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

Matter: 2014-2214-H-640
Date: August 26, 2016

Case about a laptop containing unencrypted personal health information stolen from a hospital

INTRODUCTION and BACKGROUND

1. The present Report of the Commissioner's Findings is made pursuant to subsection 73(1) of the *Personal Health Information Privacy Act* ("the *Act*") and stems from a privacy breach incident reported to our Office on December 17, 2014. The breach occurred when a laptop containing personal health information was stolen from the Moncton City Hospital, while password protected it was not encrypted.

2. Three custodians subject to the *Act* were involved in this case, Horizon Health Network, le Réseau de santé Vitalité, and FacilicorpNB because the privacy breach occurred at a hospital within Horizon's mandate, the laptop belonged to an employee of FacilicorpNB, and the individuals whose information was on the laptop were patients of the Réseau Vitalité.

3. In June or July 2013, the Bathurst and Campbellton hospitals (Réseau Vitalité) entered into an agreement with the Moncton Hospital (Horizon Network) whereby radiology exams taken in Bathurst and Campbellton would be sent to the Moncton City Hospital to be read by radiologists at that location. Radiologists would then prepare reports to be sent back to Bathurst or Campbellton. This process was adopted because there were not enough radiologists available in those regions with sufficient time to read the exams and prepare reports.

4. A FacilicorpNB employee working in clinical engineering was asked to assist from a technical viewpoint. FacilicorpNB is the arm of government that assists regional health authorities, among others, with their information technology requirements.

5. The employee configured a printer to enable reports dictated by radiologists in Moncton to be printed in a PDF format in either Bathurst or Campbellton directly as required. In addition, as a quality control measure, the employee arranged it so that he would also be emailed copies of the reports so that he could verify the number of exams sent in with the number of reports sent back to these hospitals to ensure they matched.

6. The employee kept the reports for a few days in the event that they might need to be re-sent to the hospitals and then deleted them. The reports were kept in files created on his laptop (in a Bathurst folder and a Campbellton folder). An electronic backup copy of the reports was created on a separate mobile device (USB key).

INVESTIGATION OF THE PRIVACY BREACH

Facts uncovered as to what caused the breach

7. The practice to have reports with sensitive patient information stored on a laptop computer is not common practice, but one that was adopted in this case in response to the shortage of radiologists at that time period.

8. When the laptop was stolen, the employee had already deleted 58 reports in the Bathurst folder, but was uncertain as to whether 78 reports contained in the Campbellton folder had also been deleted. Officials assumed that the copies of the reports sent to Campbellton still remained on the laptop computer at the time it was stolen, thereby resulting in a privacy breach for those patients whose information formed part of the 78 reports. By chance, of the 78 reports in question, only six contained the patients' names, but all of the reports contained personal health information such as:
    - date and time of visit and hospital unit number,
    - patient's clinical history, and
    - radiologist's findings and impressions.

9. The FacilicorpNB employee worked in an office located in the Medical Imaging Department at the Moncton Hospital; the physical office is small and is beside one of the x-ray rooms. Although a video camera is located in the hallway leading to the office, the camera is a Live-Feed Only camera and does not have a recording function. This made it impossible to review footage to determine how and by whom the laptop was taken. Review of the surveillance footage from other cameras did not capture or show a laptop in the possession of anyone.

10. Our investigation found that at approximately 9:40 am, the employee was about to leave the office to take a break and logged off the laptop computer, as per his usual practice when leaving the laptop unattended. The office had a door with a lock which meant the employee could have closed and locked it; however, the effective cause of the theft that led to the privacy breach was due to the fact that the employee left the door open on purpose. In fact, the employee's practice was not to shut his door regularly during his entire work day because his tasks required him to be in and out of his office frequently.

11. After a 20 minute break and returning to the office at approximately 10:00 am, the employee immediately noticed that the laptop computer, together with a headset and power cord were gone.

12. Given the employee's practice of not locking his office door, we find it was only a matter of time before the theft of the laptop computer would take place. The laptop was not secured by locking cables and was left in plain sight where the public clearly can access. More troublesome, the laptop was not encrypted to protect the data.

13. Another contributing cause to the breach was for the three custodians involved to have allowed the employee to continue the practice of keeping doors open that could be locked upon exiting a room or office, knowing full well there was a portable device with patient information, and for allowing the employee to continue the practice of keeping patient information stored on a laptop computer that was not encrypted.

Statutory obligation to protect patient information at all times

14. The *Act* establishes clear and unambiguous rules for custodians with regards to how they collect, use, disclose, retain and securely destroy personal health information that protects the confidentiality of the information and the privacy of the individual to whom the information belongs.

15. Furthermore, the *Act* imposes clear security safeguards of administrative, technical and physical nature that are intended to ensure the confidentiality and security of patient information at all times.

16. Laptops have been stolen in New Brunswick hospitals in cases that were reported to us before, being 7 laptops stolen in the past. We speak to that further in the present Report.

17. While theft is one concern, the overriding issue in terms of protection of patient information must remain the security features to be put on all laptops such as password and encryption, to prevent the data from being accessed by thieves or others who should never see this private information.

18. Horizon, Vitalité, and FacilicorpNB are all custodians in their own right under the *Act* and as they are equally responsible for protecting the personal health information with these safeguards, the fact that these safeguards were not in place in this case makes

them jointly responsible for what was undoubtedly in our view a preventable privacy breach.

Obligations of custodians to act when a privacy breach occurs

19. When a privacy breach occurs, those responsible must determine the cause of the breach, contain the incident to limit the consequences, notify both the Commissioner and the individuals whose information was compromised at the first reasonable opportunity, and implement corrective measures to prevent similar incidents.

20. When providing notice to individuals affected by a privacy breach, *Regulation 2010-112* states that those responsible must:

- Identify the custodian responsible;
- Provide the name and contact information of the person designated by the custodian to respond to inquiries about the custodian's information practices;
- Describe the nature of the breach of privacy;
- Give the date and location of the breach of privacy; and,
- Provide the date when the breach of privacy came to the attention of the custodian.

Notification to those affected by the breach and to the Privacy Commissioner

21. Six reports that were on the stolen laptop contained the patient's name and two reports identified the same patient. This meant that five individuals could be identified from the radiology reports when accessed by the thief. These five individuals were notified of the incident by Vitalité, being patients of Vitalité.

22. As for the remaining 73 individuals whose information was also made accessible by the perpetrator of the theft of the laptop, Horizon, Vitalité and FacilicorpNB were able to determine that these patients could not be identified without their names based on the nature of the information contained in the reports. As a result, they decided not to notify those patients.

23. We examined the patient information in question and find that while identification might be possible due to the dates and times of hospital visits, with unit number and patient history, this would require a great deal of effort in both obtaining this data and deciphering the corresponding hospital information. Without evidence that a hospital

employee might have actually been the person who stole the laptop computer, we agree with the decision that notification of the remaining 73 individuals was not required under section 49 of the *Act*.

24. The privacy breach involved three distinct custodians and while they played different roles, all three were required to follow the requirements of the *Act*, including the mandatory notification to the Commissioner's Office.

25. Notification under the *Act* is meant to result in one important outcome: to render the custodian responsible for the breach accountable and answerable for actions taken or actions that were failed to be taken.

26. Moreover, this accountability will lead the custodian to take corrective measures to ensure that the conditions that led to the breach are adjusted, improved, or removed altogether so that it does not occur again. Otherwise, patients would ask themselves:

What is the point of all of this?

27. Implementing corrective measures will be mandatory for every custodian involved in a privacy breach case, and other actions to be taken in the event of a privacy breach such as containment and notification to affected individuals will depend on the role the custodian played in contributing to the breach.

28. In the present case, the affected individuals were patients of Vitalité and it made sense that Vitalité was responsible for notification to those affected individuals.

29. We understand that all three custodians involved had discussions as to how best approach the situation and it was agreed that only one breach notification form would be sent to the Commissioner. We were notified of this privacy breach by Horizon and by Vitalité.

30. Although appropriate in this case that a team approach be taken to manage the privacy breach, all custodians responsible must adhere to their obligations and in that regard, FacilicorpNB ought to also have taken part in the notification to the Commissioner made by both Horizon and Vitalité under section 49.

31. We reiterate that notification under the *Act* is mandatory and is intended to make the custodian responsible for the breach *accountable and answerable* for actions taken or

actions that were failed to be taken. We will issue a recommendation that in future cases, FacilicorpNB uphold its obligations under section 49 and notify the Commissioner.

Containment of the consequences of the privacy breach

32. Once the privacy breach was discovered, the employee notified Hospital security without delay and a report of theft was completed by the Manager of Security and submitted to police. The police requested the serial number of the laptop and opened an investigation into the matter. FacilicorpNB did not provide this information to the police, but we remain unsure as to why it could not do so.

33. By chance, the USB key with backup data was not stolen. This meant that the data was not lost. The laptop was never retrieved.

34. Officials of Horizon, Vitalité, and FacilicorpNB were also made aware of the incident. They held a meeting to determine the initial first steps to be taken and reviewed camera footage we now know revealed nothing.

35. The employee in question indicated to officials that the laptop could be used to link on a desktop computer and access folders on a SharePoint drive (folders that contained the Campbellton and Bathurst reports). For a thief to access these reports, he or she would need to break through the password and username, and be on hospital premises for the link to be functional. Not knowing the identity of the thief, the employee contacted both facilities and requested that the files be moved or deleted so that they would no longer be accessible through the link from the stolen laptop, and these steps were undertaken.

Corrective measures as a result of this incident

36. Horizon, Vitalité and FacilicorpNB have agreed to implement the following measures:

- The employee's new laptop has been password protected and encrypted;
- The USB drive used by the employee to store an electronic back up copy of the data will also be password protected and encrypted;
- The employee has been advised to shut the office door from now on every time he leaves the office, thereby keeping the office locked at all times when he is not in attendance;

- A new committee comprised of staff members of Horizon, Vitalité and FacilicorpNB was stuck in October 2015 to establish policies and governance around devices holding personal health information (deciding on a number of factors including encryption, passwords, device physical security, incident reporting, etc.);
- A new policy will require that all portable devices are protected by passwords and encryption, and where this is not possible, communications between FacilicorpNB and the health authorities will be required in order to identify alternate safeguards to ensure the protection of the personal health information;
    - The signature of a vice-president of the health authority will be required on a special dispensation form in order to allow an exception do the policy;
    - The policy will also ensure that if the health authority procures any device outside of their information technology (IT) services, without the knowledge of IT staff, the health authority will be responsible for ensuring that the device is secure.
        - *These two factors were not in place before this incident occurred*.

37. The employee who caused the breach in this case had received privacy training in 2010 by the Chief Privacy Officer for FacilicorpNB. He also had received, previous to 2010, other privacy related training by the hospitals, and signs a Declaration of Understanding regarding confidentiality, on an annual basis, as provided for in the joint confidentiality policy between FacilicorpNB and the regional health authorities.

38. While training is supposed to take place on an annual basis, all that was reported to us was that this employee signed the Declaration every year and his last training was in 2010. The employee was not reprimanded in this case.

39. In our view, common sense failed in this case: not shutting a door knowing full well that an unsecured laptop with unencrypted patient information remained in full view and accessible.

40. Furthermore, using an unencrypted laptop for patient reports should never have been tolerated. A laptop containing patient information should never have been unsecured.

41. While we still find this case to have been clearly preventable, corrective measures listed above should prevent a recurrence in the future in order restore trust on the part of

those patients to whom Horizon, Vitalité and FacilicorpNB owe a duty as custodians under the *Act*.

Corrective measures from previous reported case of stolen laptop in a hospital

42. In 2015, a laptop containing 158 individual patients' data was stolen from the Dr. E. Chalmers Hospital (DECH) in Fredericton, namely from the Respiratory Therapy Department. We found in that case the Horizon and the Hospital failed to protect the personal health information of its patients by leaving a door open to a room where the laptop was not securely locked with cables to a mobile cart, and where highly sensitive patient data was stored on it without password protection or encryption of the data (Report of Findings 2015-2513-H-710).

43. During our investigation of that case, Horizon ramped up its examination of security measures to ensure that those that ought to be in place for electronic devices containing personal health information were in fact put in place. Those measures included the possibility of deleting patient data from mobile devices. Horizon installed password protection to all of the computers and devices used in that DECH 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.

44. Horizon was also in the process of developing a policy that would require all portable devices to have passwords and encryption regardless of their status; however, in some cases, password and/or encryption could not be possible for certain devices and FacilicorpNB and the Regional Health Authorities were to identify alternate safeguards to ensure the confidentiality of the personal health information for such devices.

45. Meanwhile, at the time of that privacy breach in 2015, only about 300 devices were encrypted; however, encryption was then deployed progressively to include approximately 2400 laptop computers used by hospital staff, as well as equipment used by Horizon and FacilicorpNB employees as we concluded that investigation.

46. This present Report of Findings therefore contains recommendations to Horizon, FacilicorpNB and Vitalité to continue with such corrective measures.

RECOMMENDATIONS

47. Based on all of the foregoing, the Commissioner recommends under paragraph 63(f) of the *Act* that all three custodians, FacilicorpNB, le Réseau de santé Vitalité, and Horizon Health Network, implement jointly and without delay:

(a) written mandatory guidelines that, before they are issued to staff members, all portable electronic devices to be used to store personal health information are password protected and encrypted without exception;

(b) written mandatory guidelines that all portable electronic devices issued used to store personal health information shall be locked securely and shall be kept in locked office or locked storage locations when not in use or when left unattended for any given amount of time without exception; and,

(c) a standard feature for all portable electronic devices issued used to store personal health information for remote data wiping, where not cost prohibitive to have this capability in all cases.

48. The Commissioner also recommends under paragraph 63(f) of the *Act* that all three custodians, FacilicorpNB, le Réseau de santé Vitalité, and Horizon Health Network, inform all their staff members of these mandatory guidelines with a notice that that failure to adhere to them, even due to carelessness, will result in disciplinary measures.

49. Finally, the Commissioner recommends that FacilicorpNB, le Réseau de santé Vitalité, and Horizon Health Network adopt and/or improve upon, those corrective measures that were being undertaken and implemented in the case of stolen laptop at the DECH case referred to above (2015-2513-H-710), and that they submit a joint progress report regarding all these recommendations to the Commissioner by no later than October 28, 2016.

Issued at Fredericton, New Brunswick, this 26th day of August, 2016.

_____

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