Office of the Access to Information and Privacy Commissioner
New Brunswick

Commissariat à l'accès à l'information et à la protection de la vie privée
Nouveau-Brunswick

REPORT OF THE COMMISSIONER'S FINDINGS

Personal Health Information Privacy and Access Act

Privacy Breach Notification: 2012-884-H-277

Privacy Complaints: 2013-1239-H-371, 2013-1240-H-372
2013-1264-H-379, 2013-1278-H-385

Date: December 18, 2014

"Case about snooping: unauthorized access to patient records."

INTRODUCTION and BACKGROUND

1. This Report of Findings is issued by the Access to Information and Privacy Commissioner under section 73 of the *Personal Health Information Privacy and Access Act* ("the *Act*") pursuant to an investigation carried out under section 69 of the *Act* into the alleged access by an unauthorized person to patient files, namely electronic patient records that contained personal health information of multiple individuals.

2. The investigation was undertaken by the Commissioner upon being notified on June 4, 2012 by the Réseau de santé Vitalité ("Vitalité") that multiple privacy breaches had taken place involving two employees of the Dr. Georges L. Dumont University Hospital Centre ("Hospital"). Notification to the Commissioner was made as per Vitalité's mandatory obligation to do so under subsection 49(1) of the *Act*:

> 49(1) A custodian shall
> …
> (c) notify the individual to whom the information relates and the Commissioner, in the manner prescribed by the regulations, at the first reasonable opportunity if personal health information is
> …
> (iv) disclosed to or accessed by an unauthorized person.

3. As stipulated in the *Act*, a privacy breach occurs whenever personal health information in the care of a custodian has been mishandled, whether accidentally or intentionally. In section 49 and section 19 of *Regulation 2010*-112, this would be the case when the information is:
   - lost,
   - stolen,
   - disposed of in an unauthorized manner, or
   - is disclosed to or accessed by an unauthorized person.

   (Emphasis added)

4. Section 49 and section 19 of *Regulation 2010-112* further stipulate that when a privacy breach incident occurs, custodians are obligated to notify both the Commissioner and those individuals to whom the personal health information relates, i.e., those individuals whose privacy was breach. This notification must be undertaken at the first reasonable opportunity.

5. Vitalité proceeded to notify the affected individuals, being those whose patient files had been accessed, but only a few months after having conducted a thorough investigation. More on this point later in this Report.

6. A few of the individuals notified of the breaches filed complaints with our Office pursuant to subsection 68(2) of the *Act* in February 2013:

> 68(2) Without limiting paragraph 1(a), an individual may make a complaint to the Commissioner alleging that a custodian
>
> (a) has collected, used, or disclosed his or her personal health information contrary to this Act, or
>
> (b) has failed to protect his or her personal health information in a secure manner as required by this Act.

7. The term "custodian" under the *Act* is used to signify a person, group or institution that has been entrusted by law to collect, use and share personal health information of individuals (such as patients in this case), and to protect such information at all times in accordance with the rules found in the *Act*.

8. This Report of the Findings will speak to the role of the Commissioner in privacy breach investigations, as well the facts uncovered, including audits to electronic patient records that resulted in the discovery of the breaches, the authorization provided to employees who work for Vitalité in the Meditech system, and in this particular case, and so on. We conclude with recommendations.

The Role of the Commissioner's Office

9. To avoid any confusion about the work of the Commissioner and her Office, it is helpful that we first set out our role and responsibilities in the carrying of investigations under the *Act*. The Commissioner is tasked to provide an independent oversight of the proper application of rules governing access to information held by government and the protection of privacy in both the public and private health care sectors. The Commissioner is an Officer of the Legislative Assembly and as such, is not part of government or the health care sector. In that regard, the Commissioner is charged with carrying out independent investigations. The protection of personal health information in the health care sector has been codified in a statute that came into effect on September 1, 2010, being the *Personal Health Information Privacy and Access Act*.

10. Where a breach of privacy is alleged, which means where personal health information has been inappropriately handled, the Commissioner must investigate as long as the complaint or breach notification is related to obligations set out under the legislation. In situations involving the possible unlawful protection of health care records by those entrusted under the statute, the Commissioner's investigation serves not only to resolve the complaint in order to uphold privacy, but also to find ways to better safeguard the information.

11. The Commissioner is not responsible for conducting any criminal investigations relating to possible offences, seeing rather to investigations that ensure compliance with the *Act*. Furthermore, in reporting the findings of her investigations, the Commissioner does not report on civil or criminal liability.

12. The Commissioner is neither no more tasked with making decisions that are akin to those of an employer. Where wrongdoing has been established, the Commissioner will not recommend that disciplinary measures be imposed; rather, the Commissioner will recommend that such measures be considered, especially in circumstances showing serious breaches of privacy.

13. In that regard, where a Regional Health Authority has reported a breach that involves one of its employees, the Commissioner's Office will maintain a respectful distance from its role as an employer, while nevertheless calling upon it to comply with the Commissioner's investigation in gathering the necessary facts for us to investigate the matter. Our investigation is carried out in parallel to that of the Regional Health Authority in this Province, all the while remaining informed of measures undertaken, of the process of notifying the individuals concerned, and while we verify the facts gathered and address all aspects of a case of a breach of privacy in accordance with our role as an oversight body.

CONTEXT OF THE PRESENT INVESTIGATION

Parties at the centre of this investigation

14. The *Act* applies, moreover, to employees of custodians, referred to as "agents" which means an individual or organization that acts for or on behalf of the custodian in respect of personal health information for the purposes of the custodian and not for the agent's own purposes. This case involves two custodians and two agents, as follows.

Vitalité Health Network and the Dr. Georges-L.-Dumont Hospital (custodians)

15. Vitalité manages a series of francophone and bilingual institutions and provides health care services to around 250,000 people in its several hospitals, community facilities, health centres, two community health centres, mental health centres, main public health offices, and so on. The unauthorized accesses to electronic patient records took place at the Dr.-Georges-L.-Dumont University Hospital Centre. The Hospital is part of Zone 1B in the Vitalité network, which serves approximately 87,000 residents in an area between Richibucto and Sackville and includes the greater Moncton region.

16. Vitalité and the Hospital are both considered "custodians" under the *Act*. As such, they are equally entrusted by law to collect, use and share health care information of patients and more importantly, to protect such information at all times, in order to protect patient privacy.

Employees A and B (agents)

17. Vitalité revealed that the unauthorized accesses to electronic patient records had been committed by two of its employees, being a medical transcriptionist hereinafter referred to as "Employee A" and a second employee, a secretary, hereinafter named "Employee B", both of whom worked in the psychiatrists' offices at the Hospital.

18. We note that there are offices of psychiatrists as well as a Psychiatry clinic at the Hospital, both equipped with separate staff. Employee A - employed only at the psychiatrists' offices, while Employee B – employed at both, i.e., at the office of psychiatrists as well as the Psychiatry clinic.

19. For their part, Employees A and B are not designated as custodians, but rather as "agents". The *Act*, however, requires agents to collect, use, share and protect privacy the personal health information of patients as should their employer-custodian, and at all time, to see to the respect for these rules to not interfere with the *Act*.

20. In this case, Employee A viewed personal health information of 99 patients and this over a period of a few months (less than one year from November 2011 until May 2012) without having permission to do so. Employee B is said to have viewed personal health information of one patient without authorization and to have done so on May 8, 2012.

21. During our investigation, we examined the circumstances that led to the allegations concerning the incidents of unauthorized accesses to electronic patient records by Employees A and B. We examined their training regarding confidentiality and protection of the privacy of patients, the level of access granted to these two employees, how the employees accessed electronic records of patients in the software which manages electronic patient records (Meditech), or in other words, all the facts that allowed us to determine whether or not the accesses were indeed justified or not.

Electronic patient records - Meditech system

22. One of the most fundamental aspect and the *Act*'s preeminent rule is that patient records be accessed only with patient consent, or where circumstances exist to lawfully permit access without consent. This case highlights the ease with which staff can access personal data in electronic patient records.

23. This ease of access requires a higher level of monitoring and control to ensure that only those who need to access patient records do so when they must do so.

24. With this concern in mind, Vitalité has put measures in place to provide and monitor access to electronic databases by its entire staff. We begin by explaining what an electronic patient record is.

Meditech system

25. An electronic patient record is a computer file created when an individual first attends a health care facility. His or her information is entered into a patient database, i.e., personal data such as name, address, Medicare number, date of birth, and health care information such as medical history, tests performed and results, diagnosis, and more. This information, referred to as *personal health information*, is recorded electronically in a single electronic file that belongs to that individual and the computer file is maintained in a specialized computer system known as Meditech.

26. Thus, for each person who first presents to receive health care services, the health authority will create an electronic patient record for that person, and that electronic record will contain all of that person's personal health information collected at that time. Where the person receives more health care services at times goes on, that person's electronic patient record is updated with those additional details.

27. Since 2006, there is also a warning message upon entering the home page in Meditech, i.e., a specific message to users regarding the importance of the protection of personal health information. There are four separate messages, each rotated every four months, namely that access is to occur only on a need-to-know basis, accessing one's own patient file or that of a family member must be done only when required by work, if access is taking place outside these parameters, it is a direct violation of policy, using someone else's or sharing a user-name or password is also a direct violation of policy, and accesses are monitored regularly.

28. Failing to follow policy directives will result in disciplinary measures.

Vitalité's practices regarding the protection of patient information stored in an electronic record

29. When any employee is hired by Vitalité, he or she must take part in a general orientation program that includes awareness about confidentiality. Employees must sign a form acknowledging their duty to uphold confidentiality, and this procedure is repeated annually. In addition, Vitalité has implemented policies and practices concerning privacy and confidentiality to ensure that all staff follows the *Act* and respects the privacy of patients at all times. Respect of the rules includes the importance of keeping confidential patient information.

30. Well before the implementation of the current *Act* that oversees the protection of patient information, Vitalité maintained a policy in which all employees were required to protect patient information and to only access and use the information. Only authorized personnel could access and use the information with the patient's consent or where required by law, including:

- Not to discuss patient information in hallways, cafeterias, elevators, etc.
- Not to mention that a particular patient was at a health care facility,
- Not to discuss a patient's case with other employees who do not need to know this information to carry out their work, and,
- Not to access patient records when not treating that individual.

31. To underline the importance of the above requirements, the policy further sets out that failing to follow any of these directives could result in disciplinary measures or even dismissal. This respect of patient privacy and confidentiality of patient information has continued and is reflected in modern day policies and practices (CONFIDENTIALITY and

PRIVACY BREACH) to ensure conformity with the principles of patient privacy, including obligations to protect personal health information of patients at all times and the consequences for failing to do so.

32. Moreover, Vitalité, as a custodian under the *Act*, has recognized and has taken steps to meet its statutory obligations in relation to privacy. Also, the Hospital has a duty to ensure that staff follows such practices.

FACTS UNCOVERED

Discovery of privacy breaches

33. In the present case, the patients' privacy breaches by Employee A were brought to the attention of Vitalité when a patient complained because she sensed that Employee A had accessed, in an unauthorized manner her electronic record. One of the patient's friends who happened to be a friend in common with Employee A seemed to be aware of the patient's personal health information but the patient had never shared it with neither the friend nor with Employee A. The patient was said to be a former friend of Employee A with whom she had personal conflicts. In addition, and according to this patient, her personal health information was shared by Employee A with another of the patient's friends, also a friend in common with Employee A.

34. Vitalité verified if Employee A had accessed the file of this patient and found that this was the case, and this led to Vitalité's investigation. Meanwhile, Employee A was suspended during the investigation.

35. In June 2012, in the Privacy Breach Reporting Form filed with our Office, Vitalité emphasizes that its internal investigation was ongoing and that more details would be forthcoming. From this notification, we undertook our own independent investigation to verify all the facts already discovered and to determine the extent of the alleged unauthorized access that had occurred in this case.

36. During its investigation, Vitalité shared with us that Employee A had also helped another employee snoop in an electronic patient record. Indeed, Vitalité continued its investigation regarding this access by Employee B and confirmed that Employee B would have viewed, with Employee A and from A's computer, personal health information of a patient.

37. Our independent investigation therefore focused on allegations of unauthorized accesses to electronic records of patients done by the two Employees A and B.

Level of authorization to access patient records

38. Vitalité employees are provided with the requisite authorization to access electronic patient records in order to do their job. As per the obligation to respect patient privacy, the employees will only be permitted to access patient records if he or she has been asked to perform a task or provide a service for a patient that requires access to that patient's personal information.

39. The work completed by the psychiatrist's offices and Psychiatry Clinic are stored in the Meditech computer system, where psychiatrists and their personnel access their patient records. To properly understand how these privacy breaches took place in this case, it is appropriate to explain how the computer systems are used at the Hospital and the psychiatrist's offices and Psychiatry Clinic.

40. To use the Meditech computer system, an employee first receives a user name and a password that will allow him or her to enter Vitalité's secure network (provided by FacilicorpNB, a public body that provides computer support services to Vitalité, as well as other agencies within the Provincial health system).

41. The username and password are unique to each employee. This enables FacilicorpNB, and by extension Vitalité, to properly track the employees' access to the Meditech system where confidential personal health information of patients is stored.

42. To summarize, access to patient records is therefore accomplished as follows: the employee logs on to the secure network with his or her assigned unique username and password. This enables the employee to enter the entire shared-computer system. Then, the employee must enter his or her username and password once again to be able to log into the Meditech system where the patient electronic records are stored. Once in the Meditech system, the employee can access the modules of the patient electronic records within his or her Zone based on the level of authorization granted to the employee in order to perform his or her work functions. At this stage, the employee is able to access a specific patient record by the patient's own name.

43. It is only possible to access electronic records of some patients by searching with the intention to do so, as well as by performing a search using the particular patient's

surname, in whole or in part. The employee can access the patient's file inadvertently, but only where the employee conducted a search for a specific patient and clicked, by mistake, on the name another patient and accessed instead the latter's file. When viewing and reading the content of the record accessed inadvertently, the error would readily reveal itself because the employee would see the full identity of the patient and then proceed to exit that electronic record.

Level of authorization granted to Employee A

44. Employee A was hired by Vitalité on May 7, 2011 as a medical transcriptionist in the psychiatrists' offices at the Hospital. Vitalité confirmed to us that at hiring, Employee A signed the Declaration of Confidentiality and Non-disclosure and completed the online module training regarding the protection of privacy and confidentiality. We note that Employee A was at work for only a year at the time the suspicious accesses were discovered; however, Employee A was fully aware of the statutory and employment obligations to respect confidentiality and personal health information of patients at all times.

45. Employee A was given a unique name username and a password and that allowed him to access Vitalité's secure network. In addition, the employee received a unique password to enable him to connect to the Meditech system and access electronic patient records.

46. Therefore, Employee A had the level of authorization necessary to accomplish the tasks of medical transcriptionist, such as typing psychiatric expertise (required by the courts or insurance companies) as well as medical reports dictated by psychiatrists. The transcribed reports were loaded onto the patients' file and sent to doctors who had requested the psychiatric consultation.

47. Employee A had access to the following modules in the Meditech system:
- admission to record the visits of all patients (this module is not restricted by location, which means that Employee A could see all the patient's different visits no matter the unit visited within the Hospital),
- archives that allows to see the patients' visit history (this module is not restricted by location, which means that Employee A can see all the patient's different visits no matter the unit visited within the Hospital), and
- "Patient Care Inquiry" module that allows consultation of transcripted reports.

48. "Restriction to the location" means access only to patients of the unit where the computer is located. For example, when an employee works from a computer in the Nephrology unit, he or she only has access to electronic records of patients in the Nephrology unit. Therefore, a no-restriction to location means that an employee can access electronic documents of all patients in Meditech, regardless of the unit, although he or she can still only to access certain modules.

Authorization level granted to Employee B

49. Employee B was hired by Vitalité on May 1st, 2006. Upon being hired, the latter signed the Declaration of Confidentiality and Non-disclosure and completed the online training module on protection of privacy and confidentiality. In addition, Vitalité informs us that Human Resources had Employee B re-read and re-sign the Confidentiality and Non-disclosure declaration during the annual work performance reviews. Therefore, we can conclude that Employee B was fully aware of its statutory and employment obligations to respect the confidentiality of the personal health information of patients at all times.

50. With respect to Employee B's level of access authorization, the latter performed some clerical tasks for the Psychiatry Clinic and for the psychiatrists' offices, such as entry of test results, management of appointments, receptionist services for patients, preparation of records, etc. Employee B occupied a position that required working in more than one place in the Hospital, so Employee B was granted two Meditech system user accounts, being an account as a receptionist in the Psychiatry clinic (unrestricted by location) and one account as a receptionist in nursing (with restriction to location).

51. When using the user account at the Psychiatry Clinic, Employee B could access in Meditech:

- the admission module to record visits of all patients (this module is not restricted by location, which means that Employee B can see all the patient's different visits, no matter the unit visited within the Hospital),
- the 'Medical Information System' module which allows to see address, telephone and facsimile numbers of doctors,
- the module to send and receive internal messages in Meditech, and
- the "Scheduling" module to schedule appointments for patients with various psychiatrists.

Employee monitoring

52. Monitoring of staff is an effective control measure to discern whether Vitalité's staff complies with its obligations to keep personal health information confidential at all time and to use their authorization level to electronic patient records only when necessary to accomplish their duties.

53. We asked Vitalité about the level of supervision over Employees A and B in question, and we were told that a particular Manager is responsible for both the Psychiatry Clinic and the psychiatrists' offices and indirectly monitors staff; interactions with employees rather take place when issues are brought to her attention. Twelve psychiatrists who work in this sector deal with the Manager about operational issues as needed. No one pointed to problems regarding Employees A and B before the discovery of the incidents which concerned this investigation.

54. Since the monitoring of employees may not always be sufficient, another way to detect if staff complies with its authorization to electronic patient records is to conduct random audits (or audits on request in the case where of a suspicion of unauthorized access).

Process for audits to detect suspicious accesses to patients' electronic records

55. An employee receives permission to access patient records when asked to perform a task in the context of his work, or with the consent of the patient. Therefore, an access to a patient's record is considered unauthorized when the employee has extracted or read a patient's personal health information outside such parameters of his work.

56. To determine if the accesses performed by personnel are authorized or not, Vitalité can undertake random audits. An audit generates a list enumerating the user access for a period of one month and allows the verification of whether the accesses are allowed.

57. The committee struck to perform these random audits is known as the Comité de sécurité et accès à l'information électronique (translated as the *electronic information access and safety Committee*) and is responsible for reviewing and monitoring users' access to electronic systems containing personal health information with a view to ensure users use and disclosure patient health information only when appropriate to do so.

58. If the audit shows that the access is suspicious, the Committee will prepare an incident report to the appropriate office (to the Privacy Officer or a unit manager) to trigger a follow-up, being an investigation. A request can be made to the Committee to conduct a further audit of the accesses of the target employee and in many cases a second audit covers a period of six months. This broader audit is carried out first by making a specific request to FacilicorpNB, which in turn will identify the necessary documents that show all accesses made by the employee during the period of six months. These documents are then submitted to the Chief Privacy Office for the purpose of review. The results of the audit of six months are reviewed in the same manner to find out if there were other suspicious accesses.

59. If additional suspicious accesses are discovered, the Chief Privacy Office performs a review of these accesses and where one or more access is deemed unauthorized, the results of this step will be enough to cause a more thorough investigation and notification to the Commissioner.

60. For example, if an employee accessed the record of a patient while the employee was not performing his work duties at the time when the access has taken place, he will be required to provide an explanation to the appropriate officials so as to detect whether the access was allowed or not. In other words, the employee will have to explain whether the access was accidental or if he had received permission from the patient to access the folder.

Employee A's suspicious accesses and admissions

61. In this case, after receiving a complaint from a patient alleging an unauthorized access to her electronic record, Vitalité conducted an audit for a period of one month on the patient's record in order to discover if there were any suspicious accesses. The result of the audit revealed three suspicious accesses on the part of Employee A. A more in-depth audit was then performed of all of accesses by Employee A for a period of 6 months in order to detect if the latter had improperly accessed other electronic patient records. The results revealed several suspicious accesses which in the majority of cases were to records of patients known to Employee A.

62. Following those results, Vitalité performed an audit dating back to the hiring of Employee A, being May 2011. The results of that audit showed that Employee A had accessed 99 electronic patient records in an unauthorized manner between the months of November 2011 and May 2012. In addition, the audit shows that Employee A

attempted to view electronic records of three individuals by searching their names, but no result was posted because these individuals had never attended the Hospital as patients.

63. With the results of the audits in hand, Vitalité held a few meetings with Employee A and asked him to share the reasons with regard to the accesses, and to reveal whether Employee A had shared the patients' personal health information with other people. According to the evidence gathered, Employee A admitted having performed a search for the names of known patients, but did not remember the reasons for having done so on patients' files whose names were not known to this employee. Employee A said to have acted out of simple curiosity and did not believe to have disclosed to others the personal information that had been reviewed. Not being sure of this fact, Employee A added that if such disclosure took place, it had occurred without malice and by accident.

64. Vitalité attempted to find out whether Employee A had indeed shared patients' personal health information, and specifically those of the patient who complained to Vitalité in this regard; however, Employee A did not admit to sharing personal health information of the patient in question.

65. According to a reasonable assessment of the facts, we deem that Employee A would have disclosed personal information of the patient who complained. The patient sensed that Employee A had accessed in an unauthorized way her electronic record since a friend in common appeared aware of her personal health information which the patients had never shared. Employee A had indeed accessed the patient's record without being authorized, and it is reasonable to draw the conclusion that Employee A shared this information with the friend in common.

66. The facts are not refuted. Employee A has admitted to having acted without authorization and deliberately out of simple curiosity by accessing 99 electronic patient records, in having tried to access three electronic patient records without success, as well as by having communicated at least one patient's personal information. Therefore, Employee A has admitted to having accessed and read personal health information of nearly 100 patients without permission and deliberately. In addition, we seriously doubt the sincerity of the explanations when this employee says to not having intended to share the personal information of individuals whose privacy was violated by this employee. Employee A voluntarily shared a patient's personal health information, without regard to its statutory and employment obligations, and without regard to the protection of the privacy of this patient, contrary to the *Act* and in violation of

paragraphs 76(1)(a) and (b), as well as subsection 76(2) of the *Act,* which provides as follows:

> 76(1) No person shall
> (a) collect, use or disclose personal health information in wilful contravention of this *Act*,
> (b) attempt to gain or gain access to personal health information in wilful contravention of this *Act*,
>
> 76(2) A person who is an employee of a custodian or information manager who, without the authorization of the custodian or information manager, discloses personal health information in wilful contravention of this Act in circumstances where the custodian or information manager would not be permitted to disclose the information under this Act, commits and offence.
>
> 76(5) A person who violates or fails to comply with subsection (1), (2), (3), or (4) commits an offence punishable under Part II of the Provincial Offences Procedure Act as a category F offence.

Employee B's suspicious access and admissions

67. It is during the several meetings held with Employee A that Vitalité discovered that Employee B had also accessed, in an unauthorized manner, the record of a patient, being the electronic record of the child of another person.

68. Vitalité officials therefore met with Employee B to determine the reason for the unauthorized access. Employee B is said to have had a personal conflict with a certain person and Employee B wanted to know the time at which this person was scheduled to attend the obstetrics clinic for an appointment, a clinic which is located nearby to the Psychiatry Clinic at the Hospital. Employee B then asked Employee A to access the electronic record of the child of that person to avoid being at the employee's work desk and avoid the person at the time of her appointment. Employee B had access to the schedules of the other clinics, including the obstetrics clinic, but still asked Employee A to access the file so that Employee B could view the file and know the time of the person's appointment.

69. Following this discovery, Vitalité conducted an audit of the record of the patient in question and determined that Employee B, by way of Employee A and from A`s computer, had accessed that individual's electronic patient record on May 8, 2012. According to Vitalité's policy, additional audits were conducted for a period of three months (between May 7 and August 16, 2012) to detect whether Employee B had

accessed any other electronic patient records in an unauthorized manner. The results of those audits showed that this was not the case, and that this employee's other accesses were justified. Therefore, Vitalité did not undertake any additional audits on Employee B.

70. According to our assessment of these unrefuted facts, we deem that Employee B contravened the *Act* during the course of employment with Vitalité since Employee B admitted to accessing and obtaining the patient's personal health information without permission and deliberately, all in contravention of paragraph 76(1)(b) of the *Act* :

> 76(1) No person shall
> …
> (b) attempt to gain or gain access to personal health information in wilful contravention of this *Act*

Are Employees A and B still employed with Vitalité?

71. As mentioned above, Employee A was suspended for the duration of Vitalité's investigation. We can report that Employee A has since resigned from work on July 26, 2012 and Employee A is no longer employed in any establishment of the Réseau de santé Vitalité.

72. Regarding Employee B, this person is always at the employ of Vitalité; however, following the discovery of a patient's breach of privacy, Employee B was imposed disciplinary measures in accordance with Vitalité's Policy for privacy breaches. Vitalité found that the privacy breach incident was intentional but not malicious, although still an offence of Vitalité's policies and of the *Act*. Disciplinary measures imposed on Employee B included: a discussion about policies on confidentiality and the relevant procedures for access to patient records and to respect privacy, more training on the protection of privacy and the consequences of non-compliance, and a recommitment by re-signing Vitalité's Declaration of confidentiality and non-disclosure.

BREACH NOTIFICATION PROCESS

73. The primary purpose of the *Act* is to protect the privacy of persons whose personal health information has been entrusted to custodians. The *Act* also requires custodians to be transparent in their practices for handling of the personal health information entrusted to them, and to ensure that these practices are followed at all times.

Furthermore, the persons affected by a privacy breach have the right to know that their personal health information has been compromised.

74. 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.

75. Therefore, in accordance with section 49 of the *Act* and its *Regulations*, affected individuals must be informed as to what has occurred and when the incident took place, including:

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.

76. In addition, any person affected by a privacy breach has the right to file a complaint with the Commissioner and must be formally advised of that right. A custodian will not be permitted to abstain from answering the questions that ensue, including explaining how the breach occurred and who is responsible.

Breach Notification in this case

77. As noted earlier, when many suspicious accesses were discovered in June 2012, Vitalité advised the Commissioner shortly after; however, Vitalité could not proceed to notify the affected patients before having verified and confirmed that the accesses were actually unjustified and that Employee A had the opportunity to provide explanations in relation to each suspicious access. In addition, it was during the investigation of the questionable access on the part of Employee A that a suspicious access of Employee B was discovered. After all the work to verify the suspicious accesses, Vitalité could proceed to inform all persons concerned, in accordance with its statutory duty under section 49 of the *Act*.

78. In our view, it was necessary for Vitalité to do so prior to the notification of close to 100 patients. We agreed that Vitalité could proceed in one mail-out so that the Vitalité's Chief Privacy Office, with arrangements in place, was able to respond to all calls from

individuals affected. For these reasons, we find that the delay encountered for notification in this case was reasonable given the circumstances.

79. Vitalité notified all people affected by the privacy breaches by letter at the beginning of the month of February 2013. Each letter informed the person of the discovery of the privacy breach, that the information accessed could have included, based on the record of the patient, demographic data, such as name, mailing address, telephone number, marital status of the patient, as well as personal health information, such as the names of the physicians, room number, private insurance information, file number, Medicare number, mother's name, date of discharge and reason for visits. Vitalité invited these people to ask questions about the case or share their concerns if they wished to do so and their right to file a complaint with the Commissioner about the breach.

80. Several of the affected individuals also contacted our Office to share their concerns and ask for information about the case. Of these, four individuals pursued their right to file a formal complaint under the *Act* and these complaints are summarized with the questions they raised for us to investigate:

- *Who is the employee who committed the breach?*
- *What personal health information was accessed?*
- *Why did it take so long to discover the breach?*
- *How and did the breach occur?*
- *Could the privacy breach result in identity theft?*

81. We have referred the questions regarding the identity of Employees A and B who had accessed their files to Vitalité, as nothing prevents it from informing the concerned individuals who make the request to the custodian, being Vitalité. We do not prescribe to publicly announce the name of an employee responsible for a privacy breach; however, there is nothing in the *Act* that prevents notifying the individual affected by such a breach of the employee's name when requested by the individual. In addition, Vitalité could respond more precisely on which personal health information was accessed in the particular case of the patients concerned. As noted earlier in this Report, we have responded to the other questions raised by the affected individuals. We now address the question of identity theft.

Can the privacy breach lead to identity theft?

82. Another concern brought to our attention was the risk of identity theft by reason of unauthorized accesses committed by these employees to the concerned patients' personal health information. It is useful to repeat that we verified the facts of this case and we have not found evidence to support that Employees A and B accessed patient records and their personal information with a view to be used to steal their identity or sell their identities to others.

83. It cannot be assumed, however, that the risk of identity theft is void when the integrity of personal information has been compromised. For this reason, we offer advice in that regard.

84. There is no agreement on the meaning of "identity theft," but the term is used to describe many possibilities, from cheque forgery and the use of stolen credit cards, to even 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.

85. 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*).

INVESTIGATION CONCLUSIONS

86. The *Act* is intended to improving the overall health care system in New Brunswick to ensure that individuals feel comfortable in sharing their personal information, knowing that they will be kept confidential and that their security will be assured, and to ensure that health care providers are better equipped to provide care through the use of more accurate information updated and complete their patients.

87. 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.

88. More importantly, the *Act* codifies the actions surrounding patients' information that will ensure the accountability of those who handle it. In that regard, the *Act* has set very clear rules on the handling of personal health information, from its collection, use, disclosure, to its retention and storage, all of which is centered upon one basic principle: keeping the information safe and secure at all times in order to protect the privacy of the individuals to whom the information relates.

89. This case concerns unauthorized accesses to 99 electronic health records of patients carried out deliberately on the part of Employee A, including disclosure of one particular patient's personal health information. This case also involves one unauthorized access on the part of Employee B. The employees in question had the necessary permission to access the Hospital's electronic patient records in the Meditech system to perform their work duties. On the other hand, the facts are unequivocal that these employees had neither the permission nor the justification, therefore were not allowed, to access the electronic patient records in the Meditech system at issue in this matter.

90. Between November 2011 and May 2012, Employee A accessed 99 records and released certain confidential information in one instance to a patient's common friend, and we have seriously doubted the sincerity of the explanations for having done so. It must be said that 99 unauthorized accesses in a short period of six months demonstrated recklessness for the *Act* and for the protection of these patients' privacy.

91. Regarding Employee B, the fact that the latter has accessed only to a single record in an unauthorized manner does not minimize the seriousness of the case; access to electronic patient records to satisfy one's curiosity is in contravention of the *Act*.

92. Finally, the custodians Vitalité and the Hospital are mandated by section 50 of the *Act* to protect personal health information by adopting practices that include administrative, technical and physical safeguards. These mandatory safeguards will are designed to ensure the confidentiality, security and integrity of the information and are elaborated upon in section 20 of the *Act*'s *Regulation 2010-112* and include to:

- ✓ limit access and use of personal health information to those specifically authorized to do so;
- ✓ protect the personal health information during its collection, use, disclosure.

93. When one or other of these rules or guarantees is not applied, followed or respected, custodians and their staffs are likely committing what is called a *privacy breach*. Having done a more enhanced surveillance would have perhaps detected Employee A's unauthorized accesses; however, the personal commitment to follow the rules as a good training to respect the confidentiality and privacy of patients and good guidelines and practices as required by Vitalité during the hiring of staff and during the period of employment should have been enough.

94. Unfortunately, this case highlights the ease of access to personal data that staff can use to navigate with ease in the records of the patients without fear or remorse of conscience or retaliation, as demonstrated by Employee A who was responsible for just under 100 patient privacy breaches in this case.

95. Snooping in medical records is quickly becoming one of the most reported and publicly reproachable actions among those undertaken by the employees having as work duties the processing of personal health information, and this, not only in New Brunswick.

96. In Newfoundland and Labrador, two employees have been charged with offences pursuant to the *Personal Health Information Act* as a result of two separate investigations conducted by the Information and Privacy Commissioner stemming from complaints received in which both individuals in question would have improperly accessed the personal health information of a number of patients. A few months ago, these two employees appeared before the Provincial Court of Newfoundland and Labrador where they were imposed a fine of $ 1,000 for one employee and $ 5,000 for the other. Those fines should signal to all the importance that the *Act* attaches to the confidentiality of personal health information, being of the most precious, and that violation of this confidentiality will not be tolerated by society.

97. In the past year, we have issued recommendations to the Réseau de santé Vitalité on the need to increase the frequency of random audits in order to detect unauthorized accesses more quickly (see reports of findings 2012-743-H-236 published on 5 June 2013 and 2014-1294-H-393 published July 31, 2014). We reiterate these recommendations that will encourage Vitalité to put in place a process and spend the necessary resources for more frequent and on-going random audits of the patient data base in Meditech.

98. In this regard, we are pleased to report that Vitalité has informed us of its decision to accept these prior recommendations and that Vitalité is currently considering options to secure this required higher level of supervision regarding access to electronic patient records.

RECOMMENDATIONS

99. In view of all of the above findings, the Commissioner recommends to Vitalité the following recommendations:

> **Recommendation 1** The Commissioner recommends that the Réseau de santé Vitalité continue its efforts of implementing a more in-depth surveillance of accesses to electronic patient records by allocating the necessary resources to permit the undertaking of more frequent and regular random audits that currently exist of accesses to the Meditech patient databases. These more frequent and regular random audits must include all health care providers and their staff employed by Vitalité.
>
> Vitalité will be required to provide the Commissioner a status update on the implementation of **Recommendation 1** by February 27, 2015.

Recommendation 2 Given the scale of unlawful accesses committed by employee A pursuant to subsections 76(1) and (2) of the *Act* and that it we wish to demonstrate that unauthorized access to personal health information will not be tolerated in New Brunswick, the Commissioner strongly recommends that Réseau de santé Vitalité consider the possibility of laying charges against employee A under the *Provincial Offences Procedures Act*.

Recommendation 3 Given the privacy breach committed by Employee B and Employee B's admissions, and given the discipline already imposed on employee B by Vitalité in light of this misconduct, the Commissioner recommends that Employee B be the subject of additional supervision (through random audits) of Employee B's accesses to electronic patient records in Meditech for a period of 3 months from the date of this Report.

100. The Commissioner will be follow-up with the Réseau de santé Vitalité over the next few weeks and months concerning the implementation of the present recommendations.

DATED at Fredericton, New Brunswick, this _____ day of December, 2014.

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