Report of Findings under the *Right to Information and Protection of Privacy Act*

by

The Honourable Alexandre Deschênes, K.C.

Delegate for the Ombud of the Province of New Brunswick

May 10, 2023

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

A. Introduction

1. This investigation arises out of a privacy breach reported by Ambulance New Brunswick (EM/ANB Inc. referred to as ANB) to the New Brunswick Ombud on February 7, 2022. Under s. 4.2(4)(d) of Regulation 2010-111 (the *Regulation*) adopted under the *Right to Information and Protection of Privacy Act* (unless otherwise indicated, the *Act*), ANB had a statutory obligation to report the privacy breach. The Ombud determined that a formal investigation was warranted and informed ANB accordingly on July 8, 2022. In August 2022, the Ombud designated me under s. 9 of the *Ombud Act* to act on her behalf with respect to the investigation as she was of the view that she was in a conflict of interest in the matter.

B. Background

2. Seven years prior to the reported breach, ANB mandated its own Information Technology employees (IT unit) to devise an intranet site using a SharePoint platform. Employees such as paramedics, with their unique ID and password, would log onto this intranet site and file Operations Internal/External incident reports and Patient Safety Incident reports. The reports filed by ANB staff would be provided only to seven designated ANB management and staff. An essential feature of this reporting system would not allow non-designated employees to have access to reports filed by other employees. The reports filed by paramedics within their own space could relate to incidents ranging from accidents or mechanical problems involving an ambulance (Operations incident reports) to any incident related to or which could impact on patient care such as a fall or error in medication (Patient Safety Incident reports).

3. In late December 2021, a newly employed paramedic used the Operations incident report section of the intranet site to file a complaint by providing a report of a highly sensitive incident involving another employee in the course of employment. As recommended by ANB to all employees, complaints or reports of a sensitive nature such as the one in question would usually be dealt with by ANB's Human Resources department and not by using the intranet site to report operational incidents. However, the fact that ANB's recommendation was not followed by the complainant in this case does not in any way detract from ANB's duties and responsibilities as a custodian of personal information found in its incident and patient safety reports.

4. The privacy breach occurred in this case when, more than a month after the complaint containing the sensitive information was filed as an incident report, a paramedic, prompted by another paramedic, used a "backdoor vulnerability" in the system to gain access and view the incident report/complaint. The unauthorized access was reported to management by the employee who had just been told how to use the "back door" which, up to that point, was unknown to ANB management. Of course, ANB immediately locked down unauthorized access to all completed reports in the system by changing the access controls. The "backdoor vulnerability" was eliminated. For those who might be interested, employees could access the reports filed by others by clicking the "employee corner" tab, clicking the "site action" and then the "manage content and structure" tabs which would then allow them to scroll

through the list of all the filed reports. ANB blocked the unauthorized access by removing the access to the "manage content" section which was supposed to be used only by the Site Owner to move, delete and copy documents within the site.

5. ANB then undertook an internal investigation into the causes and scope of the breach and notified the two affected employees as well as the Office of the Ombud. In reporting the breach, ANB indicated that the breach involved unauthorized access and disclosure of personal information. As it turns out, the lack of logging capacity allowing ANB to know who was accessing the reports other than the author of a report was another major deficiency in the system. More will be said later on this point.

6. The Ombud has the power, on her own initiative, to investigate this self-reported breach in order to evaluate the level of conformity with Part 3 of the *Act* dealing with the protection of privacy by a public body and in particular its obligation to protect personal information by making reasonable security arrangements against unauthorized access, use, disclosure or disposal of such information in accordance with the *Act* and the *Regulation* (see ss. 48.1(1) and 64.1(1)(g) of the *Act*).

C. Jurisdiction

7. ANB is a **public body** as defined in s. 1 of the *Act* as it is a **local public body** which includes a **health care body** which, in turn, includes "any other body listed in Part III of the First Schedule of the *Public Service Labour Relations Act*. EM/ANB Inc. is listed therein. As such, ANB is subject to the same obligations as other public bodies with respect to the handling of personal information under the *Act* and the *Regulation.*

8. ANB is also a health care custodian with respect to personal health information under the *Personal Health Information Privacy and Access Act*. The unlawfully viewed information by way of unauthorized access **in this case** is not targeted by the legislation just mentioned but is certainly personal information under s. 1 of the *Act* as it contained the names of the two employees involved and the aggrieved employee's version of events as detailed in the complaint. However, my view is that some discussion on the issue of the possible disclosure of personal health information is warranted by reason of ANB's incapacity to log unauthorized access to its intranet reporting system which includes reports in the "patient safety incidents" section which could, of course, contain personal health information. That is so because the definition of "personal information" under the Act includes "personal health information about the individual". The information provided in a paramedic's patient safety incident report, for example, may contain personal information about the paramedic herself or himself (i.e., extreme stress or fatigue of the reporting paramedic while being in charge of a non-identifiable patient during transportation). Any unauthorized access would allow the viewing and disclosure of that personal health information not about the non-identifiable patient but about the reporting paramedic.

9. The Ombud now has responsibilities described under the *Act* which include the power to investigate and report on matters involving the unauthorized access and disclosure of personal information by employees of public bodies including the unauthorized access and disclosure of personal health information. Of course, that power also exists under the *Personal Health Information Privacy and Access Act*.

10. In this case, ANB's own policies and directives to its employees including its report to the Office of the Ombud make it abundantly clear that the access to and disclosure of the reported incident/complaint by other employees was unauthorized as it involved access and disclosure of personal information beyond what was necessary for their work-related duties. These unauthorized accesses may constitute a provincial offense described in the *Act* and are certainly subject to disciplinary measures.

11. In terms of the Ombud's jurisdiction, there is no question that the Ombud has the power to investigate and report the facts surrounding this serious breach of personal information and to make the appropriate recommendations (see s. 64.1(1)(g) of the *Act*). As a delegate of the Ombud under s.9 of the *Ombud Act* I now have the same power to investigate and report.

D. Issues

12. Apart from the question of jurisdiction of the Ombud to investigate this breach of privacy, the issues in this investigation must revolve around ANB's duties and responsibilities as a custodian of personal information which are, in turn, mostly informed by ANB's internal policies, the *Act*, and the *Regulation.* During the course of this report, reference will often be made to provisions of the *Act* or the *Regulation* without reproducing them. The relevant provisions can be found in Appendix A to this report.

13. In general terms, the relevant provisions of the *Act* and the *Regulation* adopted thereunder make it mandatory for ANB to initiate security arrangements to control unauthorized access including recording and monitoring access to such information. In addition, apart from adopting policies requiring that all employees comply with its security arrangements, ANB was and is required to periodically test and evaluate the effectiveness of the security arrangements implemented.

14. When a privacy breach is reported to the Office of the Ombud by a public body, the primary role of this independent oversight body is to determine whether the reported circumstances demonstrate that a privacy breach occurred, and if so, to review and assess whether the public body undertook appropriate steps to investigate and respond to the situation. In this case, this investigation must also determine if ANB met its obligation at the outset to ensure that, as custodian of personal and personal health information, the SharePoint platform to be used by employees was devised and used in such a way as to protect such information from unauthorized access and to make recommendations in the case of non-compliance.

15. In my view, the main issues are as follows:

    a. the implementation of the incident reporting function on the SharePoint platform.
    b. ANB's response to the breach:
        i) containment of the breach;
        ii) notification of the affected individuals;
        iii) ANB's investigation; and
        iv) corrective measures.

16. Before dealing with the main issues, some comments are warranted with respect to the nature of ANB's cooperation with the Ombud's office. As noted, ANB was required by statute to inform the Ombud of the breach and to provide the Office with information with respect to the circumstances of the breach. Apart from the information found on the initial breach reporting form supplied by the Office, ANB had to respond to a myriad of questions submitted by the Ombud's office over the course of many months and under difficult circumstances due to a change of ANB personnel tasked with providing the answers. Despite the difficulties, ANB's cooperation throughout was excellent even though it must certainly have been obvious to ANB that some of the answers were not conducive to a favorable report resulting from this investigation. It should be noted here that most of the facts which form the backbone of this report were provided by ANB staff responding to probing questions emanating from the Ombud's office.

a) The implementation of the incident reporting function on the SharePoint platform

17. The circumstances surrounding the implementation of the incident reporting function on the SharePoint platform for employees to file operational incident or patient safety reports have already been described in the Background portion of this report.

18. In response to questions pertaining to the directives given by ANB management to its IT unit tasked with the responsibility to implement this intranet system, I was informed that ANB could not answer those questions as there was no record of it and the employee in charge of implementing the system had left ANB quite some time ago.

19. On the basis of the information provided or lack thereof, there are two possible reasons that could explain ANB's failure to provide an intranet system commensurate with its obligation as a custodian of personal information: one, the directives were simply not sufficient to convey the required message to the IT unit of what was required and expected in order to control unauthorized access or, two, the IT unit personnel simply did not have the qualifications to follow proper directives, assuming such were given.

20. Be that as it may, the facts are that ANB, for years, was equipped with an online incident reporting system which, unbeknownst to it, allowed unauthorized access to completed incident reporting forms by all authorized users on the intranet site who knew how to exploit the backdoor vulnerability.

21. Of course, one might say that the type of personal information found in the operational incident reports would generally be confined to the name of the author of the report and other insignificant details. On the other hand, an employee's unlawful access might also allow a view and disclosure of another employee's patient safety reports. As mentioned, although there are no identifiers pertaining to the personal information of a patient in such reports, the author of the reports might well provide health information about himself or herself (or another identified employee) in reporting incidents impacting on patient care while being transported by paramedics, for example.

22. The incident reporting function featured another significant oversight: there existed no audit log capacity to allow identification of employees who perpetrated these unlawful accesses which, of course, deprived ANB of an important tool to pursue a proper investigation.

23. ANB explained that such a decision was made at the outset to dispense with setting up such audit log capacity because it required the system to track everything on the platform and collect unnecessary data which could not be deleted. This collection of data would simply be too voluminous for the space the system could handle. Of course, if ANB had been provided at the outset with an iron-clad system against unauthorized access, there might be no need to be equipped with an audit log capacity to help detect unlawful accesses.

24. The absence of an audit log capacity in the system had huge implications in this case. Apart from the employee who reported the existence of the "backdoor" access, ANB was unable to determine who and how many intruders were involved, the nature of the personal information that had been viewed and disclosed and how long the "backdoor" had been used over the years.

25. I find that in the implementation of its incident reporting system, ANB failed in its obligation to incorporate the degree of safeguards necessary for the protection of personal information under its custody and control.

b) ANB's response to the breach

i) Containment of the breach

26. When a privacy breach is discovered, public bodies should immediately take steps to contain the breach to the fullest extent possible in order to reduce the exposure of the personal information involved and the potential harm that could result from the breach.

27. Upon discovering the breach, ANB immediately alerted its internal IT staff who were able to change the access permissions to block non-designated employees from being able to view any completed operational incident and patient safety reports. What appears to have been a very simple step prevented any unauthorized access from that point forward.

28. In my view, ANB responded adequately to contain the breach upon being informed of the situation.

ii) Notification of the affected individuals

29. Public bodies are required under s. 4.2(4)(c) of the *Regulation* to notify a person affected by a privacy breach as soon as possible "if it is reasonable in the circumstances to believe that the privacy breach creates a risk of significant harm to that person".

30. The *Regulation* provides the following guidance to assess whether the circumstances of a privacy breach give rise to a risk of significant harm for the affected individual:

> 4.2(5) The factors that are relevant to determining whether a privacy breach creates a risk of significant harm to the person include
>
> (a) the sensitivity of the personal information involved in the breach, and
>
> (b) the probability that the personal information has been, is being, or will be misused.

31. The requirement to notify individuals when their privacy has been breached is based on the premise that people have the right to know if their personal information has been compromised and to allow them to take the steps they deem appropriate to protect themselves from the potential harm that result from the breach.

32. While the *Regulation* is silent on what information is to be provided in notifying the affected individuals of a privacy breach, as a best practice, a notice should generally include: a description of what occurred, including a detailed description of the personal information involved; an explanation of the possible types of harm that could occur as a result of the breach; steps the individual can take to mitigate the potential harm; the name and contact information of a person designated by the public body to answer questions about the breach and the public body's information practices; a notice of the right to complain to the Office of the Ombud; a recognition of the potential impact(s) of the breach; and the steps the public body is taking to prevent similar breaches (corrective measures).

33. In this case, ANB human resource officials notified the two affected employees by telephone within two weeks of the breach being discovered. ANB explained that there was a brief delay in notifying them to allow time to ensure that it had identified the document in question and confirm the identities of the employees whose information was involved. ANB indicated that

it advised both employees of what occurred, how it occurred, what steps had been taken to correct the situation, and of the right to file a privacy complaint with the Office of the Ombud.

34. Based on the above, I find that ANB provided appropriate and timely notification.

iii) ANB's investigation

35. Investigating privacy breaches is important to understand what happened and to identify any additional steps that should be taken to prevent a similar recurrence in the future. Public bodies are required to conduct investigations of every reported privacy breach as per s. 4.2(4) of the *Regulation*. In investigating privacy breaches, public bodies should not only be looking at determining the circumstances and causes of the breach, but also reviewing the applicable safeguards, policies and procedures to determine if there are any compliance gaps and opportunities to better handle and protect personal information.

36. As mentioned above, ANB's inability to carry on a meaningful investigation of the identity of intruders was greatly hampered by its decision not to opt for an audit log capacity in its intranet program. As a result, ANB was deprived of the necessary information in terms of factual background to justify an intrusion into its employees' emails and printer logs.

37. That being said, ANB interviewed the employee who had the common sense to recognize the impropriety of what was being done and to report it. In interviewing the reporting employee, ANB learned that another employee had informed them on how to access the reports of other employees through this "back door". The reporting employee also informed ANB that it appeared that the backdoor vulnerability had been known amongst staff for some time.

38. On the basis of the information provided by ANB, there is no evidence to indicate that the name of the employee who had informed the reporting employee about the back door access was even provided to ANB or that efforts were made to interview other employees with respect to these unauthorized accesses.

39. In my view, ANB's efforts to pursue a meaningful investigation can only be classified as timid and certainly not one that could lead to the identity of the employees who might have viewed and disclosed personal information that had nothing to do with necessary work-related information.

40. ANB will never know (and neither will the victims of this unlawful access) how many of its employees viewed and disclosed the sensitive personal information in this case.

iv) Corrective measures

41. A key part of responding to a privacy breach is to identify and implement measures that will minimize or prevent similar breaches from occurring in the future. Once a breach has occurred, there is no way to change this fact, but it provides an opportunity for a public body to learn from what took place and to improve its practices accordingly. Oftentimes, privacy breaches will bring to light outdated or ineffective policies or procedures, gaps in security safeguards, the need for new or additional privacy education and training for employees, and other compliance issues.

42. ANB had in fact adopted strong policies and procedures prior to this reported privacy breach. For example, its "Information Technology Corporate Policy on Access Control" implemented in 2016 provides relevant directives to ensure access reviews for their systems on at least an annual basis and to perform regular reviews of access privileges for all systems used by employees to identify and remove inappropriate access.

43. In addition, employees are required to sign a Confidentiality- Declaration of Understanding on hire requiring employees to agree to respect the confidentiality of patients as well as other employees, to only access information required for work-related purposes and to respect policies and procedures related to privacy and the protection of personal information.

44. ANB also has an internal privacy policy (ANB Privacy Policy 3115), which requires employees to only access confidential information needed to perform assigned duties and to report all known or suspected privacy incidents and breaches to management and the Privacy and Information Access Officer.

45. ANB explained that it also requires employees to undertake privacy training as a condition of employment, consisting of a privacy training module that is part of the orientation process for new employees. Employees are also required to complete an online module on privacy and security incidents and breaches. ANB indicated that it did not have annual privacy training for employees in place but that its objective was to implement yearly privacy refreshers based on these modules.

46. In terms of administrative safeguards, it is fair to say that ANB's implemented internal policies dealing with access permissions and controls are in keeping with the legislative and regulatory requirements creating new responsibilities with respect to information practices and security safeguards which came into effect on April 1, 2018 (see Appendix B for ANB's adopted internal policies).

47. These legislative and regulatory provisions require public bodies to establish information practices and to protect personal information by making reasonable security arrangements against unauthorized access, use, disclosure or disposal of personal information. They also

require public bodies to ensure that officers, directors, and employees comply with security arrangements and to periodically test and evaluate the effectiveness of security arrangements (see Appendix A).

48. Reading through this report, it should be somewhat obvious that the problem originated some seven years prior to the discovery of the "backdoor vulnerability" and that the appropriate questions and tests to ensure that all the safeguards were in place to protect personal information from unlawful viewing and disclosure were simply not made. As ANB explained, this lack of diligence on its part took place even before a privacy officer was assigned to oversee compliance with the requirements under the *Act* and the *Regulation*. ANB could not locate any documentation as to how the access controls were set up or whether a privacy impact assessment had been undertaken at the time.

49. As mentioned, ANB was unable to determine which employees may have contributed to the breach by inappropriately accessing the complaint and/or telling other employees about the complaint. As a precautionary measure, ANB management issued a memo to all staff the week after the affected employees were notified of the breach as a general reminder of obligations under the Confidentiality Agreement that all employees were required to sign when hired and on an ongoing annual basis. The memo indicated that there had been various recent privacy incidents and breaches involving the sharing of colleagues' personal information and seeking and sharing personal information outside a need-to-know context. The memo also reminded staff that everyone was responsible to take immediate action to contain a suspected or actual privacy breach and to report the situation to management.

50. As matters now stand, it is clear that access controls were not tested or verified at the time the system was set up and likely were not verified or tested until discovery of the breach. As mentioned, in view of the absence of an audit log capacity combined with the lack of testing of its access controls on the intranet site, it is now impossible to know whether other breaches occurred as a result. The bottom line is that through the years ANB's policies and procedures in terms of administrative safeguards pertaining to personal information were not effective because they were not put into practice and followed.

51. As ANB was unable to determine which employees may have contributed to the breach I find that the corrective measures undertaken by ANB in response to this breach were not adequate for the reasons above.

E. Findings

52. In this case, the privacy breach could have been avoided had the access controls to the operational incident reporting system been verified and tested when it was first set up, and failing that, if regular and thorough reviews of access permissions to the system had been conducted. As it seems this was not done and this issue only came to light when the breach

in this case was discovered, it is possible that the system had been allowing full access to all the completed incident reports since it was set up for the employees who knew how to manipulate the options to gain access to this information.

53. It is impossible to know whether this allowed other privacy breaches to occur, given that the audit log capacity for this system was not enabled and thus there is no way to verify who accessed the information in the system.

54. The flaws in the access permissions and lack of audit capability hindered ANB's ability to thoroughly investigate the extent of the breach in this case, and consequently, to identify those employees who may have contributed to the breach and address the seriousness of the situation with them directly. This is of considerable concern, as it appears that employees may have been abusing access to the system to inappropriately view information to which they should not have been privy and further, sharing this with other employees and encouraging them to do the same.

55. Further, it is of particular concern that at least some of the employees that would seem to have been involved in the breach were paramedics. Paramedics are licensed health care professionals under the Paramedic Association of New Brunswick and thus bound by established Standards of Practice and a Code of Ethics, both of which speak to the obligation to maintain confidentiality and to develop and maintain professional relationships.

56. Based on the above, I find the following:

- a privacy breach occurred involving the personal information of the two employees involved in the reported complaint through the SharePoint incident reporting platform;
- ANB's efforts to contain the privacy breach were adequate;
- ANB provided timely and appropriate notification to the affected individuals and the Office of the Ombud;
- ANB's investigation of the privacy breach was not adequate;
- While ANB has strong privacy and security-related policies and procedures in place, they were not always followed and this contributed to the circumstances that allowed for the privacy breach to occur.
- ANB's implementation of the incident reporting system was inadequate in that it failed to provide the necessary safeguards to protect the personal information in its custody and under its control.

57. During the course of this investigation, ANB advised that it is planning to transition its internal Intranet platform to the new SharePoint Online platform and that a new incident reporting system will be built separately. Once these new initiatives are operational, ANB stated that employees will no longer submit reports through the SharePoint platform. ANB indicated

that a privacy impact assessment (PIA) will be completed for the new system and that access controls will be built in based on the principles of least access and least privilege.

58. I am pleased that ANB is taking measures to update its internal systems and will be proactively conducting a privacy impact assessment (PIA) at the outset, which should help identify security and privacy concerns and allow ANB to address them before the new system is implemented. The lessons learned in this case should reduce the risk of a similar breach occurring again in the future.

F. Recommendations

59. I recommend that ANB staff notify the Privacy and Access Information Officer at the earliest opportunity whenever they become aware of inappropriate behavior that could involve personal information.

60. I recommend that ANB review its access permissions to all systems involving personal information on its Intranet site, and that these be reviewed on at least an annual basis, as set out in ANB's Access Control policy.

61. I recommend that prior to implementing any new systems or platforms involving personal information, including personal health information, ANB conduct a privacy impact assessment that includes identifying and testing access controls to ensure that proper access permissions are in place prior to implementation. The privacy impact assessment should also explore and encourage the enabling of audit logging capacity for all systems that involve personal information.

62. I recommend that ANB develop and implement yearly privacy training as well as regular refreshers and reminders for all employees.

63. As for the new incident reporting system, I recommend that ANB provide the Office of the Ombud with a copy of the completed privacy impact assessment (PIA) and confirmation of the steps that will be or have been taken to verify access privileges in keeping with ANB's requirements under s. 48.1(1) of the *Act* and s. 4.2 of the *Regulation.*

64. I recommend that ANB provide the Office of the Ombud with confirmation of whether it accepts the above recommendations, and if so, the status of the implementation of the above by July 10, 2023.

65. In some cases, the report of an investigation does not warrant a publication on the Ombud's Website. The circumstances of the privacy breach in this case calls for such a publication in large measure because of the use of the Sharepoint platform by many public bodies as custodian of personal and health information. The publication of this report may serve as a

wake-up call to remind public bodies to revisit their system in order to provide the required safeguards to protect such information from unauthorized access.

Respectfully submitted,

The Honourable Alexandre Deschênes, K.C.

Dated the City of Fredericton,

Province of New Brunswick

The 10th day of May 2023