incidents liés à la sécurité des patients).

3. Fin décembre 2021, un travailleur paramédical nouvellement embauché a utilisé la section du site intranet servant aux rapports des incidents opérationnels pour déposer une plainte en fournissant un rapport sur un incident très sensible, qui concernait un autre employé dans le cadre de son travail. Comme le recommande ANB à tous ses employés, les plaintes ou les rapports de nature sensible comme celui dont il est question ici sont généralement traités par le service des ressources humaines de l'organisme, et non pas au moyen du site intranet développé pour les rapports d'incidents opérationnels. Le fait que la recommandation d'ANB n'ait pas été suivie par le plaignant dans le cas présent ne diminue cependant en rien les devoirs et responsabilités d'ANB en tant que dépositaire des renseignements personnels contenus dans ses rapports d'incidents et rapports liés à la sécurité des patients.

4. L'atteinte à la vie privée dont il est question aux présentes s'est produite lorsque, plus d'un mois après que la plainte contenant les renseignements sensibles a été déposée comme rapport d'incident, un travailleur paramédical, à l'instigation d'un collègue, a profité d'une vulnérabilité dans le système de type « porte dérobée » (version française du mot anglais

« backdoor ») pour accéder au rapport d'incident/plainte et le consulter. L'accès non autorisé a été signalé à la direction par l'employé à qui l'on venait d'expliquer comment tirer parti de cette vulnérabilité, laquelle était jusqu'alors inconnue de la direction d'ANB. Bien entendu, ANB a immédiatement verrouillé l'accès non autorisé à tous les rapports remplis dans le système en modifiant les contrôles d'accès. La vulnérabilité a ainsi été éliminée. Pour ceux que cela intéresserait, les employés pouvaient accéder aux rapports déposés par d'autres en cliquant sur l'onglet « Coin des employés », puis sur les onglets « Actions du site » et « Gérer le contenu et la structure », ce qui leur permettait de faire défiler la liste de tous les rapports déposés. ANB a bloqué l'accès non autorisé en éliminant l'accès à la section « Gérer le contenu », qui n'était censée servir qu'au propriétaire du site, pour déplacer, supprimer et copier des documents au sein de ce dernier.

5. ANB a ensuite entrepris une enquête interne sur les causes et la portée de l'atteinte, et a avisé les deux employés concernés ainsi que le Bureau de l'ombud. Dans son rapport, ANB a indiqué que l'atteinte avait entraîné l'accès non autorisé à des renseignements personnels et leur communication. Il s'est avéré qu'une autre lacune majeure du système résidait dans l'absence d'une capacité de journalisation, qui aurait permis à ANB de savoir qui accédait aux rapports, à l'exception de leur auteur. Nous y reviendrons plus loin.

6. L'ombud a le pouvoir, de sa propre initiative, d'enquêter sur cette atteinte autodéclarée afin d'évaluer le degré de conformité avec la partie 3 de la *Loi*, relative à la protection de la vie privée par un organisme public, plus précisément à l'obligation de cet organisme de protéger les renseignements personnels en prenant des mesures raisonnables contre l'accès, l'utilisation, la communication ou l'élimination non autorisés de ces renseignements aux termes de la *Loi* et du *Règlement* (voir le paragraphe 48.1(1) et l'alinéa 64.1(1)*g*) de la *Loi*).

C. Compétence

7. ANB est un **organisme public** au sens de l'article 1 de la *Loi*, car il s'agit d'un **organisme public local** englobant un **organisme de soins de santé**, qui lui-même comprend un autre organisme « figurant dans la partie III de l'annexe I de la *Loi relative aux relations de travail dans les services publics*. », à savoir EM/ANB Inc. À ce titre, ANB est assujettie aux mêmes obligations que les autres organismes publics en ce qui concerne le traitement des renseignements personnels en vertu de la *Loi* et du *Règlement*.

8. ANB est également, dans le domaine des soins de santé, dépositaire de renseignements personnels sur la santé en vertu de la *Loi sur l'accès et la protection en matière de renseignements personnels sur la santé*. **Dans le cas présent**, les renseignements consultés illégalement dans le cadre de l'accès non autorisé ne relèvent pas de la loi susmentionnée, mais constituent certainement des renseignements personnels au sens de l'article 1 de la *Loi*, car il s'agissait notamment du nom des deux employés concernés et de la version des faits de l'employé lésé, telle qu'elle est décrite dans la plainte. Quoi qu'il en soit, j'estime qu'il vaut

la peine d'aborder la communication éventuelle de renseignements personnels sur la santé, du fait de l'incapacité d'ANB à enregistrer l'accès non autorisé à son système de rapports intranet, y compris aux rapports traitant d'incidents liés à la sécurité des patients, qui pourraient, bien sûr, contenir des renseignements personnels sur la santé. La définition de « renseignements personnels » dans la *Loi* comprend en effet les « renseignements personnels sur la santé » de la personne physique. Le rapport d'incident d'un travailleur paramédical en ce qui concerne la sécurité d'un patient, par exemple, peut contenir des renseignements personnels sur le travailleur lui-même (c.-à-d. son degré de stress ou de fatigue extrême tandis qu'il était responsable d'un patient non identifiable pendant le transport). Tout accès non autorisé permettrait de consulter et de communiquer ces renseignements personnels sur la santé – non celle du patient, non identifiable, mais de l'employé auteur du rapport d'incident.

9. L'ombud a désormais des responsabilités décrites dans la *Loi,* dont le pouvoir d'enquêter et de faire rapport sur des affaires impliquant l'accès non autorisé à des renseignements personnels et leur communication par des employés d'organismes publics, y compris l'accès non autorisé à des renseignements personnels sur la santé et la communication de ces mêmes renseignements. Bien entendu, ce pouvoir existe également en vertu de la *Loi sur l'accès et la protection en matière de renseignements personnels sur la santé*.

10. Dans le cas présent, les politiques d'ANB et ses propres directives à l'endroit de ses employés, y compris son rapport au Bureau de l'ombud, indiquent clairement que l'accès à l'incident signalé/à la plainte et leur communication par d'autres employés n'étaient pas autorisés, car ils impliquaient l'accès à des renseignements personnels et leur communication au-delà de ce qui était nécessaire dans le cadre des fonctions liées au travail de ces employés. Ces accès non autorisés pourraient constituer une infraction provinciale décrite dans la *Loi,* et pourraient certainement entraîner des mesures disciplinaires.

11. En ce qui concerne la compétence de l'ombud, il ne fait aucun doute que cette dernière a le pouvoir d'enquêter et de rapporter les faits entourant cette grave atteinte à la vie privée, et de formuler les recommandations qui s'imposent (voir l'alinéa 64.1(1)*g*) de la *Loi*). En tant que délégué de l'ombud en vertu de l'article 9 de la *Loi sur l'ombud*, j'ai désormais le même pouvoir d'enquête et de rapport.

D. Objets

12. Outre la question de la compétence de l'ombud pour ce qui est d'enquêter sur cette atteinte à la vie privée, l'enquête doit porter sur les devoirs et responsabilités d'ANB en tant que dépositaire de renseignements personnels, qui dépendent pour l'essentiel des politiques internes d'ANB, de la *Loi* et du *Règlement*. Dans le présent rapport, il sera souvent question de dispositions de la *Loi* ou du *Règlement*, sans nécessairement que celles-ci soient reproduites. Les dispositions pertinentes figurent à l'annexe A du rapport.

13. De façon générale, en vertu des dispositions pertinentes de la *Loi* et du *Règlement* pris en vertu de celle-ci, ANB est tenue de prendre les mesures de sécurité nécessaires pour contrôler l'accès non autorisé, y compris pour la consignation et la surveillance de l'accès aux renseignements en question. Outre l'adoption de politiques exigeant que tous les employés se conforment à ses dispositions de sécurité, il incombait à ANB – et il lui incombe toujours – de tester et d'évaluer périodiquement l'efficacité des mesures de sécurité mises en œuvre.

14. Lorsqu'une atteinte à la vie privée est signalée au Bureau de l'ombud par un organisme public, le rôle principal de cet organisme de surveillance indépendant consiste à déterminer si les circonstances qui lui sont rapportées montrent qu'il y a bien eu atteinte à la vie privée et, dans l'affirmative, à déterminer si l'organisme public a pris les mesures adéquates pour enquêter sur la situation et y remédier. Dans le cas qui nous intéresse, l'enquête doit également permettre de déterminer si ANB avait respecté son obligation en s'assurant dès le départ, en tant que dépositaire de renseignements personnels et de renseignements personnels sur la santé, que la plateforme SharePoint destinée aux employés était conçue et utilisée de façon à protéger ces renseignements d'un accès non autorisé, et en formulant des recommandations en cas de non-conformité.

15. À mon avis, les principaux objets sont les suivants :

    a. la mise en œuvre de la fonction de rapports d'incidents sur la plateforme SharePoint;
    b. la réponse d'ANB à l'atteinte, en l'occurrence :
        i) la maîtrise de l'atteinte à la vie privée,
        ii) la notification des personnes physiques concernées,
        iii) l'enquête d'ANB,
        iv) les mesures correctives.

16. Avant d'aborder les principaux objets, il convient de commenter brièvement la nature de la coopération d'ANB avec le Bureau de l'ombud. Comme il a été indiqué, ANB était tenue par la loi d'informer l'ombud de l'atteinte et de lui fournir de l'information sur les circonstances dans lesquelles celle-ci était survenue. Outre l'information figurant sur le formulaire de déclaration initial de l'atteinte qui lui avait été fourni par le Bureau de l'ombud, l'organisme a dû répondre à une myriade de questions soumises par le Bureau sur une période de plusieurs mois, dans des circonstances difficiles en raison d'un changement du personnel d'ANB chargé d'y répondre. Malgré les difficultés, la coopération d'ANB a été excellente tout au long de l'enquête, et ce, bien qu'il ait certainement été évident pour elle que certaines réponses ne donneraient probablement pas lieu à un rapport favorable à l'issue de cette enquête. Soulignons que la plupart des faits à la base même du présent rapport ont été fournis par le personnel d'ANB en réponse à des questions exploratoires émanant du Bureau de l'ombud.

a) La mise en œuvre de la fonction de rapports d'incidents sur la plateforme SharePoint

17. Les circonstances entourant la mise en œuvre de la fonction de rapports d'incidents sur la plateforme SharePoint, qui permet aux employés de déposer des rapports d'incidents opérationnels ou rapports liés à la sécurité des patients, ont déjà été décrites dans la section « Contexte » du présent rapport.

18. En ce qui a trait aux questions concernant les directives données par la direction d'ANB à son unité des TI, chargée de mettre en œuvre ce système intranet, j'ai été informé qu'ANB ne pouvait répondre, car il n'y avait aucune trace des directives en question, et que le membre du personnel chargé de la mise en œuvre du système avait quitté l'organisme il y a un certain temps déjà.

19. À la lumière de l'information fournie ou de l'absence d'information, deux raisons pourraient expliquer l'incapacité d'ANB à fournir un système intranet à la hauteur de son obligation en tant que dépositaire de renseignements personnels : d'une part, les directives n'étaient tout simplement pas suffisantes pour faire comprendre à l'unité des TI ce qui était requis et attendu afin de contrôler l'accès non autorisé ou, d'autre part, le personnel de l'unité ne possédait simplement pas les qualifications nécessaires pour suivre les directives appropriées, à supposer que de telles directives aient été données.

20. Quoi qu'il en soit, les faits sont qu'ANB a utilisé pendant des années d'un système de rapports d'incidents en ligne qui permettait, à son insu, un accès non autorisé aux formulaires de rapports remplis par tous les utilisateurs autorisés sur le site intranet qui savaient comment exploiter la porte dérobée.

21. On pourrait bien sûr faire valoir que les renseignements personnels figurant dans les rapports d'incidents opérationnels se limitent généralement au nom de l'auteur du rapport et à d'autres détails insignifiants. Il n'en reste pas moins que l'accès illégal par un employé peut aussi permettre à cet employé de consulter et de communiquer les rapports d'un collègue relativement à la sécurité des patients. Comme il a été mentionné déjà, bien que l'information concernant les patients dans ces rapports soit anonymisée, l'auteur d'un rapport pourrait fort bien fournir des renseignements sur sa propre santé (ou celle d'un autre employé identifié) lorsqu'il signale des incidents ayant eu un effet sur les soins prodigués aux patients pendant leur transport par les travailleurs paramédicaux, par exemple.

22. La fonction de rapports d'incidents comportait une autre omission importante : il n'existait pas de capacité de journal d'audit qui eut permis d'identifier les employés à l'origine de ces accès illégaux, ANB se trouvant ainsi privée d'un outil important pour mener une enquête appropriée.

23. ANB a expliqué qu'il avait été décidé dès le départ de renoncer à la mise en place d'une telle capacité, car cela obligeait le système à assurer un suivi de tout ce qui se trouvait sur la plateforme et à recueillir des données inutiles, qui ne pourraient être supprimées. Cette collecte de données aurait tout simplement été trop volumineuse pour l'espace dont disposait le système. Bien entendu, si ANB avait été dotée dès le départ d'un système infaillible contre les accès non autorisés, il n'aurait peut-être pas été nécessaire d'y intégrer une capacité de journal d'audit pour aider à la détection des accès illégaux.

24. Dans le cas présent, l'absence d'une capacité de journal d'audit dans le système a eu de vastes répercussions. Hormis l'employé qui avait signalé l'existence de la « porte dérobée », ANB n'a pas été en mesure de déterminer combien d'intrus avaient profité de la faille, qui ils étaient, la nature des renseignements personnels qui avaient été consultés et communiqués ni pendant combien de temps la « porte dérobée » avait été utilisée au fil des ans.

25. J'estime que, dans la mise en œuvre de son système de rapports d'incidents, ANB a failli à son obligation d'intégrer le degré de protection nécessaire à la protection des renseignements personnels dont elle avait la garde et le contrôle.

v) La réponse d'ANB à l'atteinte, en l'occurrence :

i) La maîtrise de l'atteinte

26. Lorsqu'une atteinte à la vie privée est découverte, les organismes publics doivent immédiatement prendre des mesures pour la maîtriser dans toute la mesure du possible, afin de réduire l'exposition des renseignements personnels concernés et le préjudice potentiel susceptible de résulter d'en résulter.

27. Après avoir découvert l'atteinte, ANB a immédiatement alerté son personnel informatique interne, qui a pu modifier les autorisations d'accès afin d'empêcher les employés non désignés de consulter les rapports d'incidents opérationnels et rapport liés à la sécurité des patients; ce qui semble avoir été une mesure très simple a empêché tout autre accès non autorisé.

28. À mon avis, ANB a réagi de façon adéquate pour maîtriser l'atteinte dès qu'elle a été informée de la situation.

ii) La notification des personnes physiques concernées

29. Les organismes publics sont tenus, en vertu de l'alinéa 4.2(4)*c*) du *Règlement*, d'aviser dans les meilleurs délais une personne touchée par une atteinte à la vie privée « s'il est raisonnable de croire, dans les circonstances, qu'elle présente un risque de préjudice grave à son endroit ».

30. Le *Règlement* fournit les indications suivantes pour évaluer si les circonstances d'une atteinte la vie privée entraînent un risque de préjudice grave pour l'intéressé :

> 4.2(5) Les éléments servant à établir si une atteinte à la vie privée présente un risque de préjudice grave à l'endroit de l'intéressé sont notamment :
>
> a) le degré de sensibilité des renseignements personnels en question;
>
> b) la probabilité qu'on fait, qu'on a fait ou qu'on fera une utilisation abusive de ces renseignements personnels.

31. L'obligation d'aviser les personnes physiques concernées en cas d'atteinte à leur vie privée repose sur le principe selon lequel les gens ont le droit de savoir si leurs renseignements personnels ont été compromis et de prendre les mesures qu'ils jugent appropriées pour se protéger contre le préjudice potentiel résultant de l'atteinte.

32. Bien que le *Règlement* ne précise pas quels renseignements doivent être fournis aux fins de notification des personnes concernées par une atteinte à la vie privée, il faudrait en général inclure : une description de ce qui s'est passé, y compris la description détaillée des renseignements personnels concernés; une explication des types de préjudices susceptibles de résulter de l'atteinte; les mesures que peut prendre la personne pour atténuer le préjudice potentiel; le nom et les coordonnées d'une personne désignée par l'organisme public pour répondre aux questions concernant l'atteinte et les pratiques de l'organisme public en matière d'information; une notification du droit de déposer une plainte auprès du Bureau de l'ombud; une reconnaissance de l'incidence potentielle de l'atteinte; les mesures prises par l'organisme public pour prévenir d'autres atteintes similaires (mesures correctives).

33. Dans le cas présent, les responsables des ressources humaines d'ANB ont informé les deux employés concernés par téléphone dans les deux semaines qui ont suivi la découverte de l'atteinte. ANB a expliqué que la notification avait été quelque peu retardée pour permettre l'identification du document en question et la confirmation de l'identité des employés touchés. L'organisme dit avoir informé les deux employés de ce qui s'était passé, de la façon dont cela s'était passé, des mesures prises pour corriger la situation et du droit de déposer une plainte pour atteinte à la vie privée auprès du Bureau de l'ombud.

34. Sur la base de ce qui précède, j'estime qu'ANB a procédé à une notification appropriée en temps opportun.

iii) L'enquête d'ANB

35. Il est important d'enquêter sur les atteintes à la vie privée afin de comprendre ce qui s'est passé et de cerner les mesures supplémentaires à adopter pour éviter qu'une telle situation se reproduise. Les organismes publics sont tenus de mener des enquêtes sur toutes les atteintes à la vie privée signalées, conformément au paragraphe 4.2(4) du *Règlement*. Lorsqu'ils enquêtent sur les atteintes, les organismes publics ne doivent pas seulement

chercher à en déterminer les circonstances et les causes, mais aussi examiner les mesures de protection, les politiques et les procédures applicables pour déterminer s'il existe des lacunes en matière de conformité et des possibilités de mieux traiter et protéger les renseignements personnels.

36. Comme il a déjà été mentionné, l'incapacité d'ANB à mener une enquête sérieuse sur l'identité des intrus s'explique en grande partie par sa décision de ne pas inclure de capacité de journal d'audit dans son programme intranet. L'organisme s'est, de se fait, trouvé privé de renseignements nécessaires, en termes de contexte factuel, pour justifier une intrusion dans les courriels et les journaux d'impression de ses employés.

37. Cela dit, ANB a interrogé l'employé qui avait eu le bon sens de reconnaître l'irrégularité de la situation et de la signaler. Ce faisant, l'organisme a appris que c'est un autre employé qui l'avait informé de la marche à suivre pour accéder aux rapports de collègues par cette « porte dérobée ». L'employé à l'origine du signalement a également fait savoir à ANB que la vulnérabilité semblait connue du personnel depuis un certain temps déjà.

38. Sur la base de l'information fournie par ANB, rien n'indique que le nom de l'employé qui avait informé l'employé déclarant de l'existence de la porte dérobée ait été communiqué à l'organisme, ou que des efforts aient été déployés pour interroger d'autres employés au sujet de ces accès non autorisés.

39. À mon avis, les efforts d'ANB pour mener une enquête sérieuse ne sauraient être qualifiés que de timides; il ne s'agissait certainement pas du genre d'enquête qui eut pu permettre de déterminer l'identité des employés susceptibles d'avoir consulté et communiqué des renseignements personnels sans rapport avec leur travail.

40. ANB ne saura jamais (et les victimes de cet accès illégal non plus) combien de ses employés ont consulté et communiqué les renseignements personnels sensibles dans cette affaire.

iv) Les mesures correctives

41. Un aspect clé de la réponse à une atteinte à la vie privée consiste à trouver et à mettre en œuvre des mesures qui empêcheront des atteintes similaires de survenir, ou permettront de les atténuer. Une fois qu'une atteinte est survenue, il n'y a aucun moyen de revenir en arrière, mais cela donne l'occasion à un organisme public de tirer des leçons de ce qui s'est produit et d'améliorer ses pratiques en conséquence. Souvent, les atteintes à la vie privée mettent en lumière des politiques ou des procédures obsolètes ou inefficaces, des lacunes dans les mesures de sécurité, la nécessité d'une éducation et d'une formation nouvelles ou supplémentaires des employés en matière de protection de la vie privée, ainsi que d'autres problèmes de conformité.

42. ANB avait en fait déjà adopté des politiques et des procédures solides avant cette atteinte. Par exemple, sa politique intitulée « Politique d'entreprise – sécurité des technologies de l'information : Contrôle d'accès », mise en œuvre en 2016, fournit des directives pertinentes pour assurer des examens de l'accès à ses systèmes au moins une fois par an, et pour l'exécution d'examens réguliers des privilèges d'accès à tous les systèmes utilisés par les employés, afin de déceler et d'éliminer les accès inappropriés.

43. Les employés sont également tenus de signer, lors de leur embauche, une déclaration de confidentialité dans laquelle ils s'engagent à respecter la confidentialité des patients et des autres employés, à n'accéder qu'à l'information nécessaire à leur travail et à respecter les politiques et les procédures relatives à la vie privée et à la protection des renseignements personnels.

44. ANB dispose par ailleurs d'une politique de confidentialité interne (la politique 3115), qui exige des employés qu'ils n'accèdent qu'à l'information confidentielle nécessaire à l'exécution des tâches qui leur sont confiées et qu'ils signalent à la direction et au responsable de la confidentialité et de l'accès à l'information tous les incidents liés à la protection de la vie privée ainsi toutes les atteintes, connus ou suspectés.

45. ANB a expliqué qu'elle exigeait aussi de ses employés, comme condition d'emploi, qu'ils suivent une formation à la protection de la vie privée consistant en un module de formation sur le sujet, qui fait partie du processus d'orientation des nouveaux employés. Les employés sont en outre tenus de suivre un module en ligne sur les incidents et les atteintes à la vie privée, ainsi que ceux ayant trait à la sécurité. ANB a indiqué qu'elle n'avait pas instauré de formation annuelle à la protection de la vie privée pour les employés, mais comptait mettre en œuvre des programmes de mise à jour annuelle basés sur ces modules.

46. En termes de garanties d'ordre administratif, on peut dire que les politiques internes mises en œuvre par ANB relativement aux autorisations et aux contrôles d'accès sont conformes aux exigences législatives et réglementaires créant de nouvelles responsabilités en matière de pratiques d'information et de garanties qui sont entrées en vigueur le 1er avril 2018 (voir l'annexe B pour les politiques internes adoptées par ANB).

47. En vertu des dispositions législatives et réglementaires susmentionnées, les organismes publics sont tenus d'établir des pratiques en matière d'information et de protéger les renseignements personnels en prenant des mesures de sécurité raisonnables contre l'accès, l'utilisation, la communication ou l'élimination non autorisés des renseignements personnels. Ils doivent également veiller à ce que les dirigeants, les administrateurs et les employés se conforment aux dispositions de sécurité et tester et évaluer périodiquement l'efficacité des mesures de protection adoptées (voir l'annexe A).

48. À la lecture de ce rapport, il devrait être assez évident que le problème est apparu quelque sept ans avant la découverte de la « porte dérobée », et que les questions et les tests appropriés pour s'assurer que toutes les garanties étaient en place afin de protéger les renseignements personnels de toute consultation et communication illicites n'ont tout simplement pas été posées/effectués. Comme l'a expliqué ANB, ce manque de diligence de sa part s'est produit avant même qu'un responsable de la protection de la vie privée ne soit désigné pour veiller au respect des exigences de la *Loi* et du *Règlement*. ANB n'a pu trouver aucune documentation quant à la façon dont les contrôles d'accès avaient été mis en place, ou qui permettrait d'établir si une évaluation des facteurs relatifs à la vie privée avait été réalisée à l'époque.

49. Comme il a été indiqué déjà, ANB n'a pas été en mesure de déterminer quels employés auraient pu contribuer à l'atteinte en accédant de façon inappropriée à la plainte et (ou) en parlant de cette dernière à d'autres employés. Par mesure de précaution, la direction d'ANB a transmis une note à l'ensemble du personnel la semaine suivant la notification des employés concernés par l'atteinte, afin de rappeler les obligations découlant de l'entente de confidentialité que tous les employés sont tenus de signer lors de leur embauche et annuellement par la suite. La note indiquait qu'il y avait eu, récemment, plusieurs incidents et atteintes à la vie privée impliquant la communication des renseignements personnels de collègues et la recherche et la communication de renseignements personnels sans qu'il y ait réellement besoin que ceux-ci soient connus. Elle rappelait également au personnel qu'il est de la responsabilité de chacun de prendre des mesures immédiates pour maîtriser une atteinte à la vie privée présumée ou avérée et de signaler la situation à la direction.

50. En l'état actuel des choses, il est clair que les contrôles d'accès n'ont pas été testés ni n'ont fait l'objet d'une vérification au moment de la mise en place du système, et qu'ils n'ont probablement jamais été vérifiés ni testés jusqu'à la découverte de l'atteinte. Comme il a été mentionné, compte tenu de l'absence de capacité d'audit et de l'absence de tests des contrôles d'accès au site intranet, il est désormais impossible de savoir si d'autres violations ont été commises. Au bout du compte, au fil des ans, les politiques et procédures d'ANB en matière de garanties administratives se sont révélées inefficaces, parce qu'elles n'étaient pas mises en pratique et respectées.

51. Comme ANB n'a pas été en mesure de déterminer quels employés pourraient avoir joué un rôle dans l'atteinte, j'estime que les mesures correctives adoptées par l'organisme en réponse à cette atteinte étaient inadéquates, pour les raisons susmentionnées.

E. Conclusions

52. Dans le cadre de la présente affaire, l'atteinte à la vie privée aurait pu être évitée si les contrôles d'accès au système de rapports d'incidents opérationnels avaient été vérifiés et testés lors de la mise en place du système et, à défaut, si des examens réguliers et approfondis

des autorisations d'accès au système avaient été effectués. Comme il semble que cela n'ait pas été fait, et que le problème n'a été mis en lumière que lorsque l'atteinte a été découverte, il est possible que le système ait permis un accès complet à tous les rapports d'incidents remplis, puisqu'il était configuré de façon à ce que les employés qui savaient comment manipuler les options puissent obtenir l'accès à l'information en question.

53. Il est impossible de savoir si d'autres atteintes à la vie privée ont ainsi pu survenir, étant donné que la capacité de journal d'audit du système n'était pas activée, et qu'il n'existait donc aucun moyen de vérifier qui avait accédé aux renseignements qui s'y trouvaient contenus.

54. Les failles dans les autorisations d'accès et l'absence d'une fonction d'audit ont entravé la capacité d'ANB à enquêter de façon approfondie sur l'étendue de l'atteinte dans le cas présent et, de ce fait, à déterminer qui parmi ses employés pourrait avoir contribué à la violation pour aborder directement la gravité de la situation avec les personnes concernées. Cette situation est très préoccupante, car il semble que des employés aient abusé de l'accès au système pour consulter des renseignements auxquels ils n'auraient pas dû avoir accès, voir même communiqué ces renseignements à d'autres employés en les encourageant à faire de même.

55. Plus inquiétant encore : au moins certains des employés concernés par l'atteinte étaient des travailleurs paramédicaux, c'est-à-dire des professionnels de la santé titulaires d'un permis de l'Association des paramédics du Nouveau-Brunswick et assujettis, de ce fait, à des normes de pratique établies ainsi qu'à un code de déontologie, qui traitent tous deux de l'obligation de préserver la confidentialité et d'établir et de maintenir des relations professionnelles.

56. Sur la base de ce qui précède, mes conclusions sont les suivantes :

- une atteinte à la vie privée est survenue, concernant les renseignements personnels des deux employés touchés par la plainte déposée par l'intermédiaire de la plateforme de rapports d'incidents sur SharePoint;
- les efforts déployés par ANB pour maîtriser l'atteinte ont été suffisants;
- ANB a notifié en temps opportun, de façon appropriée, les personnes physiques concernées et le Bureau de l'ombud;
- l'enquête d'ANB sur l'atteinte à la vie privée était inadéquate;
- bien qu'ANB ait mis en place de solides politiques et procédures en matière de protection de la vie privée et de sécurité, ces dernières n'ont pas toujours été respectées, ce qui a contribué aux circonstances ayant permis à l'atteinte à la vie privée de survenir;
- la mise en œuvre par ANB du système de rapports d'incidents était inadéquate au sens où l'organisme n'a pas offert les garanties nécessaires pour protéger les renseignements personnels qui se trouvaient en sa possession et sous son contrôle.

57. Au cours de cette enquête, ANB a fait savoir qu'elle prévoyait opérer la transition de sa plateforme intranet interne vers la nouvelle plateforme SharePoint Online, et qu'un nouveau système de rapports d'incidents serait mis en place séparément. Une fois que ces nouvelles initiatives seront opérationnelles, ANB a déclaré que les employés ne présenteraient plus de rapports par l'intermédiaire de la plateforme SharePoint. L'organisme a indiqué qu'une évaluation des facteurs relatifs à la vie privée (EFVP) serait réalisée pour le nouveau système, et que des contrôles d'accès seraient mis en place sur la base des principes du droit d'accès et du privilège minimaux.

58. Je me réjouis qu'ANB prenne des mesures pour mettre à jour ses systèmes internes et procède de façon proactive à une EFVP, dès le départ, ce qui devrait permettre de cerner les problèmes de sécurité et de respect de la vie privée, de sorte que l'organisme puisse les résoudre avant la mise en œuvre du nouveau système. Les enseignements tirés de la présente affaire devraient permettre de réduire le risque qu'une atteinte similaire se reproduise.

F. Recommandations

59. Je recommande que le personnel d'ANB informe le responsable de la protection de la vie privée et de l'accès à l'information dès qu'il a connaissance d'un comportement inapproprié susceptible d'impliquer des renseignements personnels.

60. Je recommande à ANB de revoir ses autorisations d'accès à tous les systèmes où se trouvent des renseignements personnels dans son intranet, et ce, au moins une fois par an, comme le veut la politique de contrôle d'accès d'ANB.

61. Je recommande qu'avant de mettre en œuvre tout nouveau système ou toute nouvelle plateforme par où transiteront des renseignements personnels, y compris des renseignements personnels sur la santé, ANB procède à une EFVP, consistant notamment à déterminer quels sont les contrôles et à les tester, dans le but de vérifier que des autorisations d'accès adéquates sont en place. L'EFVP devrait également explorer et encourager l'établissement d'une capacité de journal d'audit pour tous les systèmes susmentionnés.

62. Je recommande à ANB d'élaborer et de mettre en œuvre une formation annuelle sur la protection de la vie privée, ainsi que des mises à niveau et des rappels réguliers pour tous les employés.

63. En ce qui concerne le nouveau système de rapports d'incidents, je recommande qu'ANB fournisse au Bureau de l'ombud une copie de l'EFVP et une confirmation des mesures qui seront ou ont déjà été prises pour vérifier les privilèges d'accès, conformément aux obligations d'ANB en vertu du paragraphe 48.1(1) de la *Loi* et de l'article 4.2 du *Règlement*.

64. Je recommande également qu'ANB confirme au Bureau de l'ombud son acceptation des recommandations susmentionnées et, le cas échéant, l'état de leur mise en œuvre d'ici le 10 juillet 2023.

65. Dans certains cas, il n'y a pas lieu de publier le rapport d'enquête sur le site Web de l'ombud. Dans le cas présent, cependant, les circonstances dans lesquelles l'atteinte est survenue s'inscrivent en faveur de cette publication, car bon nombre d'organismes publics dépositaires de renseignements personnels utilisent une plateforme Sharepoint. La publication du rapport pourrait rappeler aux organismes publics de revoir leur système afin d'inclure les mesures nécessaires pour protéger ces renseignements d'un accès non autorisé.

Le tout respectueusement soumis,

L'honorable Alexandre Deschênes, C.R.

Fait à Fredericton,

Province du Nouveau-Brunswick

Le 10^{e} jour de mai 2023