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

REPORT OF THE COMMISSIONER'S FINDINGS

Personal Health Information Privacy and Access Act

Privacy Breach Notification Matter: 2015-2513-H-710
Complaint Matters: 2015-2587-H-729; 2015-2588-H-730; 2015-2589-H-731
Date: January 28, 2016

"*Case about the theft of a laptop computer containing personal health information*"

INTRODUCTION

1. The present Report of the Commissioner's Findings is made pursuant to the *Personal Health Information Privacy and Access Act*, S.N.B. c.P-7.05 ("the *Act*") and stems from an investigation carried out into a notification of a breach of privacy made to the Commissioner pursuant to section 49 of the *Act*.

2. The investigation was undertaken by the Commissioner upon being notified on June 16, 2015 by Horizon Health Network ("Horizon") that this privacy breach had occurred upon discovering that a laptop computer containing personal health information of 158 patients was stolen from a hospital.

3. At the time we were notified, Horizon had not yet notified the individuals whose patient information was contained in the missing laptop computer. We speak more on this point later in this Report.

4. This Report of Findings will encompass the following elements: the context of this case and facts uncovered in this investigation, the steps taken to contain the breach, the notification process undertaken, the requirement of security safeguards, the correctives measures commenced to rectify the breach, and our conclusions. We finish this Report with our findings and recommendations pursuant to the *Act*.

5. We now proceed to the elements of this Report of Findings.

INVESTIGATION

FACTS UNCOVERED ABOUT THE INCIDENT

6. There is a Respiratory Therapy Department at the Dr. Everett Chalmers Hospital (the "Hospital").

7. The Respiratory Therapy Department is responsible for performing various tests to measure patients' lung function. One of the tests performed is known as a Spirometry test.

8. The main entrance to the Respiratory Therapy Department is only accessible by authorized personnel (between 19 and 21 of them). These staff members enter by swiping their security access cards.

9. Although the Department's main entrance only allows authorized personnel and the door remains shut, we were informed that this entrance had been kept opened during the daytime shift (8:00 am to 4:00 pm). This practice was adopted because of the continuous flow of Respiratory Therapists wheeling equipment in and out of the Department on a daily basis. By keeping the entrance open, this meant that authorized personnel did not have to swipe their access cards every time they entered the Department's main entrance.

10. In that Department, there is another door to the outside, namely a fire door that remains shut and locked at all times; for obvious reasons, staff can open it from the inside in order to exit in an emergency.

11. In that Department, personnel work all the time, made up of full-time, to part-time and casual employees. The shifts are daytime, evening and night time, as follows: personnel who work between 8 am to 4 pm, those who work from 8 am to 8 pm, and from 8 pm to 8 am. Due to the functions of the job that requires them to go to other parts of the Hospital, however, personnel are not always present inside the Department.

12. We note that the practice of keeping the entrance open was only adopted by the daytime personnel, i.e., they would shut the entrance upon leaving at 4 pm for the next shift work.

13. On Thursday, June 11, 2015, the personnel at the Department found the room very warm during the day, and that it had remained warm despite the entrance being open. Therefore, to cool it down, the personnel leaving at 4 pm made the decision to leave the entrance open when they left. They usually shut the entrance upon leaving at 4 pm.

14. As per the normal shift, other staff was working until 8 pm that evening, and again due to the nature of their work that requires them to go back and forth to other areas of the Hospital, those staff members were in and out of the Department between the hours of 4 pm and midnight that evening. The only difference on June 11, 2015 was that during that shift, the entrance to the Department was left open.

15. In order to properly report on this breach, it is important to understand how the laptop computer was stolen, beginning with where it was located, who had access to it, and how it was stolen. Then, we determine what data was contained on the laptop.

Stolen laptop computer

16. The Department used three computers to perform its tests. There is a desktop computer located on top of a desk inside the Department, and there are two laptop computers, each of which is located on a mobile cart (there being two carts in total).

17. The first laptop computer was secured to its mobile cart with a cable and a lock; however, the combination lock was not secured. The other was secured to its mobile cart with a cable and a lock and the combination lock was secured.

18. One of these laptop computers was stolen, and it was the one without the secure lock. In addition, this is the laptop was neither password protected, nor encrypted.

19. In fact, we later found out that none of the computers (neither of the 3) were password-protected or encrypted.

20. We understand that the stolen laptop contained the personal health information of 158 patients who had undergone Spirometry testing since February 2015 (the type of test conducted at this Department). More specifically, the data collected and stored on the laptop included: the patients' names, Medicare number, dates of birth, physician's name, patient's height and weight, reasons for the exam, medical query/suggested diagnosis, significant respiratory history, raw test data, and patient's respiratory and/or cardiac medications. We note that the patients' address or phone numbers were not stored on the laptop.

21. The laptops were used to conduct Spirometry tests, as well as other respiratory tests. They were placed on mobile carts in order to perform these tests either at patient's bedside in the Hospital or in the ECG Department of the Hospital, or also in the Pulmonary Function Lab for outpatients who attend with appointments. Both the ECG Department and the Pulmonary Function Lab are located close to the Respiratory Therapy Department and the Department's personnel (Respiratory Therapists) wheel out the mobile cart on which a laptop computer is kept, to either of those locations. Once the tests are completed, the mobile cart is wheeled back to the Department.

22. As stated above, on the day of the incident, the Department daytime staff left the entrance propped opened after 4 pm in the hopes of cooling it down during the evening.

23. According to Horizon Health Network's internal investigation, it would then appear that the laptop computer went missing between the hours of 4 pm and midnight on the night of June 11, 2015, being the time during which the entrance to the Department was left opened. It was only upon discovering that the laptop was missing from its cart shortly after midnight that the entrance to the Department was closed.

24. We know, according to staff's routine, that the Department is left unattended for undetermined periods of time, and this would mean that the Department was left unattended with its entrance opened during both the evening and the nighttime shifts (between 4 pm and 12 midnight when the entrance door was closed).

25. Shortly after midnight, the staff member noticed that one of two laptop computers was not on its mobile cart. Thinking that it had been sent for servicing, the staff member did not report the missing laptop to the daytime staff upon finishing his shift at 8 am. According to the facts, it appears that the daytime and evening staff also failed to notice the missing laptop, as it was only in the late afternoon or early evening of June 12 that a staff member noticed that it was not situated on its designated mobile cart.

26. Not knowing whether the laptop computer had been sent for service or had been stolen, the staff member asked the Department's Respiratory Therapy Clinical Coordinator of its whereabouts. It was only then that everyone discovered that the laptop computer had not been sent for servicing and was in fact missing.

27. The Respiratory Therapy Clinical Coordinator then instructed the staff person to contact the Hospital's Administrative Officer and Security Office, and the Coordinator then filed an Incident Report with the Hospital reporting the missing laptop computer.

28. The laptop computer was never recovered, and the Security Office indicated there was not footage to show someone with the laptop during that time in the hallways. We note that there is no surveillance camera located at the entrance to the Department. Horizon's investigation did not reveal any suspicious activity, except for one patient that was in the area and was later questioned about the matter as well as having the patient's room searched for the laptop. Again, it was not found.

Laptop computer's missing security safeguards

29. As part of our investigation, we set out to find the reasons why the laptop computer was not secured to its mobile cart by cable and combination lock, and why it was

neither password-protected, nor encrypted. More importantly, we had many questions as to why the Department was left totally accessible to anyone passing by due to the entrance being propped open and the Department unattended.

30. We point out that the Department was supposed to be accessed only by authorized personnel, and that overriding concern had been addressed by having authorized personnel attend only by swiping their approved security access cards. We therefore find that the main cause of this breach incident to have been the opened entrance to the Department while staff was not in attendance.

31. We also opine that the incident could have been avoided by simply having the entrance closed and accessible to only those authorized. Otherwise, and as took place in this case, a passerby could see there was a laptop on a cart, and seized the opportunity to take it.

32. More troubling is that Horizon and the Hospital's policy to have medical equipment secured by cable and lock when mobile carts are used were not followed.

33. In the past, both laptops in the Department were always secured to their mobile cart with a combination lock; however, at the time of the incident the laptop in question only appeared to be locked when in fact it was not. Again, easy for an individual to seize the opportunity to try to take the laptop and to succeed where the lock was not secure.

34. Although Horizon recognized this to be a one of the causes of the privacy breach, it explained that this oversight occurred when the laptop in question was purchased from FacilicorpNB in February 2015 to replace the old laptop. The old laptop had been securely locked to its mobile cart by cable with a combination lock. There was also a change in staff in the Department and those responsible for the service and maintenance of the Department's laptops (being FacilicorpNB's Clinical Engineering division, as described below). The staff turnover resulting in no one knowing the combination for the old laptop's combination lock. The lock was therefore cut off and replaced by a new combination lock.

35. Further, lack of communication between the Department staff and the Clinical Engineering Department in deciding who was responsible for assigning a combination to the new lock resulted in the combination lock never being properly secured to the mobile cart.

36. FacilicorpNB's IT division is responsible for the installation of all computer hardware in Horizon's organization and to ensure that data and information are safely and securely stored and managed. That said, however, the use of the computers, including how the data will be placed and/or stored on the computers, remains the responsibility of Horizon and or Hospital and staff that use the equipment. On the other hand, FacilicorpNB's Clinical Engineering division maintains and inspects the specialized diagnostic and therapeutic medical equipment used by health care professionals.

37. When these devices are used by Horizon to store patients' sensitive information, it is Horizon's and FacilicorpNB's policy that the data be stored on Horizon's secure network system, which allows the data to be retrieved in the event of a computer malfunction, or a theft, such as it occurred in this case.

38. Horizon purchased the laptop computer in question from FacilicorpNB in February 2015 to update an old computer. As well, the laptop was purchased from FacilicorpNB because the vendor for the Spirometry testing software and diagnostic device did not provide a computer, even though one was required to operate the medical device. That software and hardware solutions were tested with limited success, and accordingly, it was not possible, at the time of the theft, for the laptop computer to be encrypted because the operating software and the data resided on the same device.

39. The laptop computer, therefore, was purchased for the sole purpose of operating respiratory software that would record the results of the respiratory tests.

40. When FacilicorpNB initially issued the laptop computer, a login password was installed on the laptop; however, during installation of the Spirometry testing software, the login function was removed because the computer (and its data) was not going to be connected to Horizon's secure network system.

41. Horizon informed us that prior encryption techniques, present at the time of the incident, required the use of a separate password from the login password to enable encryption. Given that certain devices are shared by multiple users around the clock, including the Spirometry test devices and laptop computers, the requirement of a separate password from the login password was not a workable solution in various medical settings where devices were shared between multiple rotating staff. Regional Health Authorities cannot risk that staff might not being able to access medical information due to a password not being communicated or changed.

STEPS TAKEN TO CONTAIN THE BREACH

42. We know that upon discovering that the laptop computer had in fact gone missing or was stolen, steps were taken to determine where it was and whether video surveillance revealed any clues to locate the device, but this proved unsuccessful.

43. As a result, Horizon reported the theft to the Fredericton Police Force, and also contacted several local pawn shops, but again without success.

44. At a meeting held on June 17, 2015, FacilicorpNB was asked whether the webcam on the stolen laptop could be remotely activated to determine clues as to its location, but as the laptop was not connected to Horizon's secure network, the wireless cards had not been activated in the first place.

45. The data was stolen, but not lost as the same information of patients' tests was retrieved from paper physical files.

46. Therefore, this breach resulted in patient health care data being put in the hands of unauthorized individuals.

NOTIFICATION PROCESS

47. The *Act* requires health care providers or custodians[1], as defined in the *Act*, to protect personal health information of its patients and clients at all times by adopting information practices that include reasonable administrative, technical and physical safeguards that ensure the confidentiality, security, accuracy and integrity of the information. In this case, the responsible custodians are the Hospital and Horizon.

48. When personal health information becomes is stolen, lost, disposed of, disclosed to, or accessed by an unauthorized person, this constitutes a privacy breach under the *Act* and the responsible custodian, in this case, Horizon and the Hospital, are obligated to notify those affected and the Commissioner pursuant to paragraph 49(1)(c) of the *Act*.

49. When a device is not encrypted, the data can be accessed by the person who stole the device, someone who was not authorized to see it. Therefore, notification is especially

[1] "Custodian" under the *Act* is defined as a person, group or institution that has been entrusted by law to collect, use and share health care information of individuals (such as patients in this case), and to protect such information at all times in accordance with the rules found in the *Act*.

important where the theft of personal health information could lead to the identification of individuals, to whom the information relates, thereby putting their privacy and their identity at risk.

50. Horizon reported the breach to the Commissioner on June 16, 2015. Then came the task of notifying those affected. To these individuals whose information was saved on the laptop computer, the Department staff immediately began to cross-reference the patients who had undergone Spirometry testing since the laptop computer had been purchased in February 2015. Staff reviewed patient lists, visit histories and workload, as well as the patients' physical medical file, where a copy of the Spirometry test results had been printed and inserted. This took some time and effort, but by process of elimination, the Department was able to confirm that the lost information belonged to 158 patients.

51. Notification to all these individuals was carried out by letters issued on July 13, 2015, in which they were informed of:

- the details of the breach;
- the specific personal health information contained on the laptop;
- the impact of the theft, which was unknown at the time;
- that the breach notification had been to the Privacy Commissioner;
- that the Fredericton Police had been notified of the theft;
- the contact information for obtaining a new Medicare number;
- the steps taken by Horizon for this serious incident, including its review of internal processes;
- the contact information of Horizon's Chief Privacy Officer; and
- and that the patients had a right to contact* the Privacy Commissioner (with contact information).

**We note for the record that patients must be advised of their right to complain to the Privacy Commissioner, rather than simply contacting our Office.*

52. Of the 158 patients notified, 26 contacted Horizon's Privacy Office directly and inquired further about the breach incident. Our Office also received inquiries and complaints from several individuals, three of which chose to file formal complaints as allowed to do under subsection 68(2) of the *Act*:

> 68(2) Without limiting paragraph 1(a), an individual may make a complaint to the Commissioner alleging that a custodian

> (a) has collected, used, or disclosed his or her personal health information contrary to this Act, or
> (b) has failed to protect his or her personal health information in a secure manner as required by this Act.

53. These individuals were all concerned as to whether the loss of their personal health information could lead to identity theft, given that their Medicare Number had been stolen as well. Our investigation of these complaints was included in the breach notification file we had commenced when first notified of the incident.

Can the loss of personal information lead to identity theft?

54. We are often asked about the risk of identity theft in incidents of this nature.

55. The information lost in the present case included the patients' names and other medical information, including the patients' Medicare number. Fortunately, the data did not include the patients' phone number or address.

56. While it is impossible to determine with any degree of certainty the risk to an individual regarding identity theft when one's personal information has been compromised, we cannot assume that there is no risk and therefore, the loss of any information should be taken seriously. With each additional piece of identifying information that is compromised, the risk of fraud and identity theft increases.

57. There is no agreement on the meaning of "identity theft," but the term is used for everything from cheque forgery, the use of stolen credit cards, to sophisticated scams in which an impostor adopts somebody else's identity to gain access to their assets. Credit monitoring will not be possible in order to monitor the lost personal information.

58. A prudent approach whenever someone is concerned about the risk of identity theft is to adopt simple measures in his or her monthly schedule to lessen the chances that personal information winds up in the wrong hands, such as:

- keeping track of when credit card statements are supposed to arrive, and calling the credit card company if the statement is late;
- reviewing all credit card and bank statements to make sure there are no unauthorized purchases;
- getting an annual credit report (major credit reporting bureaus provide one free report per year);
- creating a new password and changing it often for each online account. A strong password is one which is hard for anyone to guess;

- remaining vigilant and suspicious of emails that appear to come from banks, government agencies, credit card companies which ask to provide personal information online. Real banks and other agencies do not send such emails, yet scammers often use real logos to make their fraudulent messages look authentic; and,
- reading more other useful information and tips on how to report and correct the damage resulting from identity theft or related frauds (we suggest consulting the website of the Office of the Privacy Commissioner of Canada found at www.priv.gc.ca).

59. In some special cases for patients who show a greater degree of risk, they may be referred to Medicare Services at the Department of Health to request a new Medicare Number.

60. Patients were also guided to monitor their bank accounts and notify their bank if they had any concerns. In addition, Horizon has offered to pay for any requested credit checks.

CORRECTIVE MEASURES

61. Horizon has been undertaking several corrective measures to prevent similar incidents from recurring. As a starting point, the Department in question must now ensure that security measures that ought to be in place for electronic devices containing personal health information are in fact put in place. Those measures will include the possibility of deleting patient data from mobile devices.

62. Horizon installed password protection to all of the computers and devices used in the Department, locked the laptops to their respective mobile carts, and required that the entrance door remain shut locked 24 hours a day, 7 days a week. It can only be opened with a swipe card. This took place within two weeks of the incident.

63. A new policy is currently under development that will require all portable devices to have passwords and encryption regardless of their status; however, there exist some devices where password and/or encryption are not possible. In these cases, there will need to be clear communication between FacilicorpNB and the Regional Health Authorities identifying alternate safeguards to ensure the confidentiality of the personal health information is maintained.

64. We understand that on a larger scale, encryption has been progressively deployed for approximately 2400 laptop computers used by hospital staff, as well as equipment used by Horizon and FacilicorpNB employees. At the time of the incident, approximately 305 devices were encrypted; however, since the incident, 98% of the 2400 laptop computers have been encrypted and have received passwords.

65. Other measures, mainly for the proper administration and maintenance of security safeguards were also undertaken that should, in our view, avoid a recurrence of circumstances that led to no one being able to know what was the combination to the lock, whether the device could be encrypted, etc.

66. Again, simply put, we find that the theft of the laptop could have easily have been prevented in the first place by keeping the door shut and having a secure lock on the laptop.

COMMISSIONER'S FINDINGS

67. This breach incident was substantial in that it affected a large number of patients whose personal health data was collected and stored on a laptop computer without proper security measures.

68. This incident conclusively demonstrates the vital requirements of safeguarding sensitive data on electronic devices, such as the laptop computer, especially where the sensitive data is stored directly on the device's hard drive instead of on a secure network.

69. The Spirometry testing software was not compatible to Horizon's secure network. Therefore, we find that Horizon should have taken other steps to ensure password protection and encryption was installed on the laptop computer.

70. Our investigation revealed that Horizon and the Hospital's Respiratory Therapy Department failed to protect the personal health information of its patients in the following manner:

a) By leaving the entrance door open, while the room was unattended for an undetermined amount of time;
b) By not securely locking the laptop computer to the mobile cart's cable, as required;
c) By using allowing the highly sensitive patient data to be stored on the laptop knowing that it was not secure; and,

d) By failing to password protect and encrypt the data on the laptop.

LACK OF SECURITY SAFEGUARDS

71. This privacy breach incident has brought Horizon to review its security measures in place regarding personal health information that is stored on electronic devices, as it should.

72. Horizon, as a custodian who maintains personal health information in electronic form must implement additional safeguards required by the *Act* and its *Regulations* where the emphasis is placed on the requirement of greater protection for all mobile devices (USB keys, laptop computers, etc.) was required to ensure that such devices remained password protected at all times.

73. Furthermore, electronic devices used to store personal health information, such as in the case of a laptop computer, will require an added layer of protection. There is a heightened degree of caution whenever using these devices and additional security measures must be adopted, as per subsections 50(4) of the *Act*, and 20(1) and (2) of its *Regulations*:

> 50(4) A custodian who maintains personal health information in electronic form shall implement any additional safeguards for the security and protection of the information required by the regulations.
>
> 20(1) A custodian shall establish and comply with a written policy and procedures with respect to information practices for the protection of personal health information containing the following requirements:
>
> (a) measures to protect the security of personal health information during its collection, use, disclosure, storage and destruction;
> (b) measures, for example by the use of passwords and encryption, to ensure that removable media used to record, transport or transfer personal health information is appropriately protected when in use;
> (c) measures to ensure that removable media used to record personal health information is stored securely when not in use;
> (d) measures to ensure that personal health information is maintained in a designated area and is subject to appropriate security safeguards;
> (e) measures that limit physical access to designated areas containing personal health information to authorized persons;
>
> 20(2) A custodian shall keep a record of all security breaches by recording the security breaches and corrective procedures taken to diminish the likelihood of future breaches.

74. While the practice of not requiring a password to login to the stolen laptop may have allowed patients the advantage of being served more quickly, it had the harmful effect of rendering the patients' personal health information susceptible to a privacy breach.

75. This is not to say that this would have prevented the theft of the laptop computer, however, it would have reduced the risk of unauthorized accesses to the sensitive data had the laptop computer been protected with passwords and encryption.

76. For all of the above reasons, we find that, at the time of the breach incident, the security measures collectively adopted and used by the Hospital and Horizon did not meet the standards required of custodians for the protection of personal health information of patients under the *Act*.

77. As well, we find that the measures in effect at that time were not in compliance with the *Act*. As such, Horizon and the Hospital failed in their lawful duty to protect the personal health information of the Hospital's patients.

78. The *Act* not only mandates the use of security safeguards, but also establishes a pragmatic way of implement these safeguards by referring to two standards described above: reasonableness and appropriateness for the level of the data's sensitivity.

79. The first standard calls for safeguard measures to be reasonable, that is, to keep the information reasonably safe when viewed objectively rather than according to subjective choices. Reasonableness does not mean that security safeguards have to be perfect, but rather, they should appear reasonable depending on the circumstances.

80. The second standard calls for safeguards to be determined in conjunction with the level of sensitivity of the information the custodian aims to protect. The higher the level of sensitivity of the information, the higher the level of the security safeguards required.

81. Other reasonable security measures can be derived from common sense observations. Locked doors and drawers are effective security safeguards. Regrettably, as was the case in this matter, it is often the lack of attention to everyday practices that presents the greatest security concerns.

82. At a minimum, we find that the laptop computer ought to have been securely locked to the mobile cart in the manner in which it was required, and the main entrance door to

the Respiratory Therapy Department should not have been left opened without anyone in attendance within the Department.

83. We are pleased that corrective measures have been implemented to ensure greater protection of patient information in the future. We remind all, however, that hundreds of patients who benefited from the services provided by the Respiratory Therapy Department entrusted their sensitive information to those with a duty to protect it.

84. The *Act* is designed to improve health care by ensuring that patients feel confident in surrendering their health information to medical staff with the belief that their private information will be used in the most effective and safe manner possible. This confidence is not only premised on the advantages of modern technology to support the delivery of their health care, but also on the notion that those who use this modern technology will employ reasonable secure methods to protect their privacy.

85. Let's not forget that this is case is not only about the ease of use of portable devices, or leaving a door open, it is about protecting a person's private information and when that does not happen, it can fall into the hands of those who should not have it. This is what took place in this case.

86. We do add that Horizon and the Hospital took this privacy breach matter seriously and their duty to adopt significant corrective measures to ensure that similar incidents do not recur in the future.

RECOMMENDATION

87. Based on the above findings, the Commissioner recommends that Horizon and the Hospital continue with the implementation of all of the corrective measures it has shared with us, some of which have been identified in this Report of Findings, until they have been fully implemented, and that Horizon provide to the Commissioner's Office a status update of this progress or completion by no later than the end of July 2016.

Issued at Fredericton, New Brunswick, this 28th day of January 2016.

_____

Anne E. Bertrand, Q.C.
Access to Information and Privacy Commissioner