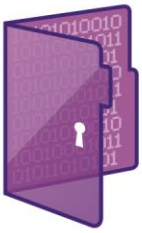
Office of the Access to Information and Privacy Commissioner
New Brunswick



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: 2012-743-H-236

Complaint Matters: 2012-816-H-255, 2012-818-H-257, 2012-819-H-258, 2012-821-H-260, 2012-823-H-261, 2012-826-H-262, 2012-829-H-264, 2012-831-H-265, 2012-873-H-273

Date: June 5, 2013

Commissioner's Investigation

Privacy breaches - unauthorized access

Introduction

1. This Report of the Commissioner's Findings is issued following several complaints that were made to the Office of the Access to Information and Privacy Commissioner. The complainants alleged that the Lamèque Hospital and Community Health Centre (hereinafter the "Hospital and Community Health Centre") and Vitalité Health Network failed to safeguard their personal health information, in violation of the *Personal Health Information Privacy and Access Act* (hereinafter the "*Act*").

2. In this Report of the Commissioner's Findings, we discuss our conclusions based on the investigation we conducted alongside that carried out by Vitalité Health Network. We also provide our recommendations in this matter.

3. According to the *Act*, a privacy breach occurs when personal health information is lost, stolen, disposed of, disclosed to or accessed by an unauthorized person. When one of these situations occurs, the person, group or organization which was entrusted with the personal health information is required to take action. This person, group or organization is referred to as a "custodian" under the *Act*. A custodian is one that handles personal health information in order to provide or assist in the delivery of health care.

4. In this case, the Hospital and Community Health Centre and Vitalité Health Network are both custodians, that is, organizations in the health care system upon whom it was incumbent to protect the personal health information of patients particularly affected by incidents of privacy breach in this case. In that regard, these two custodians must answer the allegations raised in the present privacy breach cases.

Context

5. The privacy breach cases are alleged to have occurred when an employee of the Hospital and Community Health Centre accessed without authorization the electronic records containing the personal health information of more than 150 patients. Amongst those patients were co-workers, members of the employee's family and other individuals in the community.

The personal health information accessed included the following:

- patients' names
- patient's demographic data
- dates of their visits to the Hospital and Community Health Centre, and
- reasons for these visits.

6. There are also facts to suggest that some of this personal health information may have been disclosed by the employee in question, in violation of the *Act*.

7. Before we begin with our findings concerning these privacy breach cases, we feel it to be appropriate to describe the custodians in this case, their duties and, lastly, how the breaches occurred.

8. Vitalité Health Network is a Francophone organization that manages a series of Francophone and bilingual institutions and programs. These institutions and programs have their own identity that is reflected in strong ties with the community. Vitalité Health Network, which is headquartered in Bathurst, provides health care services to around 250,000 people. Its team consists of more than 7,600 employees and nearly 470 physicians—of whom 227 are specialists—and 1,200 volunteers. Vitalité Health Network is comprised of several hospitals, community facilities, health centres, two community health centres, not to mention mental health centres, main public health offices, and many others.

9. Operating under the Vitalité Health Network umbrella, the Hospital and Community Health Centre is a unique facility designed to house not only certain clinical departments typically found in hospitals, but also those that meet a range of community health needs.

10. Among other things, the Hospital and Community Health Centre provides interdisciplinary services, for instance those found in a walk-in clinic, a doctor's office, and for physiotherapy. The following services are housed under one roof: reception and admissions, chronic condition clinics, therapies, Family Medicine Unit, Medical Unit, medical imaging, lab, food services, and many others.

11. The Hospital and Community Health Centre is therefore a significant part of the community, and it enjoys an excellent reputation among the people it serves. As we were told and as we saw for ourselves, the facility's ability to offer such a wide range of health services depends entirely on its caring and competent employees.

12. Consequently, it goes without saying that the Privacy Officer for Vitalité Health Network and the Hospital and Community Health Centre and its staff were dumbfounded upon learning of the present privacy breach cases. How could such a thing have happened in such a capable facility adamant about its primary mission to protect the privacy of its patients?

13. In fact, both custodians emphatically acknowledge and uphold their statutory duty to protect their patients' personal health information at all times, in accordance with the relevant provisions of the *Act*. Numerous security safeguards prescribed by the *Act* require that they adopt practices based on internationally recognized information technology security standards and practices that include administrative safeguards to protect this information in electronic form (section 50).

14. It is therefore incumbent upon Vitalité Health Network and the Hospital and Community Health Centre to establish a directory of patients' electronic records in sophisticated and secure computer systems. Also, since these electronic networks can be accessed fairly easily, these establishments must specifically ensure that their employees do not use them unless they have permission to do so.

15. As a result, we examined the circumstances that enabled an employee to commit such breaches of the *Act*. Neither the management nor the staff of the Hospital and Community Health Centre suspected that the employee in question was accessing the electronic records of the facility's patients, some of whom included staff members, without permission.

16. We investigated this strange conduct by examining the duties assigned to this employee at the time, the employee's level of authorized access to the patients' electronic records, supervision of the employee's work, and the security safeguards in place at the Hospital and Community Health Centre.

The employee in question

17. In this case, the employee responsible for the privacy beaches held two casual positions at the Hospital and Community Health Centre. The employee received one salary but reported to two managers: to perform clerk duties relating to admissions, registration and scheduling for patient intake; and, to provide administrative tasks to the Family Medicine Unit (being a medical doctors' office).

18. As admissions clerk, the employee had to perform various admissions processing duties, i.e., all the steps required to register hospital patients. The employee also looked after patient transfers and discharges, including for patients from the walk-in clinic. To perform these duties, the employee had to print out and prepare records, wristbands, hospital cards and forms by admission type, and perform actions in the central appointment system in the Meditech computer network.

19. While working as an admissions clerk, the employee was supervised by a manager. According to our investigation into the facts, the manager in question never had any reason to believe or suspect that the employee was accessing patients' electronic records without permission. In fact, the manager reported that the employee in question was a hard worker and got along well with the staff.

20. In the employee's administrative support position at the Family Medicine Unit, the employee performed various duties that are required in a doctor's office. One of the employee's specific duties in this position, however, was to scan medical notes and reports generated externally to the Unit in order to file them in the patients' electronic records at the Unit.

21. Once again, we were told that in supervising this employee, management was never concerned that the employee was accessing patients' electronic records without permission. As in the admissions clerk position, the employee in question was a hard worker and had a good reputation among the staff of the Family Medicine Unit.

Two computer systems

22. In our investigation of the unlawful conduct of the employee in question in this case, we took it upon ourselves to review the computer systems used by the facility's staff. The Hospital and Community Health Centre employees use two computer systems: Meditech and another software application known as Purkinje. The Meditech system is used to register patients by entering demographic data, manage patient appointments, and handle all other billing-related functions. The Purkinje system is used among others by the Family Medicine Unit, i.e., the medical support staff. In that system, doctors' notes can be transcribed and tracked following patient visits. While the Hospital and Community Health Centre also has physicians on staff, it is the Meditech computer system that is used for hospitalized patient records.

23. According to the Meditech system modules used specifically by the Hospital and Community Health Centre, doctors' notes or reports cannot be scanned by staff. Therefore, one can decipher fairly easily based on the appearance of the document whether it was created by using the Purkinje or Meditech system in that facility.

24. Consequently, when the employee in question was providing administrative support at the Family Medicine Unit, tasks performed required the use of the Purkinje system, including when having to schedule patients' appointments, scan their medical reports and any other duties of this position requiring access to the patients' electronic records.

Discovery of the privacy breaches

25. At the beginning of the work shift in the morning of February 29, 2012, an employee of the reception, admissions and appointment centre discovered a scanned document in the printer. At first glance, the employee saw that the document contained a patient's personal health information and thought this odd because it was not created using the Meditech computer system that staff at admissions use when performing their duties. The employee therefore alerted the admissions unit supervisor about this discovery.

26. The admissions unit supervisor enquired from the Hospital and Community Health Centre's clinic supervisors who scan documents as part of their duties in order to find out if one of them had inadvertently printed the document found in the printer.

27. The printers are grouped together in a multi-printer network that serves the entire facility. Since protection of the confidentiality of patient information is an overarching concern at this facility, when an employee inadvertently prints a document in another office at the Hospital and Community Health Centre outside his or her area of supervision, an incident report has to be filled out to explain why such an error occurred. In this case, the clinic supervisors informed the admissions unit supervisor that was not what had taken place.

28. Being unable to determine the origin of the document found in the printer in the admissions unit, the admissions supervisor contacted the IT support office to trace who gave the command to print the document (in other words, from which computer the document had been printed and therefore which employee had printed it during the work shift of February 28).

29. The first audit looked at the February 28, 2012 shift only. It was discovered that the employee in question had used the authorization level granted at the start of employment in the course of the tasks carried out at the Family Medicine Unit to access the electronic record where the scanned document originated. There was no indication that the employee had permission to access those electronic records. More worrisome was the fact that according to the audit, the employee in question had accessed not only records that were not related to the employee's duties as an admissions clerk, but also to 33 records in the Purkinje computer system, despite not having permission to do so when the files were accessed.

30. On discovering these facts, the admissions supervisor wondered whether the employee in question had been catching up on work that was normally part of the employee's duties at the Family Medicine Unit (scanning medical notes and reports using the Purkinje system). In other words, during the shift of the previous evening, was the employee doing work for the Family Medicine Unit while on duty in the admissions department, i.e. the employee's second position? The manager of the Family Medicine Unit informed the supervisor that this was not the case.

31. These facts raised doubts for management at the Hospital and Community Health Centre as to whether the access undertaken by the employee was legitimate. The facility therefore contacted the Privacy Officer for Vitalité Health Network on March 1, 2012 and a decision was made to conduct a six month audit of the employee's access history. Additionally, the electronic access of this employee was immediately revoked and the employee was suspended from work during the investigation. This audit revealed that more non-authorized access had been performed by the employee in question during this period.

32. The manager met with the employee on March 2 to find out why the document had been printed while the employee was working in the admissions unit. The employee did not provide a satisfactory response and denied having accessed information when not authorized to do so. When confronted with the results of the first audit (of February 28) which presented proof of non-authorized access, the employee modified the statement given and this reaction raised suspicion on the part of the manager.

33. Therefore, on March 13, the facility undertook to carry out a third audit without delay to determine the access carried out by the employee from the date at which the employee was first employed (approximately a three year period). This third audit revealed that the employee in question had accessed more than 150 electronic records of several patients,

including those of co-workers who were themselves patients, members of the employee's family and friends, when the employee had no right to do so.

Breach Notification Process

34. In accordance with the *Act*, a custodian, such as the Hospital and Community Health Centre or Vitalité Health Network, who discovers that a privacy breach has taken place, must notify the Commissioner immediately. The custodian must also notify everyone affected that the confidentiality of their personal health information has been compromised. This notification process is set out in section 49(1)(*c*) of the *Act* and is mandatory in most cases.

35. In this notification process, the affected individuals must be informed as to what has occurred and when the incident took place. The *Act* and its Regulations require the custodian to provide the following information in such cases:

    a) the name of the custodian;
    b) the name and contact information of the person designated by the custodian to respond to inquiries about the custodian's information practices;
    c) a description of the nature of the privacy breach;
    d) the date and location of the privacy breach; and
    e) the date the privacy breach came to the custodian's attention.

36. In addition, these individuals must be advised of their right to file a complaint with the Commissioner. The custodian may waive its obligation to issue such a notice, but only in specific and limited circumstances, which did not exist here.

37. In the notification process of the present matter, however, Vitalité Health Network wondered whether notification could be dispensed with in certain cases. For example, should notification be made if:

    - the notice, by virtue of its contents, would disclose the name of the member of the custodian's staff, or even identify those persons whose privacy was also breached?
    - in the case of breaches in a small community where the custodian, its employees and the persons concerned all know each other, the act of notifying the members of the community could reveal the name of the employee responsible for the breaches, or make it possible for some people to easily determine who the other victims of the breaches are?

- it could reveal to the community the name of the employee responsible for the breaches and therefore cause trouble for the employee?

38. In our view, while these are valid concerns, they cannot allow a custodian to set aside its statutory duty to notify everyone affected by a privacy breach. The primary purpose of the *Act* is to protect the privacy of persons whose personal health information has been entrusted to a custodian. The *Act* also requires custodians to be transparent in their practices for handling the personal health information entrusted to them, and to ensure that these practices are followed at all times. Furthermore, custodians are responsible for the actions of their employees in connection with the personal health information entrusted to them, and the persons affected by a privacy breach have the right to know that their personal health information has been compromised.

39. The *Act* was neither intended to conceal the conduct of the custodian (or its staff) that led it to fail in its legal obligation, nor to hide its identity in privacy breach cases. On the contrary, and for this reason, the notification process under the *Act* requires that the custodian in question be named. Any person affected by a privacy breach has the right to file a complaint with the Commissioner, and the custodian will not be permitted to abstain from answering the questions that ensue, including explaining how the breach occurred and who is responsible.

40. While we understand that the notification process is arduous in most cases, we firmly believe that notification will prove beneficial for everyone by:

- making the custodian accountable for its statutory obligations;
- reassuring the person affected that such conduct will not be repeated in the future; and
- prompting the custodian to rebuild the individual's trust, which without question will have been shaken by the privacy breach.

Notification in these cases

41. We find that Vitalité Health Network discharged its duty to notify in the present cases. When the multiple instances of unauthorized access were discovered, Vitalité reported these privacy breaches to the Commissioner on March 8, 2012. Naturally, Vitalité and the Hospital and Community Health Centre wanted to notify the community about the breaches immediately.

42. More imminently, both custodians wanted to reassure the community that such conduct by their employees was very rare, that it would not be tolerated and that it in no way reflected just how seriously the facility and staff took the privacy of the public's personal health information.

43. Given its obligations under the *Act*, nothing in these cases prevented Vitalité Health Network from notifying the persons affected by the unauthorized access to their medical records:

- of the reason why such an incident occurred; and
- by virtue of its nature and explanations, notification could result in the identification of other affected persons or reveal the identity of the employee responsible for the breaches.

44. Vitalité began notifying the affected persons by mail in April 2012. Each notification letter informed them of the privacy breach resulting from unauthorized access to personal health information by a Hospital and Community Health Centre employee. These persons were also advised that they had the right to file a complaint with the Commissioner regarding the breach.

45. Of the hundreds of persons notified, several turned directly to the Hospital and Community Health Centre for further information, and staff had to answer numerous questions about the incident. These individuals were referred to Vitalité's Privacy Officer. More than 50 individuals contacted her office.

46. Several individuals affected by the breaches contacted Vitalité's Privacy Officer to find out the name of the employee responsible. In keeping with its obligations set out under the *Act* and the advice we gave Vitalité on this issue, the identity of the employee in question was disclosed only to those affected persons.

47. Roughly 30 of these individuals asked the Hospital and Community Health Centre for a copy of their personal health information that the employee in question had accessed without their consent.

48. Several of these individuals also contacted our Office to share their concerns and ask for information. Of these, nine filed a complaint under the *Act*. Their complaints are summarized in their questions below:

- What is the name of the employee who committed the breach?
- How and why did the breach occur?

- Does the employee in question still work at Vitalité Health Network? and
- Could the privacy breach result in identity theft?

Identity of the person who caused the breach

49. Failing in one's duty to protect a person's privacy is not an offence. Collecting, using or disclosing personal health information in wilful contravention of the *Act*, however, does constitute an offence under section 76.

50. An employee of a custodian who accesses and wilfully discloses personal health information without authorization to do so commits an offence under section 76(2). An offence is punishable under Part II of the *Provincial Offences Procedure Act*, and proceedings in relation to an offence are initiated by laying an *information* with a Provincial Court judge.

51. Having debated the matter of the custodian's duty to report privacy breaches, even though the breaches affect the privacy of several people in a small community, we point out that protecting the identity of the employee responsible for the breaches is not a relevant consideration in the custodian's decision whether or not to issue notices to the affected individuals. Similarly, there are no grounds for not disclosing the name of the employee responsible to the affected individuals who ask the custodian for it.

52. We are not recommending that the names of employees responsible for privacy breaches be publicly announced. There is nothing stipulated in the *Act*, however, that prevents the person affected by such a breach from being notified of the employee's name when that person so requests.

Why and how did the employee commit these breaches?

Access authorization and permission to use it

53. To properly understand how the employee committed the multiple privacy breaches, it would be appropriate for us to explain how the computer systems used at the Hospital and Community Health Centre operate.

54. Patients' personal health information is stored in electronic records created in the Meditech and Purkinje computer systems. Confidential data collected by the staff is

governed by the overarching principle of maintaining the confidentiality of personal health information at all times.

55. The Privacy Officer for Vitalité Health Network and the Director of the Hospital and Community Health Centre told us that they take the importance of confidentiality in the workplace seriously. The concept of confidentiality is discussed when applicants are interviewed for positions at the facility. Applicants are judged by their reactions and responses to scenarios designed to illustrate the importance of maintaining confidentiality. This confidentiality affects the privacy of patients, co-workers and the facility.

56. When new employees are hired, they take part in a general orientation program that includes an awareness session about confidentiality. Attendance at this session is compulsory. Employees are also required to sign a form acknowledging their duty to uphold confidentiality, and this procedure is repeated annually when employees' performance is appraised.

57. Before granting authorization to access data containing the personal health information of patients in the Meditech and Purkinje systems, supervisors must first specify what the new employee's level of authorization will be. This is done at the time of hiring. In other words, the supervisor will determine the access level that new employee needs in order to perform the duties of his or her position.

58. Access levels are granted on a password basis. Passwords are issued based on the instructions given by supervisors. Vitalité notifies FacilicorpNB of new the employee's name and level of authorization for access to the systems, and it obtains the passwords created for the new employee. FacilicorpNB is a public agency that provides IT support services to Vitalité Health Network, as well as others in the Province's health care system. Although FacilicorpNB installs and maintains all the computer hardware in the institutions in the Vitalité Health Network, including the secure network and computer systems, the facilities themselves are responsible for giving direction to their staff on the use of these work tools when processing data, i.e. the personal health information of their clients and/or patients.

59. Lastly, to access the Meditech and Purkinje systems, the employee needs a user number which is provided at the start of employment, as well as two passwords. The first password allows the employee to access Vitalité's secure network, i.e. the network managed by FacilicorpNB. The employee is given a second password to access the

Meditech and Purkinje computer systems. Where the employee's duties require work to be done in both computer systems, he or she uses the same second password to access either system.

60. A new Hospital and Community Health Centre employee therefore receives authorization to access Vitalité's secure network, in addition to a second password for accessing the Meditech and/or Purkinje systems. It is the duties of the employee's position (or positions) however that determines when the employee may use this authorization. In other words, at what point in the employee's work he or she will be permitted to use his or her authorization to access patient records in the Meditech and/or Purkinje systems.

61. A new employee at a medical clinic who is granted the authorization to access the medical records of every patient at the clinic will not have permission to access the records of every patient on any day. The employee has the authority to access the information at all times but he or she is not permitted at all times to do so.

62. The employee will only be permitted to do so if he or she has to perform a task or provide a service for a patient that requires access to that patient's personal information.

63. Consequently, to illustrate this concept, the employee of a medical clinic has permission to access Patient Smith's record:

- When the employee must verify Patient Smith's next appointment and to provide the date; or
- When the doctor asks the employee to send a medical report about Patient Smith to another clinic. At that moment, the employee has permission to access Patient Smith's record to obtain the report. Once the employee has completed that very task, however, he or she no longer has permission to access Patient Smith's file unless asked to perform another service or task for this patient.

Authorization granted to the employee in question

64. When the employee in question was hired, the Hospital and Community Health Centre granted the authorization level that was deemed necessary to access the computer systems in order to perform the duties of both positions. Since the employee had to access the Meditech computer system in order to perform the duties of admissions clerk in addition to the Purkinje system in order to provide administrative support to the Family

Medicine Unit, the employee was granted a first password to use the secure network, and a second password for the Meditech and Purkinje systems.

65. The Meditech access authorization level that was granted to the employee was based on the need to register patients and manage their appointments. The authorization level granted to the employee to access the Purkinje system, however, was much broader given the multitude of administrative support duties to be performed at the Family Medicine Unit. The employee in question was therefore authorized to access patients' entire medical histories, in addition to information about care incidences, current and previous medication, lab results, and many more information found in the patients' records.

66. In addition, the employee in question did not have to be working directly at the Family Medicine Unit to access the Purkinje system, because it could be accessed from the computer available to the employee in admissions while working in that area. The employee in question could therefore access patient records in the Purkinje system from the employee's computer in the admissions unit. This was how the document created in the Purkinje information system ended up on the printer in the admissions unit, resulting in the discovery of the privacy breaches in this case.

67. Confronted with the findings of the audits conducted in this case, the employee in question admitted having accessed the records without permission, but denied using or sharing the information. The employee in question explained having done so out of personal curiosity. It appeared that the employee was having personal problems, and to ease the tension, the employee would check out what problems other people were having by looking at their demographic data, i.e., dates of and reasons for their visits.

The employee in question did not have permission

68. It is acknowledged that the employee in question had the necessary authorization to access the electronic records of Hospital and Community Health Centre patients in the Meditech and Purkinje systems to perform the duties of both positions. The facts are clear, however, that the employee did not have permission and was therefore not allowed to access the electronic records of the 150 patients in the Purkinje system, which included co-workers and family members, at the moment when the employee did so.

69. In fact, the employee in question was not allowed to make any of the accesses in the previous years that were uncovered by Vitalité Health Network's audits carried out in this case.

70. In addition, the employee clearly violated the *Act* by using the said confidential information, i.e., printing them on a Hospital and Community Health Centre printer. We also discovered that, over the same period of time the employee is accused of breaching the privacy of several people in the community, one of the persons affected was questioned by someone else about a particular aspect of their physical health that could only have been known if someone had read or disclosed that individual's personal information from their medical file.

71. For these reasons, we have strong doubts regarding the sincerity of the employee's explanations when the employee states not having intended to use or share the personal information of the individuals gravely offended by the employee's actions. Nor can we accept the employee's explanation—that the employee repeatedly breached the privacy of so many people over three years and counting, solely to satisfy personal curiosity.

72. In our opinion, the employee in question committed a most egregious breach of the *Act*. The employee in question wilfully and repeatedly accessed the patient records in violation of the *Act*, disregarding not only the employee's statutory and employment-related duties, but also the privacy of the persons known to the employee.

Is the employee responsible still working for Vitalité Health Network?

73. When the Hospital and Community Health Centre and Vitalité Health Network became aware of these privacy breaches, Vitalité immediately revoked the employee's access to all the computer systems. In addition, the employee was suspended for the duration of Vitalité's investigation. After the extent of the breaches became known, the employee was removed from both positions, and we are told that the employee in question no longer works in any Vitalité Health Network facility.

Could unauthorized access to personal information lead to identity theft?

74. Another concern brought to our attention was the risk of identity theft due to the unauthorized access to personal health information.

75. In these privacy breach cases, the employee responsible does not seem to have been motivated by a desire to steal the identities of the persons affected. As indicated above, we do not accept the employee's explanation for snooping in the medical records of all these people, namely that the employee did so simply to satisfy personal curiosity or a

personal need. Having said this, there is nothing that would lead us to believe that the employee in question wanted to mine the identities of these persons for fraudulent purposes.

76. Nonetheless, we cannot assume that there is no risk of identity theft when the integrity of this personal information has been compromised. For this reason, we provide advice in that regard.

77. 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 and persons under 19 years of age 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.

78. 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. The following are some examples:

- 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 difficult for anyone to guess;
- remaining vigilant and suspicious of emails which appear to come from banks, government agencies or credit card companies and ask to provide personal information online. Actual banks and other agencies do not send such emails, yet scammers often use their logos to make their fraudulent messages look authentic; and
- reading 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 under *Identity Theft and You*, then *Guidance Document*).

Measures being taken to correct these breaches and to prevent similar future incidents

79. Certainly, this case will not stop the necessary authorizations from being granted to employees so they can access patients' electronic records in the course of their duties. Nonetheless, these privacy breaches have prompted a review of the security measures that Vitalité Health Network and the Hospital and Community Health Centre use to protect the confidentiality of the personal health informed stored in the electronic records under their control.

80. This review is essential for the said custodians to satisfy their obligation set out in section 20(2) of the *Act*:

> *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.*

81. In addition, and considering that the scope of the misconduct by the employee in question went unnoticed despite regular supervision, a review of the security safeguards governing the granting of authorizations and permission to use them is essential.

82. In that regard, officials of Vitalité Health Network and the Director of the Hospital and Community Health Centre continue to stress the importance of confidentiality in the workplace. As indicated above, new employees take part in a compulsory session on confidentiality and are required to sign a form during their annual performance appraisals to indicate that they understand their duty to uphold confidentiality. Staff may also be given additional training on confidentiality through education sessions offered by Vitalité. These sessions are offered throughout Vitalité's network, and PowerPoint presentations are made available on the shared directories in each zone, such that employees can access them at any time.

83. The awareness sessions informing employees about the importance of the confidentiality of patients' personal health information underscore the seriousness of privacy breaches and, more specifically, the difference between inadvertent breaches and wilful breaches. Also, employees are educated that *deliberately* violating the *Act* will lead to consequences

based on the circumstances of the incident, ranging, for example, from a simple warning from the manager and suspension from duty to more severe measures, up to and including the laying of an information for committing an offence under the *Act*.

84. Although Vitalité has explained to us that awareness sessions are given to all new employees, we learned that this training is not mandatory for employees already in Vitalité's employ. The module designed to educate employees about the importance of confidentiality and patient privacy has been given only to employees in Vitalité Zone 1. Unfortunately, we are told that to date that only 2,700 of Vitalité's 7,000 employees have taken part in these training sessions. Vitalité has committed to providing this training to employees in the other zones, and, to facilitate their participation, the training will be offered in person and online.

85. As of this writing, the Hospital and Community Health Centre staff has received this training. In addition, the Director of the Hospital and Community Health Centre has reassured us—and we truly believe—that she is taking every possible opportunity to remind her staff about the importance of confidentiality both during and after office hours.

86. The duty to protect patients' personal health information at all times at the Hospital and Community Health Centre is posted in every department. In order to increase staff awareness of its duty to maintain the confidentiality of personal health information, the Director of the Hospital and Community Health Centre Director told us that she has held several meetings with employees to inform them about the situation and about possible repercussions of failing to discharge their duty. We point out that none of the names of the patients affected were disclosed during these meetings.

87. Most employees took part and were able to talk among themselves not only about their concerns, but also about the impact of these privacy breaches on them and their family members. While no one realized that the employee in question had been committing such breaches, everyone felt ashamed about it.

88. Without being asked to do so, the staff volunteered on the spot to sign the personal health information confidentiality form, clearly signalling that the misconduct of the employee in question was not under any circumstances to be considered a reflection of their ethics or honesty.

89. The facility and the community it serves suffered during this unfortunate episode and want nothing more than to rebuild public trust. In our opinion, and as our observations lead us to believe, the Hospital and Community Health Centre will regain the public's trust as time passes, given all the new data protection measures it has put into place.

90. As a direct consequence of these privacy breaches, Vitalité Health Network has also told us that it is currently reviewing the policy on the audits it conducts to monitor staff compliance with patient privacy. Vitalité currently relies on FacilicorpNB to perform audits on request as well as random audits. The audit reports are subsequently forwarded to Vitalité's Chief Privacy Officer for validation and follow-up. Vitalité has indicated that when FacilicorpNB is asked to perform audits, it produces access history reports which reveal dates, the user, patient files that were accessed, and the type of access.

91. Vitalité is currently doing test-runs with data access policies, the purpose of which is to establish parameters for performing random audits. These audits could detect cases of unauthorized access sooner and prevent privacy breaches of the scope that the custodians and members of the public were confronted with in this case.

92. For this reason, we suggest that Vitalité Health Network continue its efforts along these lines. More urgently, we recommend that it conduct random audits to detect cases of unauthorized access more quickly. In that regard, and to prevent any more employees from accessing patient records without permission, Vitalité has already informed its employees of its intention to conduct random audits.

93. The Commissioner will ensure that she be kept informed of the various measures undertaken so she can be certain the confidentiality and security of the personal health information of the patients served by the Hospital and Community Health Centre and Vitalité Health Network is being maintained.

Commissioner's final remarks

94. Our investigation revealed cases of grave breaches in that they had the effect of violating the privacy of a very large number of individuals and were committed over several years by a single employee in a hospital in a small community where the employee and the victims live and know each other.

95. The Hospital and Community Health Centre and Vitalité Health Network have assured us that they continue to be mindful of their obligations and of the need to remain vigilant

concerning the adoption of and compliance with policies on access to personal health information, and the general application of appropriate security measures to protect the personal health information of patients at all times.

96. Enhanced precautionary measures are being implemented to improve the protection of personal health information obtained from patients. Audits will no longer be conducted only when a privacy breach is discovered or suspected. Rather, they will be conducted randomly to identify breaches more quickly. In addition, compulsory awareness sessions for all employees will help educate them about the importance of the confidentiality of patients' personal health information.

97. We are hopeful that the corrective measures being applied will better protect patient information in the future.

98. In conclusion, we add that the *Act* is intended to improve health care by ensuring that patients feel comfortable disclosing their personal health information to hospital and medical staff, knowing that their confidential information will be used as efficiently and securely as possible. This trust is based not only on the benefits supporting the delivery of health care, such as the creation of computer systems that hold the medical records of thousands of people and provides ready access to them. It is also based on the premise that only those persons who are authorized to access these systems will use them to carry out their duties, and only when they have permission to do so rather than to satisfy a personal need.

99. A policy intended to educate employees about their obligation to protect the patients' privacy when they are dealing with the personal health information of individuals in their community, along with a caution that shirking that obligation can have repercussions, is in our opinion an essential practice for the custodian to meet its statutory obligations under the *Act.*

100. While a policy to protect vital information should be instituted, it is meaningless if steps cannot be taken to verify compliance. In our opinion, better outcomes will be obtained by adopting good practices, including ongoing efforts to remind employees about their duty to protect the confidentiality of personal information.

101. A practice aimed at encouraging employees to admit the mistakes they make when handling confidential information is wise when those incidents involve accidental privacy violations. A custodian seeking to sustain this practice by reassuring staff that no one will

be blamed even where there is proof of a wilful violation of the *Act* would be, in our view, a serious departure from its statutory obligations.

102. This matter illustrates the ease with which employees can access personal information when given authorization to do so when they are hired. Being able to browse with ease through medical records without fear, guilt or reprisal, as was demonstrated in this matter by the employee responsible for causing several hundred privacy breaches, is the single reason why we support Vitalité Health Network's efforts to undertake a much stricter surveillance by performing random audits of access to computer systems.

103. In our view, it is certainly possible to prevent any recurrence of such privacy violations by adopting a practice to amend or remove the access authorization that is first given to employees at the start of their employment in cases where they change jobs or when they have completed a task and no longer require access to certain information - in specific computer systems - to carry on with their work.

104. Still, these efforts alone will not serve as a deterrent to prevent others from attempting to commit similar violations in the future. We must dissuade all those responsible for the protection of confidential information entrusted to them who are indifferent to the privacy of the individuals to whom the information belongs.

105. This is why we are contemplating harsher measures against the employee in question, i.e., possibly laying *informations* against this person for having committed multiple violations of the *Act*. As indicated above, an employee of a custodian commits an offence if, without the employer's authorization, he or she wilfully discloses personal health information in circumstances where the employer would not be authorized to disclose the information under the *Act*.

106. In this case, it is clear that the employee in question violated the *Act* and committed offences on several occasions. The employee admitted to accessing the personal health information of more than 150 patients without permission, and therefore did so deliberately. Although the employee in question explained that these actions were the result of personal problems, there is in our opinion no excuse for this conduct. It also bears repeating that we have reason to believe that the employee in question disclosed the personal health information of certain patients to others in the community without the employer's authorization, in violation of the *Act*.

107. In our view, the facts in this matter are of sufficient severity and of such scale for a breach of privacy that we are bound to take action in order to demonstrate that unauthorized access to personal health information is not tolerated.

Recommendations

108. In view of the above findings, the Commissioner recommends that the measures contemplated by Vitalité Health Network to prevent future occurrences of similar type privacy breaches be implemented in the following manner:

a) That all Vitalité employees, who at hire were given authorization to access the systems where records containing personal health information are stored in order to carry out their duties, receive adequate and complete training in confidentiality and protection of privacy of these persons to whom the information belongs;

b) That the training referred to in paragraph (a) above especially covers when employees may use this authorization to access patients' records, i.e., when in the course of their duties employees have legitimate permission to access these records;

c) That the training referred to in paragraph (a) above be given first to employees already on staff;

d) That the training referred to in paragraph (a) above be given to employees at continuing education sessions to be held within three years of their last training session;

e) That Vitalité inform the Commissioner as to when it plans to commence and complete the training referred to in paragraph (a) which has been further clarified in paragraphs (b), (c) and (d) above;

f) That Vitalité stipulate in every job description that employees are duty-bound to maintain the confidentiality of personal health information at all times;

g) That without delay, Vitalité adopt a new practice concerning random audits of user access involving the computer systems used in its network, i.e., Meditech and Purkinje;

h) That without delay, Vitalité adopt a new practice to immediately suspend the access privileges of any employee who wilfully violates the *Act*, and that it notify the Commissioner at the first reasonable opportunity;

i) That without delay, Vitalité adopt a new practice to review the access privileges of employees who no longer need to access a specific computer system because they have completed a task or no longer perform duties requiring such access, and that this practice apply to staff at all its facilities, including the Hospital and Community Health Centre; and

j) That the management of the Hospital and Community Health Centre continue its efforts to educate staff about their duty to protect the confidentiality of personal information at all times.

109. The Office of the Commissioner will follow up with Vitalité Health Network and the Hospital and Community Health Centre in September 2013 to ensure that these recommendations have been followed.

110. Lastly, the Commissioner gives notice of her intention to take steps regarding the laying of *informations* against the employee responsible for these multiple violations of the *Act*.

Dated at Fredericton, New Brunswick, this 5th day of June, 2013.

_____

Anne E. Bertrand, Q.C.
Commissioner