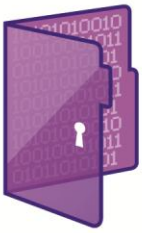
Office of the Access to Information and Privacy Commissioner
New Brunswick



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

Breach Notification Matter: 2011-472-H-143
Complaint Matters: 2011-535-H-167, 2011-537-H-168, 2011-548-H-171
Date: September 13, 2012

Commissioner's Investigation

Privacy Breach Incident – theft of portable computer from a hospital

Background

1. The Dr. Georges-L.-Dumont University Hospital Centre in Moncton ("the Hospital") houses a specialized treatment centre in nephrology and urology ("the treatment centre"), which also holds a clinic for outpatients requiring care in urodynamic testing ("the clinic").

2. On the morning of Monday, August 29, 2011, upon arriving at the treatment centre and entering the clinic, an employee noticed that the portable computer normally located inside the single room which constitutes the clinic was missing. The missing portable computer was equipped with specialized software for diagnostic use by the clinic. The employee notified the officials at the Hospital.

3. The Hospital, the treatment centre, and the clinic all come under the management of Réseau de santé Vitalité ("Vitalité"). The Hospital immediately informed the Privacy Officer for Vitalité of this incident who examined what had occurred. Based on the evidence uncovered, which is described below, Vitalité believed the missing portable computer was in fact stolen, and reported the theft to the local detachment of the Royal Canadian Mounted Police.

Privacy breach notification

4. According to the *Personal Health Information Privacy and Access Act* ("Act"), a privacy breach occurs when personal health information is stolen, lost, disposed of, disclosed to, or accessed by an unauthorized person. When one of these situations occurs, the person, group or organization that had been entrusted with the personal health information is required to take action. They are referred to as 'custodians' under the *Act*. A custodian is one that handles personal health information in order to provide or assist in the delivery of health care. Accordingly, Vitalité is a custodian, as well as the Hospital, the treatment centre and the clinic.

5. In the present case, the privacy breach of personal health information belonging to patients of the clinic occurred when the portable computer, which was not password-protected and which contained patients' medical data was stolen. This meant their private information could be viewed by an unauthorized person, i.e., the person or persons who stole the portable computer.

6. Paragraph 49(1)(c) of the *Act* requires a custodian that discovers a privacy breach to notify, as soon as possible, all of the individuals to whom the information relates that their personal health information has been compromised. This is referred to as a notification process. The *Act* also requires the custodian to advise the Commissioner of the privacy breach as soon as possible. In this notification process, the affected individuals must be informed as to what has occurred and when the incident took place. In addition, these individuals must be advised of their right to file a complaint with our Office pursuant to subsection 68(2) the *Act.* If they choose to do so, the complaint will allow the Commissioner to investigate the privacy breach incident and provide her conclusions and recommendations, if any, in relation to the breach in a Report of Findings.

7. Upon discovering this theft, Vitalité reported the privacy breach incident to the Commissioner, as well as to the Chief Privacy Officer for the Department of Health. This took place on August 31, 2011. In the present Report of Findings, we discuss our conclusions based on the investigation we conducted alongside that undertaken by Vitalité.

8. Vitalité ascertained that the stolen portable computer had been used to store personal health information belonging to several hundred patients of the clinic. The stored data included their personal information and health information. These patients comprised of three groups: adult patients, child patients, and patients now deceased. Notification to all these individuals, their parents or guardians, or their relatives (depending on the type of patient) was carried out by letters issued in early October 2011. In these notification letters, individuals were informed that the breach was the result of the theft of the clinic's portable computer and that they had a right to file a complaint with the Commissioner regarding the privacy breach.

9. Of the several hundred patients notified, a number of them contacted Vitalité's Privacy Office directly and inquired with those officials about the breach incident. Our Office received inquiries, complaints and concerns from five individuals. Among those, three individuals chose to file formal complaints under the *Act*. Their complaints are summarized below.

Complaints by affected patients

10. Upon being notified of the privacy breach, three individuals filed complaints with our Office and we began a formal investigation into the matter. These individuals sought answers to the following principal questions:

Why was the computer located in an area accessible to the public where it could be stolen?

Why did the computer not contain more security features?

Could loss of personal information lead to identity theft and affect one's financial history?

What actions are being taken to correct the breach and to prevent similar future incidents?

11. This Report of the Commissioner's Findings provides answers to these questions, and includes a description of the event, the reasons why the breach occurred, and the recommendations issued in relation to corrective measures to prevent a similar occurrence in the future.

Why and how did the breach occur?

12. On average, approximately 500 to 600 patients attend the treatment centre each day specifically to go to the clinic. The work shift for the clinic's approximately 30 employees begins at 8:30 am and ends at 4:30 pm every day, except on weekends where the clinic is closed. It is to be mentioned that while the work of the clinic finishes at 4:30 pm, the public is still allowed in the treatment centre until 7:00 pm.

13. The clinic comprises of a single room, the room where the portable computer was located. The door to the room locks automatically when the door is closed; however, the door is deliberately left open to allow the cleaning staff to enter at the end of the work shift. When the cleaning staff is done, the door to the room is then closed which locks the room automatically as the cleaning staff leaves. We understand that cleaning of the room is done usually by 6:00 pm.

14. On Fridays, the last employee leaves the clinic at 4:30 p.m. and the clinic re-opens on the following Monday morning. Security personnel normally conduct their security check of the area around 6:00 pm every day, same for Friday nights, when security personnel ensures the door to the clinic (i.e., to the room) is locked at that time. This room will remain locked until 7:00 am on the following Monday morning. At that time, security personnel unlocks the clinic (the door to the room) to allow access to the clinic by employees who arrive for their work shift. The clinic's employees usually arrive between 8:00 am and 8:15 am.

15. We can therefore conclude that the door to the room of the clinic where the portable computer was located remains unlocked and unattended between 4:30 pm and 6:00 pm each day, apart for time during which the cleaning staff is present, and for approximately one hour in the mornings between 7:00 am and the time when the clinic's first employee arrives, which is around 8:00 or 8:15 am. Before the weekends, the clinic remains unattended and unlocked between 4:30 pm and 6:00 pm on Friday night, apart for time during which the cleaning staff is present. When cleaning staff leave the clinic, it remains locked from 6:00 pm to Monday morning at about 7:00 am when security unlocks the room. At this time, the clinic is left unlocked and unattended for approximately one hour before employees arrive, which is around 8:00 or 8:15 am. We understand the door can only be unlocked by security personnel.

16. In this privacy breach case, the facts show that the last employee left the clinic at the end of the day on Friday, August 26, 2011, around 4:30 pm. The door was left unlocked to allow the cleaning staff to enter. We know that security personnel conducted its walkthrough at 6:00 pm that evening as usual and reported that the door to the clinic was locked. The door to the clinic remained locked until 7:04 am on Monday, August 29, 2011, the time at which security personnel unlocked the door to allow access for the clinic's employees. The first employee, who arrived approximately one hour later that day (just after 8:00 am) was the one who noticed that the portable computer was missing.

17. It is not clear when the portable computer was taken, but according to the investigation undertaken, it was between Friday evening and Monday morning when the clinic was left unattended as there was no sign of forced entry. A search to find the missing portable computer was unsuccessful. Security cameras located in the clinic did not record any evidence to help in this investigation. Vitalité believes the portable computer was stolen in this case and reported the theft to the police. Regrettably, there are no leads from the police regarding the possibility of recovering the portable computer.

18. The computer in question was a portable computer containing specialized software to be used in the clinic's specialized testing. It was attached by a cord and locking device to a diagnostic machine and both of these pieces of equipment were placed on a mobile cart.

19. It was only discovered after the theft that the cord which attached the portable computer to the diagnostic machine and which was left behind along with a broken piece of the locking device, was supposed to be attached to the portable computer to secure it from removal. Instead, the cord had been attached to a padlock. Attaching the cord in this way made the portable computer more likely to be taken from the clinic. A USB key to be used with this portable computer was also left behind after the theft.

20. In accordance with Vitalité's policy, data recorded on the portable computer was supposed to be encrypted and accessed by a USB key that contained encryption software. In addition, Vitalité's approved procedure regarding storage of such sensitive data requires employees not to save the data on the computer's hard drive, but rather on the secure network system (referred to as MediTech), a system managed by FacilicorpNB. Facilicorp NB provides information technology support services to Vitalité, among others in this Province's health care system. Facilicorp NB is responsible for the installation of all computer hardware in the Vitalité organization but the use of the computers, including how the data will be placed and/or stored on the computers, remains the responsibility of institutions which use the equipment, such as the hospitals, the clinics, and their staff. Storing the data on the secure network system allows the data to be retrieved in the event of a computer malfunction, or a theft, such as occurred in this case.

21. The investigation in this case revealed that the medical information belonging to the clinic's patients had in fact been stored directly on the portable computer's hard drive. On occasion, information would be saved directly to the desktop of the computer in order for the staff to access the information in a quick manner. Further, the data recorded on the portable computer was not encrypted. These actions made the data accessible to anyone without having to use a specialized USB key containing encryption software.

22. The medical information was therefore lost with the theft of the computer. Luckily, staff of the clinic had a practice of generating a printable format of the patients' diagnostic information so that it could be reviewed and interpreted later, and these paper reports were placed in the patients' files. It is for this reason alone that the personal health information of these patients was not entirely lost.

23. The portable computer in question contained personal health information regarding diagnostics of approximately 550 patients of the clinic, including their names, sex, dates of birth, the names of the physician requesting the test, and some notes regarding the patient's diagnosis; however, none of the patients' address, Medicare number, or phone number were stored on this portable computer.

What is an acceptable level of security of the information?

24. Protection of sensitive data is done by adopting information practices that include reasonable administrative, technical and physical safeguards. While the administrative safeguards will ensure that the accuracy and integrity of the information is maintained (for instance, privacy policies and procedures, staff training on policies and procedures), physical and technical safeguards ensure that the sensitive data remains confidential and secure:

Physical safeguards include:
- physical building security;
- locked filing cabinets;
- locked storage areas, mobile devices being securely stored when not in use (not to be left unattended on a desk, etc.);
- secure practices when staff is away from desk or computer during the day or in the evening (cleaning staff/who has access?, etc.).

Technical safeguards include:
- access controls to ensure only employees who need to access the information to do their jobs are given access;
- strong passwords and encryption for computers, wireless networks and all mobile devices;
- automatic log-offs and machine locking when devices are not in use, etc.

25. Notably, custodians who maintain 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, portable computers, etc.) by ensuring that such devices are password protected at all times, by changing passwords regularly, and by ensuring that the information is encrypted so that it cannot be accessed if the device is lost or stolen. Mobile electronic devices should never be left unattended and be stored in a physical area that limits access to only those who have the proper authorization.

26. Electronic devices used to store personal health information, such as in the case of a portable 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;
> (…)

27. The *Act* not only mandates the use of security safeguards, but also establishes a pragmatic way to implement safeguards by referring to two standards (described in subsections 50(1) and 50(2)), that of :

a) reasonableness; and,
b) appropriateness for the level of the data's sensitivity.

28. 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.

29. 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.

30. Again, circumstances will determine which level of security measures are reasonably needed to protect personal health information in each case. For example, a computer disk containing the names of physicians who are scheduled to participate in a health survey will not demand the same security measures as a computer disk containing the medical files of their

patients. As is noted above, these additional requirements are intended to make everyone aware of the higher degree of attention required whenever protecting personal health information in electronic format. Passwords and encryption for data stored on computers have become the standard, and they must be used in wireless networked systems, flash drives, and other mobile electronic devices such as portable computers.

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

Why was the computer located in an area accessible to the public where it could be stolen?

32. The main concern expressed by affected individuals in this privacy breach incident was why a portable computer, i.e., a mobile device, containing sensitive personal health information of hundreds of patients, was so susceptible to theft. The area where the clinic is located is regularly patrolled by security personnel; however, the portable computer did not remain secure.

33. According to the facts obtained, the clinic (the room) where the portable computer was located was left unlocked and unattended for a short period of time starting at 4:30 pm on Friday night when its door was left open for cleaning staff until cleaning staff closed the door when done. It is not known precisely what time the cleaning staff finished on that Friday evening, but we know, from the security personnel's evidence, that the door was locked at 6:00 p.m. We recall the fact that other people remain present in the treatment centre, where the clinic is located, even after the clinic's door is left unlocked and unattended at 4:30 pm, and this, until 7:00 pm. In addition, on the Monday morning in question, if the portable computer was not stolen on Friday night before the room was locked, it would have been left unattended in an unlocked room for approximately one hour between the time the room was unlocked at 7:04 am and the time when the clinic's first employee arrived around 8:00 am.

34. Hospital staff believed that they had locked the computer in place; however, the portable computer had been removed from the locking device that was meant to keep it securely attached to the mobile unit (diagnostic equipment).

35. Adopting more secure methods to protect the portable computer during the times when the door to the room is left opened yet unattended is essential. Having a staff member of the clinic or the treatment centre check on the unlocked room during those times when the

room is still accessible to the public but left unattended would be a reasonable security measure given the need to protect the portable computer which is used to collect such sensitive data. At a minimum, the portable computer ought to have been securely locked in the manner in which it was supposed to be. While it may have seemed less important to check the locking device rather than providing a service to patients, and necessary to provide access to cleaning staff, the responsibility to protect the data stored on the portable computer remained.

36. More conclusively, this incident demonstrates the vital requirement of not storing such sensitive data on the hard drive of any portable computer. This action alone is a direct cause of this privacy breach. Rules have been established by Facilicorp NB and Vitalité directing staff from storing (saving) the data collected from patients, i.e., their personal health information, on the computer's main drive. Rather, employees must take the additional step of ensuring that the data is stored directly on the secure network MediTech system. Today, the *Act* makes these same rules mandatory: protect the data at all times.

Why did the computer not contain more security features?

37. This question is simple, yet it carries so much weight in light of the facts which caused this incident. The stolen portable computer was used to store very sensitive medical information belonging to several hundred patients when it should not have been used in this way, and without encryption, making the data completely accessible to unauthorized users, including the thief or thieves.

38. Hundreds of patients who benefited from the services provided by the clinic in exchange entrusted their sensitive information to those who operate it. The clinic, together with the Hospital and Vitalité, therefore owed a duty to protect the personal health information of these patients, and in accordance with subsection 50(1) of the *Act,* to protect it at all times with a high level of security. Regrettably, these custodians failed to protect the information in this manner.

39. In this case, the portable computer was not password protected and the data was not encrypted as was required. The data was stored on its hard drive, rather than on MediTech, the secure network. On occasion, information collected was saved directly to the computer's desktop in order to access the data quickly. We were assured that all computers, whether portable or desktop, used by staff of the Vitalité, carry the same level of security features such as password protection to prevent unauthorized access; however, no explanation was provided as to why this portable computer did not carry password protection.

40. Additionally, for the majority of clinics under management by Vitalité, the personal health information collected on computers is stored on the MediTech system run by FacilicorpNB. To access the MediTech system, two levels of passwords are needed before being able to access the data. Again, in this case, the sensitive data was arbitrarily stored on the portable computer's hard drive making the personal health information less secure. While that practice 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.

41. The use of passwords and storage of data on the system run by FacilicorpNB are, in our view, proper security safeguards for the personal health information collected from patients at the Hospital, the treatment centre, and the clinic. Such information should not have been stored on the portable computer's hard drive, and it could have been lost forever had it not been for the printed paper format reports placed in the patients' files.

42. Given the sensitivity and amount of personal health information of hundreds of patients' electronic files stored on the portable computer, we find that it is reasonable to demand a very high standard of security safeguards in this case. Unfortunately, we found deficiencies in the security of the data to include:

- the room where the portable computer was located left unattended for a short period of time on a regular basis in a busy clinic and in the treatment centre known to be accessible by the public;
- not securely locking the portable computer to the mobile diagnostic equipment as required;
- using an unapproved practice of storing highly sensitive patient personal health information on the portable computer's hard drive;
- not adopting the approved practice of storing (and therefore backing up) the data on the secure network known as MediTech;
- not using password protection on the portable computer containing highly sensitive patient personal health information; and,
- not using data encryption for the highly sensitive patient personal health information stored on the portable computer.

43. For these reasons, we find that the security measures collectively adopted and used by the Hospital, the treatment centre, the clinic and Vitalité at the time of the breach did not meet the standards required of custodians for the protection of personal health information of patients under the *Act*, and the measures in effect at that time were not in compliance with the

Act. We find these custodians to have failed in their lawful duty to protect the personal health information of the Hospital's patients.

What actions are being taken to correct the breach and to prevent similar future incidents?

44. This privacy breach incident has brought about a review by Vitalité of its security measures to protect personal health information which is placed or stored on electronic devices, as per its obligations to do so found in subsection 20(2) of the Regulations:

> 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.

45. We have also been informed that Vitalité has reviewed its policy regarding the use of portable computers and whether it is appropriate for the clinic to use a portable computer in this manner. It was determined that the portable computer, which is attached to the diagnostic machine on the cart, is the best equipment to carry out the testing on patients due to its mobility. Having said this, however, and while mobile units such as these will continue to be used, Vitalité will no longer authorize staff to use portable computers to store the personal health information of patients.

46. Also as a direct consequence of this privacy breach, Vitalité has recommended to all outpatients clinics under its management to conduct a review of their security measures currently in place regarding the protection of computers placed in similar examination or testing rooms to ensure that they are compliant with the security safeguards outlined in the *Act*, particularly with a view to prevent similar privacy breaches in the future.

47. We know that other security measures have now been instituted to prevent similar privacy breaches from occurring, and these measures include:

- staff can only use the new portable computer acquired for the clinic with a username and password;
- usernames and passwords have been assigned only to those health professionals who need to use the machine for urodynamic testing at the clinic;
- the access key that allows an employee to operate the portable computer is currently stored securely;
- the new portable computer is now attached to the mobile diagnostic equipment on that cart unit with a metal cable that increases the level of protection against theft

and any attempt to remove the portable computer unlawfully will cause the display screen to be damaged, thereby making it very difficult to be removed or taken;

- patient information collected is now stored directly on the secure information network MediTech managed by FacilicorpNB rather than on the hard drive of the portable computer; and,
- a secure back-up copy of the patient data collected will be prepared by FacilicorpNB for the clinic.

48. While they are not subject to the *Act*, we know that cleaning staff of the treatment centre and the clinic have access to rooms and offices where patients' personal health information is stored. We were assured by Vitalité that cleaning staff does receive training regarding the importance of protecting equipment in a hospital setting that contains sensitive data and that this training is the same as that provided to health care employees on the very topic of protection of the information.

49. Finally, and also part of Vitalité's review in this matter, the Commissioner will be kept informed of the various steps undertaken to ensure that all involved in this case incorporate the security safeguards mandated by the *Act*.

Could loss of personal information lead to identity theft and affect one's financial history?

50. Another main concern brought to our attention was the risk of identity theft due to the loss of personal health information. The information lost in this case includes patients' names and other medical information, but fortunately, the lost data did not include the patients' Medicare number, phone number, or address.

51. 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 isn't any 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. We would consider this concern to be lower in this case given the fact that the personal information lost in this privacy the breach did not contain a lot of identifying information.

52. There is no agreement on the meaning of "identity theft," but the term is used for everything from cheque forgery and the use of stolen credit cards to sophisticated scams in which an impostor adopts somebody else's identity to gain access to their assets. Children, or

persons under the age of 19 years, cannot establish financial or other credit history due to their age; as a consequence, being watchful of their lost personal information would not include credit monitoring.

53. 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).

Commissioner's concluding comments

54. Our work with officials from Vitalité Health Network and the Dr. Georges-L.-Dumont University Hospital Centre in this privacy breach provided all the facts as described in this Report. Immediate action was taken to gather the preliminary facts and the Commissioner's Office as well as individuals affected by this privacy breach were notified in a timely manner.

55. This breach incident was substantial in that it affected a large number of patients of one clinic, where all data collected was stored on a single portable computer, without proper security measures to protect the sensitive information. These details highlighted to all concerned how easily a violation of one's privacy can occur when proper safeguards are not in place.

56. Our investigation also led us to meet with officials from FacilicorpNB and learn more about the interplay between it and Vitalité in the installation, use, and overall responsibility of the equipment used for the collection, use and storage of patient's medical information. We are assured that both are aware of their respective duties and of the need to remain vigilant on the adoption and respect of policies regarding the collection and storage of personal health information, the secure manner in using mobile electronic devices such as portable computers, and the overall use of proper security measures to protect patient information at all times.

57. Improved protective practices have already been put in place to better safeguard personal health information collected from patients when a specialized mobile unit such as the one in this case must be used. Sensitive data collected in this fashion will no longer be stored directly on the portable computer's hard drive, but rather on the secure network maintained by FacilicorpNB. We are confident that these corrective measures now implemented will ensure greater protection of patient information in the future.

58. Finally, it is important to state that 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.

RECOMMENDATIONS

59. Based on the above findings, the Commissioner agrees with the measures undertaken by Vitalité to prevent further occurrences of similar type privacy breaches, namely that:

- Vitalité must review its security measures to protect personal health information which is placed or stored on electronic devices, as per the obligations under the *Act*;
- Vitalité must review the policy regarding the use of portable computers and whether it is appropriate for the clinic to use a portable computer in this manner;
- all outpatients clinics under the management of Vitalité will conduct a review of their security measures currently in place regarding the protection of computers placed in similar examination or testing rooms to ensure that they are compliant with the security safeguards outlined in the *Act*;
- staff can only use the new portable computer acquired for the clinic with a username and password;

- usernames and passwords must be assigned only to those health professionals who need to use the machine for urodynamic testing at the clinic;
- the access key that allows an employee to operate the portable computer be stored securely;
- the new portable computer be attached to the mobile diagnostic equipment on that cart unit with a metal cable the way it was intended to in order to make it very difficult to be removed or taken;
- the patient information collected will be stored directly on the secure information network MediTech managed by FacilicorpNB rather than on the hard drive of the portable computer; and,
- Vitalité ensures the clinic makes arrangements with FacilicorpNB to back up the patient information collected.

60. The Commissioner's Office will follow-up with Vitalité in December 2012 to ensure that these steps have been undertaken.

Issued at Fredericton, New Brunswick, this 13th day of September, 2012.

_____

Anne E. Bertrand, Q.C.
Commissioner