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: 2013-1294-H-393

Privacy Complaints: 2014-1743-H-491; 2014-1796-H-469
2014-1797-H-500; 2014-1802-H-502
2014-1976-H-541

Date: July 31, 2014

"Case about a physician's unauthorized access to electronic patient records"

# TABLE OF CONTENTS

# TABLE OF CONTENTS

## 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 March 15, 2013 by Vitalité Health Network ("Vitalité") that these multiple privacy breaches had taken place by a physician in a 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. At the time we were notified, Vitalité had not notified the individuals whose patient files had been accessed. We speak more on this point later in this Report.

4. Our investigation also included examining the related complaints filed with our Office by individuals whose information was accessed in this case, and those complaints were filed pursuant to subsection 68(2) of the *Act* in late February and early March of 2014 after they were notified of the breach to their privacy by Vitalité:

> 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.

5. 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 health care information of individuals (such as patients in this case), and to protect such information at all times in accordance with the rules found in the *Act*.

6. This Report of Findings will encompass the following elements: the role of the Privacy Commissioner, the meaning and significance of privacy in the field of health care, custodians' statutory obligation to protect privacy as per the *Act*, the context of this case and facts uncovered in this investigation, the question of random audits used to monitor access to electronic patient records, random audits carried out in this case with resulting discoveries, actions undertaken, and conclusions. We finish this Report with our findings and recommendations pursuant to the *Act*.

## The Role of the Commissioner's Office

7. 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*.

8. The Commissioner is both an Access to Information Commissioner and a Privacy Commissioner who is tasked by legislation 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 she is not part of government or the health care sector operated by government. In that regard, the Commissioner is charged with carrying out independent investigations.

9. These rules have been codified in two statutes that came into effect on September 1, 2010: the *Right to Information and Protection of Privacy Act* and the *Personal Health Information Privacy and Access Act*, and the Commissioner obtains her powers of investigation from both of these statutes.

10. The Commissioner's investigations function as a means to make findings of fact and provide recommendations to the relevant government institutions and/or health care providers with a view to promote compliance with the rules, i.e., with the *Acts* and to ensure that rights of access and privacy rights are respected.

11. It is in this regard that the Commissioner plays a crucial role in the investigation and resolution of complaints alleging the improper handling of personal information, in particular, personal health information which is regarded as citizens' most private details about themselves.

12. Personal health information is protected as of right under the *Personal Health Information Privacy and Access Act*, and this right corresponds to an equally important statutory obligation imposed upon all health care providers who are required to handle personal health information of citizens in order to carry out their work.

13. 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.

14. The Commissioner must investigate even where the very subject of the complaint may amount to an allegation that an offence under the statute has taken place. The Commissioner's primary role and function is to conduct administrative investigations in order to conclude whether a breach of privacy has taken place.

15. 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. The investigations permit the Commissioner to review the general administration within institutions as well as how individual health care providers have handled the information in relation to the allegations.

16. The Commissioner's investigations provide an independent verification of the facts in determining whether the law was followed, and where it was not followed, to provide facts as to why and recommendations to ensure it does not take place in the future. Investigations therefore can serve to uncover evidence of wrongdoing; however, the Commissioner does not enforce the *Act* – she does not conduct any criminal investigations relating to possible offences.

17. Furthermore, in reporting the findings of her investigations, the Commissioner does not report on civil or criminal liability. In certain circumstances, the Commissioner may report on facts that point to a wilful contravention of the *Act*; in such a case, the Commissioner does not decide culpability as that power remains solely in the realm of a judge's decision after the prosecution has laid charges pursuant to the *Provincial Offences Procedure Act*.

18. Our investigations are carried out in parallel to those of the two Regional Health Authorities in this Province when either of them report a breach of privacy to our Office under section 49. Such a reporting will require the health authorities to provide us with the results of their investigation, to date and on-going, in accordance with our *Reporting of Privacy Breach* form, a form that has been developed by our Office to capture all of the facets of a privacy breach case. The reporting form contains specific questions that must be answered as to when the alleged breach occurred and by whom, how and why it took place. The answers to these questions are facts that become the basis upon which the Commissioner will investigate the matter thoroughly. It is the statutory responsibility of those involved in a privacy breach to comply with the Commissioner's investigation, as it is an offence under subsection 76(1) of the *Act* not to do so.

19. Finally, the Commissioner is no more tasked with making decisions that are akin to that 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. In that regard, where a Regional Health Authority has reported a breach that involves one of their employees, the Commissioner's Office will maintain a respectful distance from their role as an employer, while nevertheless calling upon them to comply with the Commissioner's investigation in gathering the necessary facts for us to investigate the matter.

20. The Commissioner's Reports of Findings will present the facts uncovered, whether a privacy breach took place and if so, reasons why it took place. Recommendations are issued by the Commissioner to ensure that similar breaches of privacy do not recur and that personal health information be kept confidential and secure at all times; these recommendations, issued under section 73 of the *Act*, allow the Commissioner to continue her oversight role and see to the intended full compliance with the law.

21. Due to the complexities of the case, including the Meditech system and its use including search functions, the audit process, the interpretation of the audit logs, the independent verification of these facts, gathered by both Vitalité and our Office, a decision was made to distribute a draft version of the facts of the case to the custodians who were the focus of this investigation. This was done to verify the accuracy of the facts to ensure that our findings and recommendations were supported and as we considered it necessary to assist the Commissioner in the discharge of her duties in this case.

## Commissioner's Protocol on identifying custodians in privacy breach reports

22. The question of identifying the physician at the heart of this case when the breaches were first alleged was the subject of much reflection on the part of all those involved in the case. Physicians are custodians under the law and are ultimately responsible for the protection of personal health information of their patients. In this case, the physician was also an employee of another custodian, namely Vitalité.

23. While it was not the first time that the Commissioner has reported on an investigation of unauthorized access to patient's personal health information (commonly referred to as "snooping cases"), this is the first case in New Brunswick's history that involved the actions of a physician alleged to have committed breaches of this nature.

24. When our Office was first created, there were no set protocols on this point and no direction in the *Act*, and as the Commissioner is the master of her own procedure where the legislation is silent, we established a protocol that would be both fair and applied consistently when having to report our findings and whether to identify those responsible for the breach. Early on in our mandate, in 2011, we were presented with cases of privacy breaches that involved custodians and their employees. Some of these cases were publicly known and some were not.

25. Our protocol provided that our Office would identify, in all cases, breaches caused by a public sector custodian, as the public sector has been provincially regulated in this field for several years. Public sector custodians include regional health authorities, Ambulance NB, Department of Health, hospitals, public health care clinics, as well as salaried physicians, nurses, and other health care professionals who are employed by a public sector custodian.

26. The protocol, however, also provided that private sector custodians would not be identified, even where the privacy breach incident had been reported in the news. The reasoning behind this included such factors as that these were the first cases being reported under a provincial legislation that had been in effect for less than a year, private sector health care providers were for the first time subject to a regulatory legislation and our oversight. At that time, there was evidence that the private sector custodians were not familiar with the requirements of the law.

27. We also recognized that this disparate application of the rule for private sector custodians was only a short term measure in order to allow them time to adopt the rules of the *Act* in their private practices.

28. Our protocol since that time has been adapted and calls for the identification of public and private sector health care professionals who are responsible for a breach. The protocol continues to address the question of identifying a custodian versus employees of a custodian. We approached this latter question from the perspective that custodians are ultimately responsible for a breach of privacy, including when a breach is committed by their employees who are not themselves custodians under the law.

29. In the case of an employee who is not a custodian who caused a breach of privacy, the Commissioner will identify the custodian but not the employee. We add, however, that those affected by the breach of privacy caused by an employee of a custodian have the right to ask and be informed of the identity of the employee who mishandled their private information. Where a breach of privacy is alleged to have been caused by an employee who is also a custodian, however, both the employee-custodian and the employer-custodian will be identified based on the fact that both are accountable under the law and are the focus of our investigation.

30. For these reasons, and in following our protocol, we are identifying all custodians that are the focus of this investigation in this matter, including the public sector salaried physician employed by Vitalité and who is a custodian in his own right under the law.

31. While we fully appreciate the effects the publication of a Report of Findings will have on any custodians involved, we would be remiss in not making it clear to all concerned that the *Act*, uniquely designed to protect citizens' most private and sensitive information, demands that those who wilfully contravene the *Act* be held accountable. This accountability signifies that some loss of privacy of those responsible for the privacy breach will be justified in the circumstances of rendering findings public in order to report on who caused the breaches, when, how, and why they occurred.

32. We now proceed to the other elements of this Report of Findings.

## CONTEXT OF THE PRESENT INVESTIGATION

### Parties at the centre of this investigation

33. The *Act* applies to a wide range of health care professionals. The definition of custodian is broad and includes: an individual or organization that collects, maintains or uses personal health information for the purpose of providing or assisting in the provision of health care, and planning and delivery of services. That definition includes health care providers who are registered or licensed to provide health care under an Act of the Legislature or who are members of a class of persons designated as a health care provider in the regulations. This case involves four custodians and we address each one in turn.

***Vitalité Health Network***

34. 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.

***Dr.-Léon-Richard Oncology Centre, Dr. Georges-L.-Dumont University Hospital Centre***

35. The unauthorized accesses to electronic patient records took place at the Dr-Georges-L.-Dumont University Hospital Centre (the "Hospital"). The Hospital was formerly part of the Beauséjour Regional Health Authority at a time when there were eight regional health authorities in New Brunswick. Today, these services have been combined under the umbrella of two regional health authorities (Vitalité and Horizon Health Network).

36. The Hospital is part of Zone 1B in the Vitalité network, as both regional health authorities continue to have defined zones. Zone 1B serves approximately 87,000 residents in an area between Richibucto and Sackville and includes the greater Moncton region.

37. Operating as part of the Hospital, the Dr.-Léon-Richard Oncology Centre ("Oncology Centre") is a specialized cancer treatment facility that provides comprehensive services in radiation therapy, medical oncology and gynecology-oncology for all of Zone 1B.

***Dr. Fernando Rojas Lievano***

38. The privacy breach notification filed with our Office by Vitalité revealed that the case involved unauthorized accesses to electronic patient records by one of its salaried physicians, a radio-oncologist employed at the Oncology Centre.

39. It was alleged that the radio-oncologist, Dr. Fernando Rojas Lievano, had used his access privileges to the electronic patient database when he was not authorized to do so, and those accesses were to multiple patient files over the past years.

***All custodians under the law in this case***

40. Vitalité, the Hospital, the Oncology Centre, and Dr. Rojas Lievano are all 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.

41. In this privacy breach and privacy complaints investigations, we examined the circumstances that led to alleged multiple incidents of unauthorized accesses to electronic patient records by one physician, namely Dr. Fernando Rojas Lievano.

42. We also examined how patient records are accessed by physicians at the Oncology Centre at this Hospital under the guise of Vitalité to assess the correctness of their privacy practices.

43. In special detail, we looked into how electronic patient records are accessed by physicians, including the computer systems and programs that house electronic patient records, the process by which access is granted, and in this case, the physician's level of access and his use of that access to determine whether the accesses were justified or not.

## MEANING AND IMPORTANCE OF *PRIVACY* IN HEALTH CARE

### Privacy and confidentiality of patient information

44. This Report deals with the handling of personal health information belonging to patients who received services in a health care zone. In particular, this case is about these patients' right to privacy, a right to the confidentiality and protection of their information that has been collected and recorded in their electronic patient records.

45. What is meant by privacy? A term widely used but perhaps not well understood to its full measure. Having looked to many experts who define or describe 'privacy', we found it best described by the Office of the Privacy Commissioner of New Zealand, as per the following paraphrased extract:

> We often define our relationships with people by what information we choose to share with them; therefore, if we are unable to control who knows information about us, we will feel insecure - at least in part because the boundaries of our relationships become uncertain. We become tense when we are constantly under scrutiny and as human beings we need security to be able to function normally in their social environment.
>
> In this light, a common understanding about privacy has emerged, in New Zealand and in many countries overseas and our modern laws that protect privacy reflect this common understanding. People need to be able to protect information about themselves and people need the opportunity to withdraw - physically or mentally - from society. From this common understanding, we appreciate that privacy is important to ensure that we feel secure. So privacy, which supports or creates feelings of security, is an important human right. If we feel secure, we're more likely to play a full part in society.
>
> (Source: Privacy Commissioner of New Zealand, *The Meaning of Privacy*, Posted 2013)

46. Handling of information belonging to those who are patients of the health care sector is centered upon the fundamental rule of the confidentiality of patient information – to protect their privacy.

47. To this end, the *Act* has codified those same rules and principles, well-established and followed by health care professionals for a considerable time as reflected in their respective professional codes of conduct, codes of ethics and professional practice guidelines, policies and practices, all of which ensure the protection of privacy of patients.

## Established practices in health care sector

48. Confidential data collected by custodians and staff is governed by the overarching principle of maintaining the confidentiality of personal health information at all times, so as to ensure the privacy of those to whom the information belongs. Protection of privacy is neither new nor novel. It has been the foundation for the practice of medicine for a very long time, particularly when we note its long standing expression found in codes of ethics of many professional fields, as well as all physicians' Hippocratic oath that solicits this important promise:

> The Hippocratic Oath is one of the oldest binding documents in history. Written in antiquity, its principles are held sacred by doctors to this day: treat the sick to the best of one's ability, preserve patient privacy, teach the secrets of medicine to the next generation, and so on. "The Oath of Hippocrates," holds the American Medical Association's Code of Medical Ethics (1996 edition), "has remained in Western civilization as an expression of ideal conduct for the physician." (Source: Peter Tyson, *The Hypocratic Oath Today*, Posted, March 27, 2001).
>
> (Emphasis added)

49. Privacy has also been integral to the very practice of medicine. For instance, the *Medical Act* (the 1981 law that governs the medical profession in New Brunswick) includes a Regulation entitled *Code of Ethics*, in which privacy and confidentiality of personal health information of patients is specifically addressed in sections 31 to 37. Our review of those sections shows that these directives reflect well and complement the rules found in the *Act* regarding the privacy and confidentiality of personal health information in the health care sector (the *Medical Act* is found on the *College of Physicians and Surgeons of New Brunswick*'s website).

## Vitalité's practices

50. When physicians and employees are hired by Vitalité, they are required to take part in a general orientation program that includes awareness about confidentiality. Attendance at this session is compulsory. Physicians, like employees, are also required to sign a form acknowledging their duty to uphold confidentiality, and this procedure is repeated annually. This is but another example of how the privacy laws, such as those rules found in the *Act*, have codified well-established practices for patient privacy.

51. Those confidentiality and privacy policies and practices of Vitalité are meant to ensure that all staff follows the law and respect the privacy of patients at all times, including the importance of keeping patients' information confidential.

52. Even several years ago and well before the implementation of the current *Act* that oversees the protection of patient information, Vitalité (then known as Beauséjour) maintained a policy IV.20.10 dated September 30, 2002 in which all employees, physicians, volunteers, interns, and so on were required to protect patient information and to only 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.

53. 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. In addition, the employees were required to sign an undertaking attesting to their promise to adhere to these directives every year.

54. This respect of patient privacy and confidentiality of patient information has continued and is reflected in modern day policies and practices. In particular, Vitalité's policy GEN.6.30.15 dated December 15, 2010 entitled CONFIDENTIALITY, as well as a policy GEN.6.30.20 entitled PRIVACY BREACH both contain detailed and specific practices 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.

55. Also, policy GEN 6.30.15 requires that Vitalité staff sign a Confidentiality and Declaration of Understanding (déclaration de confidentialité et de non-divulgation) that attests that they will handle and protect patient information in a safe and secure manner at all time.

56. Moreover, Vitalité, as a custodian under the law, has recognized and has taken steps to meet its statutory obligations in relation to privacy. For instance, under subsection 49(1) of the *Act*, a custodian is required to designate a person to assist in ensuring compliance with the *Act*. In Vitalité's case, this has been accomplished by creating a

new office and appointing a head that will see to the compliance with Vitalité's policies and practices and the law: that of the Chief Privacy Officer and staff. That office is tasked with raising awareness for the policies regarding patient privacy and make arrangements to have training modules available (20 minutes taken on-line). In addition, all staff of Vitalité, including physicians, are required to follow the training each year.

57. Another measure of control for the respect of these legislated rules to protect patient privacy is found where Vitalité grants working privileges for medical professionals to work in its institutions. Vitalité requires that physicians sign a *Declaration* on a yearly basis before their privileges are renewed attesting to the fact that they are familiar with and accept to abide by Vitalité's administrative policies and regulations, as well as their own professional code of ethics.

58. An important additional measure of control to ensure that patient information is kept confidential at all times is derived from random audits. Random audits are conducted from the very database where the electronic patient records are housed to obtain lists of accesses and to verify whether these accesses carried out by various users of the database are authorized. Audits are viewed as an essential component of regional health authorities' overall mandate to protect and keep confidential patient information. More notably, audits emphasize the point that health care professionals remain responsible and accountable at all times for their handling of patient information. We speak more on the topic of audits further in this Report as it pertains to this particular case.

## The law in New Brunswick today

59. It is with the appreciation and the respect for patient privacy and confidentiality of personal health information that New Brunswick, as in the case of many other Canadian jurisdictions, has adopted laws that codify the very principle of a patient's right to privacy and the corollary responsibility for all those who have access to the patient's personal health information, i.e., has put into law the same principles and rules that are followed by health care providers everywhere.

60. Found in section 2 of the *Personal Health Information Privacy and Access Act* is its dominant purpose:

> to establish a set of rules that will see to the protection of the confidentiality of personal health information and the privacy to whom the information relates.

61. Part 4 of the *Act*, entitled *Collection, use and disclosure of personal health information,* then sets out the overriding principles of handling personal health information:

> only those who need to know the information to carry out their work when providing or assisting in the delivery of health care will be authorized to collect, use and share it; further, they can only do so with the minimum amount required to perform their tasks.

62. Again, these are well-known, recognized and adopted rules that are essential to the practice of health care. To disregard these rules means to disregard one's lawful authority to access, use or share patient information.

## Health care providers

63. All of this to say that there are clearly established professional guidelines, codes of ethics, practices, policies as well as the law, all of which are derived from a single dominant principle: patient privacy is a right and all those working in the health care sector, including physicians, have a professional and legal obligation to keep patient personal health information confidential at all times.

64. As we can see from the above, the rules of the *Act* have neither replaced nor changed the essential practices that have been integral to the health care industry for years.

65. In other words, the *Act* has solely adopted and made into law the already well-established and long standing fundamental principles of patient privacy and confidentiality of patients' health care information. Those rules and principles alike are imposed on health care providers, known as custodians under the *Act*.

66. Any health care professional or custodian who claims being unaware of the existence of the *Act* is in effect claiming ignorance of one's professional and ethical obligation to protect patient privacy.

## FACTS UNCOVERED

### Electronic patient records - Meditech system

67. 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 (see the entirety of **Part 3 – Consent re Personal Health Information** and **Part 4 – Collection, Use and Disclosure of Personal Health Information**) The ease with which health care providers and their staff can access electronic patient records have undoubtedly provided much assistance to them and to the individuals they serve for obvious reasons; however, the ease of access is a double-edged sword as it requires a greater level of supervision and control measures to ensure that only those who need to access patient records do so when they must do so.

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

***Electronic patient records in Zone 1B***

69. 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.

70. 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.

71. According to the facts that we obtained during our investigation, when a person presents to receive health care, an electronic patient record is created for that person under that person's full name.

72. In addition, where the person received care in a Vitalité facility anywhere in Zone 1B, the person – patient - is assigned an identifier number and that number is recorded in the patient's electronic record. The identifier number is specific to the patient who received health care in Zone 1B and the number has no meaning in other zones in the rest of the Province. It is simply an administrative function to track where the patient received care should more information be required when the patient attends a different facility within the facilities operated by Vitalité.

73. The Oncology Centre in this case operates from only one computer system and it is the Meditech system. The Oncology Centre uses the Meditech system to manage its patients and their personal health information and physicians who work at the Oncology Centre must use the Meditech system to access their patients' records.

74. Physicians at the Oncology Centre have been given unrestricted access to electronic patient records for all patients in the entire Zone 1B. This means that physicians working at the Oncology Centre have access to electronic patient records in Zone 1B for all individuals who have received health care services in Zone 1B, not simply for those who are patients of the Oncology Centre or their own individual practice.

75. This level of access is granted on the basis of allowing physicians to provide their medical expertise and consultations for other health care facilities and clinics throughout Zone 1B, and is intended to facilitate their ability to do so when called upon.

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

## Authorization to access patient records

77. As stated above, physicians are provided with the requisite authorization to access electronic patient records in order to do their job. The names of all physicians who are approved to access the system are added to a list of users that the electronic

information access and safety committee (known as the Comité de sécurité et accès à l'information électronique) uses to conduct random audits. As per the obligation to respect patient privacy, the physician 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.

78. 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 Oncology Centre of the Hospital.

79. Patients' personal health information is stored in electronic patient records created and maintained in the Meditech computer system. In order to use the computer system that stores patient electronic data, a physician first receives a user name and a password to enter Vitalité's secure network (provided by FacilicorpNB).

80. The username and password are unique to each physician. This enables FacilicorpNB, and by extension Vitalité, to properly track physicians' access to the Meditech system where the confidential patient personal health information is stored. After authorization to access the Meditech system has been granted to a physician, it is reviewed each year.

81. The renewal of authorization to access patient data is part of the physician's overall re-application to be granted privileges to practice. This is carried out for the fiscal year ending March 31. The physician is asked to complete and sign a "privileges form" that sets out the request to renew all privileges, including access based on the fact that the physician's declaration that he or she is in good standing, has not been the subject of complaints or professional misconduct, whether privileges were suspended or limited in any fashion in the past, and whether the physician suffers from any physical or mental illness that would affect his or her ability to practice. In addition, the physician agrees to follow all of Vitalité's rules, regulations, bylaws and administrative policies and to abide by codes of ethics adopted by physicians and surgeons in Canada. Finally, the physician has to attest to the fact that he or she has a valid permit to practice medicine in New Brunswick.

82. When the physician signs the annual privileges form, it is submitted through a process involving five separate levels of approval. When everything is found to be in order, the physician is granted privileges to practice and authorization to access Vitalité's secure network and Meditech for another year.

83. To summarize, access to patient records is therefore accomplished as follows: the physician logs on to the secure network with his or her assigned unique username and password. This enables the physician to enter the entire shared-computer system. Then, the physician must enter his or her username and password once again to be able to log into the Meditech system where the patient electronic files are stored. Once in the Meditech system, the physician can access all patient records within his or her Zone, and is able to access a specific patient's file by a variety of search options that are explained below.

***Search for patient records in the Meditech system***

84. We enquired from audit experts of Vitalité and FacilicorpNB as to whether a physician is able to access patient records inadvertently or without knowing the patient's name. We asked whether a search could be performed without specifics or identifiers simply to access any patient records and examine their contents. We also asked whether it was possible to run a query search in the Meditech system in random fashion to look at any electronic patient files. We were informed that this is possible and provided with explanations about how Meditech works.

85. To search for a particular patient's information in the Meditech database, physicians have a variety of options to find specific patient information. Physicians can search and select from a list of their own patients, a location within a facility, by admission or discharge date, and by emergency room visit, and so on.

86. When using these options, there is no need for a physician to input any information to see the results. For example, the system allows for a search "by name (Recent Visits Only)". This means that when this search option is selected, Meditech will populate and display an alphabetised list of all the patients who have been designated in the system as having recently visited, thus allowing a physician to see all of the names of the patients who fit this criteria.

87. Similarly, where the option of searching "by location" is selected, the system will populate and display a list of all of the patients who have been admitted to the selected location.

88. To search the database by a specific patient name, however, Meditech allows only two options.

89. First, a physician can search the database by using all or part of a patient's last name. When the first letter is inputted into the last name field, the database will populate and display a list of all patients whose last names begin with that letter. This search function only works for last names and the system does not allow for a similar search to be conducted by using first names.

90. Second, a physician can use another search option that works by inputting all or part of a last name, which will populate and display both exact and similar matches for that last name. Where only the first letter of the last name is inputted, it will populate and display a list of all patients whose last names start with that letter. For example, a search for the last name "Arseneau" will display all patients whose last names match or are similar (Arseneau, Arsenault, etc.). This same search function allows a physician to conduct a more defined search by using additional parameters known about the patient, including first name, initials, sex, and approximate age.

91. Therefore, accessing specific patient records can only be the result of intentionally selecting a person's patient file either by selecting from a populated list or by conducting a search for a person's full or partial last name.

92. A physician is able to access patient records inadvertently but only in a case where the physician was looking for a specific patient and mistakenly clicked on the incorrect patient name and entered that electronic patient file. When viewing that file, the error would be revealed quickly as the physician would see the patient's full identity and exit that file.

***Authorization granted to Dr. Rojas Lievano***

93. Dr. Rojas Lievano was first hired by Vitalité in 1998. Vitalité confirmed that Dr. Rojas Lievano signed privileges forms for each year relevant to this case, namely 2009-2010, 2010-2011, 2011-2012, and we have verified these forms. Apart from some administrative comments that are not relevant to this case, Dr. Rojas Lievano signed the forms in each of these years to the effect that he was in good standing, has not been the subject of complaints or professional misconduct, his privileges were not suspended or limited in any fashion in the past, and he did not suffer from any physical or mental illness that would affect his ability to practice. In addition, Dr. Rojas Lievano agreed to follow all of Vitalité's rules, regulations, bylaws and administrative policies and to abide by codes of ethics adopted by physicians and surgeons in Canada. Finally, Dr. Rojas

Lievano attested to the fact that he had a valid permit to practice medicine in New Brunswick.

94. During the course of this investigation, Dr. Rojas Lievano has indicated to our Office that, at the time of the incidents, he was not aware of the existence of the policies regarding privacy and that he was not aware of the significance of his actions and that he would not have intentionally violated the Hospital's policies or the *Act*.

95. In addition and as explained earlier in this Report, policy GEN 6.3.15 entitled CONFIDENTIALITY requires physicians to sign a Confidentiality and Declaration of Understanding form.

96. Dr. Rojas Lievano signed the Confidentiality and Declaration of Understanding form in October 2013 and completed the online training module regarding privacy and confidentiality; however, we are not aware whether he had undergone this same training and has signed this form in previous years.

97. Having signed the privileges forms, Dr. Rojas Lievano's privileges were renewed in each year relevant to this case and he was therefore granted authorization to access patient records through the electronic records system in order to practice. According to our investigation, Dr. Rojas Lievano was granted access to all of the electronic patient files for Zone 1B.

98. Therefore, since 2010, Dr. Rojas Lievano has had a username and password unique to him to access Vitalité's secure network, as well as a password unique to him to log on to the Meditech system and access patient electronic files.

## Discovery of the privacy breaches

99. In the present case, allegations of privacy breaches by Dr. Rojas Lievano came to our attention from Vitalité in March of 2013 as a result of random audits into access made by him to electronic patient records of Zone 1B.

100. Vitalité noted that its internal investigation was still on-going and that more details would be forthcoming. With this notice, we embarked on our independent investigation with a view to verify all facts already discovered and to find out the full extent of the alleged unauthorized accesses that might have taken place in this case. In that regard, our investigation was parallel to that of Vitalité's as we remained informed of the steps

undertaken and the process that would follow for notification to affected individuals and our interview of those involved. In essence, we would verify facts uncovered while ensuring that all aspects of a case of privacy breach be addressed in accordance with our oversight role.

101. It is in this overall and specific context that we looked into the allegations of unauthorized access to patient records by Dr. Rojas Lievano in our independent investigation of the matter.

***Process for random audits - access to electronic records***

102. In 2005, a process was implemented by the then known Beauséjour Regional Health Authority to perform audits on demand or random audits through a committee specifically created to perform this function in certain health care zones under this Authority in the Province. At that time, there were eight regional health authorities in New Brunswick and each zone had its own audit process. Today, these zones have been combined under the umbrella of two regional health authorities (Vitalité and Horizon) and Beauséjour is knows as Zone 1B of the Vitalité Health Network.

103. The committee struck to perform these random audits was known as the Comité de sécurité et accès à l'information électronique (translated as the *electronic information access and safety committee*). This committee was responsible for reviewing and monitoring users' access to personal health information electronic systems with a view to ensure users comply with use and disclosure of patient health information. The committee performed random audits to monitor access to patient electronic records for all staff in Zone 1B, including access carried out by physicians of Vitalité.

104. In performing random audits in relation to physicians' accesses, the committee would undertake the following steps. Each month, the committee members randomly selected five physicians who were authorized users and performed an audit on their accesses for the previous month. Where the committee met in October, for example, the audit was for accesses made during the previous month of September. The results of that search query were produced in a record referred to as an audit log.

105. For each physician selected, the audit log showed:
    - name of the physician (user);
    - period during which the audit was run;
    - date and time of the accesses performed by the physician, along with:
        - the name of the patient,
        - the patient's identification number,
        - the data sources (modules) of the patient record visited by the physician,
        - the total time (minutes, seconds) that the physician viewed the patient record,
    - the device used to access the record (number assigned to the specific computer used to access the patient record);
    - the location of the device used (a specific computer located in specific place within the Hospital; and,
    - the patient's location in the Hospital at the time of access to the patient's record (for ex. patient located in Unit 4D of Hospital).

106. The committee then selected five accesses on each page of the audit log produced (audit log can be several pages depending on the number of accesses performed by the physician in the month). Those accesses were reviewed to determine whether any appeared questionable or suspicious, i.e., whether accesses were in relation to the physician's family member, or co-worker(s), or outside of the physician's field of specialty, etc. In other words, an access that rose questions requiring further review.

107. Where any suspicious access is flagged, the committee members forward this information to the appropriate office for follow-up (privacy officer or medical supervisor). This includes verification of the patient paper file and discussion with the physician to determine authority for the access. This feedback information is then provided to the committee for conclusion or further review.

108. For example, if a physician has accessed a patient record that is not in his field of practice, through the appropriate channels, the physician is asked to explain himself or herself. If the physician states that a co-worker had asked to check on test results, then this fact is verified through examination of the patient's file (a note to this effect) or directly with the co-worker. The committee is then advised whether the access was authorized or not.

109. If the access was authorized and there was no note, the physician is asked to put a note on file; however, if the access was not authorized, the committee prepares an incident report. It takes only one unexplained access to generate an incident report.

110. The incident report is forwarded to the Chief Privacy Officer for Vitalité, and an investigation is launched as per the Chief Privacy Office's practices. One of these practices is to review the incident report and call upon the committee to conduct a more in-depth audit of that same physician's accesses. In many cases, a second audit is carried out for a period of six months. That more involved audit is carried out by first asking FacilicorpNB to pull the necessary records showing all accesses made by the physician during a six month period (FacilicorpNB is a public agency that provides IT support services to Vitalité, as well as others in the Province's health care system). Those records are then submitted to the Chief Privacy Office for review.

111. The results of the six month audit are reviewed in a similar manner in order to uncover whether there have been any additional suspicious accesses. Where some have been uncovered, the office of the Chief Privacy Officer carries out a review of those accesses, and where access is found not to have been authorized, the results of that further review warrants further investigation and notification to the Commissioner.

## Audits undertaken in the present case

### *Random audit – October 2012*

112. In this matter, a random audit was performed in October of 2012 for five physicians selected by the committee, including Dr. Rojas Lievano. The audit showed their accesses to patient records for the month of September 2012, as per the committee's usual process.

113. The audit logs would reveal accesses to some or all of the various modules composing the patient record, namely registration information, summary of treatment, history of treatment, diagnosis, lab results, pathology, etc. As a salaried physician and by that nature, an independent employee of Vitalité who has no direct supervision, Dr. Rojas Lievano had been provided with unlimited access to patient records in Zone 1B in the Meditech system.

114. Once the log of the audit was generated, the committee reviewed five random accesses per page for each physician. In regards to Dr. Rojas Lievano, it was determined that two accesses were suspicious on the basis that the patient electronic health records accessed were those of two co-workers of Dr. Rojas Lievano.

115. The committee informed Medical services for Zone 1B of these suspicious accesses. Medical Services is an office that oversees physicians and their work. In particular, the committee informed the head of that office referred to as the Medical Director. In their discussions, it was believed that the co-workers might have given permission to Dr. Rojas Lievano to access their patient records. The committee asked one of the co-workers directly and the co-worker denied having given such permission to Dr. Rojas Lievano. This was sufficient for the committee to complete an incident report on the unauthorized access.

116. We reiterate that the audit revealed the physician as a user, in this case, Dr. Rojas Lievano, the date and time of the accesses performed by that user, along with the name of the patient and so on. More importantly, the audit also revealed the specific computers used by Dr. Rojas Lievano to access these patient records in this case, all of which were computers located in the Oncology Center, in the basement of the Hospital, as well as in Dr. Rojas Lievano's own office.

***Six month audit - January 2013***

117. As a result, the committee completed an incident report and forwarded it to Vitalité's Chief Privacy Office in January of 2013 for further review.

118. As part of its practice when one unauthorized access is discovered, the Chief Privacy Office requested that FacilicorpNB produce the necessary records for a six-month audit period of Dr. Rojas Lievano's accesses. The six month audit would cover the period between July 1, 2012 and January 18, 2013.

119. A preliminary evaluation of that audit revealed 12 suspicious accesses involving eight patients between the period of July and October 2012. The Medical Director was advised of such and a process was put in place to look further into the matter. It was agreed by the Chief Privacy Office and Medical Director for Zone 1B that the local Chief of Staff and the Radio-Oncology Department Head (Chef du service de radio-oncologie), given that Dr. Rojas Lievano is a radio-oncologist, be made aware of the situation and that a meeting be arranged with Dr. Rojas Lievano to discuss the accesses.

120. These officials also proceeded to advise the Commissioner in March of 2013 of the situation through the privacy breach notification process under the *Act*.

***Initial meeting with Dr. Rojas Lievano - March 2013***

121. Given the preliminary assessment of the six-month audit, Dr. Rojas Lievano was asked to meet with the Medical Director and the Radio-Oncology Department Head in March in order to provide explanations concerning these suspicious accesses. This meeting took place on March 25, 2013, where Dr. Rojas Lievano was informed that a random audit had been performed showing an unauthorized access to co-worker's patient file and a preliminary review of a larger second audit of six months had also revealed 12 other suspicious accesses.

122. During that meeting, Dr. Rojas Lievano was visibly shaken and stated that it was poor judgment on his part. He admitted to not having had the permission to access the patient records in question. Dr. Rojas Lievano failed to provide any other reason for having accessed these records. Dr. Rojas Lievano qualified his actions by adding that he had neither copied nor communicated any of the information he had viewed in the electronic health records of these patients.

123. It appeared to those officials present that Dr. Rojas Lievano did not have bad intentions when he accessed the patient records but he recognized having absolutely no business looking at these files. A summary of this meeting was forwarded to the Chief Privacy Officer for further follow-up.

124. In essence, officials from Medical services and the Chief Privacy Office felt that the lack of explanations provided by Dr. Rojas Lievano and the laws regarding patient privacy required them to continue with the audit process.

125. Dr. Rojas Lievano was then informed that a more extensive audit would be carried out going back to September 2010.

***Retrospective audit – April 2013***

126. The Chief Privacy Office continued its investigation and carried out a third audit to determine the full extent of the accesses carried out by Dr. Rojas Lievano.

127. The audit was retrospective to the date of the coming into force of the *Personal Health Information Privacy and Access Act* in 2010. This audit was performed in April 2013 and it covered all of Dr. Rojas Lievano's accesses to patient electronic records from September 1, 2010 to January 18, 2013.

128. This signified that in total, the three audits examined the accesses to patient records made by Dr. Rojas Lievano during the period of September 1, 2010 to January 18, 2013, just over a 28-month period.

***Meetings with Dr. Rojas Lievano-May 2013***

129. A partial review of the third audit revealed a significant number of suspicious accesses, and a second meeting was decided had to be held with Dr. Rojas Lievano to impose restrictions on his access to patient records.

130. On May 16, 2013, he met with the local Chief of Staff and the Radio-Oncology Department Head. Dr. Rojas Lievano was advised of the process to be continued in relation to the suspicious accesses. His accesses would be monitored daily (prospective audits would be performed), his access privileges to patient records would be limited to those of the Oncology Centre so not to restrict his ability to practice and treat his own patients. Dr. Rojas Lievano was also given a copy of Vitalité's policy on PRIVACY BREACH.

131. Meanwhile, the systematic review of the third audit was on-going.

132. A third meeting was then held on May 27, 2013, involving Dr. Rojas Lievano, the local Chief of Staff and the Radio-Oncology Department Head, and an officer for Vitalité's Human Resources. The purpose of that meeting was to advise Dr. Rojas Lievano of his right to speak to the matter, to be informed of the restrictions already placed upon his work, and of possible disciplinary measures. In addition, Dr. Rojas Lievano was asked to explain twelve suspicious accesses made in eight patients' records that had been discovered during the audit. He was given the names of the patients. He said he had no idea who they were but knew of some who were co-workers. He said that one patient in particular had asked him to look in her file for test results.

133. When asked how he came to search for these specific patient names, he said he had used a query function of the Meditech system and performed random searches. Dr. Rojas Lievano was asked if he was familiar with the law regarding patient privacy and he

said he was not before but that he was currently, adding he was sorry and that his actions were stupid. He stated he made a mistake.

134. The officials put to him that his accesses were all women patients and of a certain age, Dr. Rojas Lievano replied it was not the case, denied it being so as he knew some of the patients personally. When asked for the reason why he was going into patient files, Dr. Rojas Lievano replied that he was not aware of the harm he was causing.

135. After having been reminded that the analysis of the larger third audit was still on-going, Dr. Rojas Lievano admitted that the officials would find more suspicious accesses.

136. A formal letter summarizing both meetings of May 16 and May 27, 2013 was forwarded to Dr. Rojas Lievano by the local Chief of Staff, and a copy sent to the Chief Privacy Officer, the Medical Director and the soon to become Medical Director, the Regional Chief of Staff, Radio-Oncology Department Head, and Vitalité's Human Resources officer involved in the case. In that letter, it was remarked that Dr. Rojas Lievano had demonstrated an exemplary cooperation.

***Review of retrospective audits -August 2013***

137. The Director of Clinical Programs-Oncology (la Directrice de programmes Clinique-oncologie) is responsible for the delivery of all services offered at the oncology unit for the Hospital. She was asked by the President and Chief Operating Officer for Vitalité to be tasked with the analysis of the retrospective audit of Dr. Rojas Lievano's accesses since September 1, 2010.

138. The results of the third audit had shown that Dr. Rojas Lievano had, in total, accessed patients' electronic records over 2300 separate times during this period of time, some of which would be during the course of his normal duties and functions at the Hospital. To determine which of these accesses were legitimate, the Director of Clinical Programs-Oncology enlisted the help of the Radio-Oncology Department Head to help with this task, given that this physician would have a better understanding of the details of the audit log. These two officials embarked on a systematic process to review and rule out those accesses that were in conformity with Dr. Rojas Lievano's duties and functions. Those accesses included those of his own patients, in addition to those of patients he was required to treat while on call at the oncology unit during that period of time.

139. From this first analysis derived from the audit log, officials were left with approximately accesses to 337 patient records that remained unexplained.

140. The next step in the analysis would require that each patient record be cross-referenced with the access and that could only be done by retrieving patient paper records. This was a more laborious undertaking that took a few months.

141. This work required a certain degree of care and attention to ensure that only the questionable accesses would be put to Dr. Rojas Lievano. In order to verify whether these accesses were legitimate, each patient physical paper file was pulled in relation to each suspicious access. Those files were retrieved from Hospital's archives. The paper file permitted these officials to cross-reference and look for any connection with Dr. Rojas Lievano and his work that would explain his having to access the electronic patient record on that particular day or at all.

142. Meanwhile, officials had held another meeting with Dr. Rojas Lievano on September 17, 2013 to apprise him of the continuing analysis of the third audit, as well as to question him on four accesses found to be questionable during the prospective on-going monitoring, i.e., accesses found suspicious since his access had been restricted in May of 2013. These four accesses were verified and found to be authorized. Vitalité and the Oncology Centre were of the view that the limits and restrictions on his accesses to patient records and on-going monitoring were effective.

143. The exercise of cross-referencing the paper records to the audit log continued until all suspicious accesses to the 337 patient records were analyzed. Some paper files showed Dr. Rojas Lievano was not the patient's treating physician and more clarification would be required to determine if he had been given permission or otherwise had authority to access those patient records. Also, some patients did not have paper files in archives which made that verification quite difficult.

144. The results of this analysis were provided to the Chief Privacy Officer, and it was found that suspicious accesses remained unanswered for 168 patient records. It was decided that Dr. Lievano would have to provide these answers.

***January 24, 2014 meeting with Dr. Rojas Lievano***

145. With their audit and review work completed, the Chief Privacy Officer, the Director of Clinical Programs-Oncology and the Radio-Oncology Department Head met Dr. Rojas

Lievano on January 24, 2014. That meeting was to review each and every one of the remaining questionable accesses to 168 patient records.

146. That meeting lasted several hours. Dr. Rojas Lievano was able to speak to each of the accesses. Some patients were identified as patients that Dr. Lievano had been asked to assist and therefore, he was provided facts to confirm that those accesses were justified.

147. Officials confirmed that Dr. Rojas Lievano had accessed the files of 144 patients when not authorized to do so, i.e., there was nothing in the patient file that indicated Dr. Rojas Lievano had permission to access the record. During that meeting, he provided more explanations regarding three of those patients' files based on his personal connection, with their consent, and this was confirmed to our Office in recent weeks with additional facts. In doing so, three of these patients' names were removed from the list as having provided permission to Dr. Rojas Lievano to access their file.

148. Therefore, Vitalité and Medical services established that there were unauthorized accesses of records belonging to 141 patients, and Dr. Rojas Lievano did not deny that finding. For these 141 patients, there were a total number of 350 separate incidents of unauthorized accesses.

149. According to the final list Vitalité put together, and being the same list presented to Dr. Rojas Lievano on January 24, 2014, and that verified the justified or non-justified accesses, the end result was that Dr. Rojas Lievano accessed without authority 141 patient files, and 350 unauthorized accesses in total during the audit period.

150. Vitalité also confirmed, for the period covering September 1, 2010 to January 18, 2013, the following:

- total number of patients affected was 141 and they were women;
- total number of unauthorized accesses was 350; and,
- these women were not his patients and he was not involved in providing health care services to them.

151. While Dr. Rojas Lievano had initially indicated to Vitalité and Medical services that the accesses were an error in judgment when interviewed previously (March and May of 2013), during the January 24, 2014 meeting, he was encouraged to provide more explanations given the results of the audits, the verifications, and his admissions.

152. He told these officials that he did not know who these women were, except for those identified as co-workers and those he had worked with or met in the Hospital in the past. Dr. Rojas Lievano stated that he was looking at these patient files out of personal interest and to find out their age. He admitted to having accessed these files without the patients' consent or knowledge, and that he had no professional reason to access their files.

153. These findings, as well as the Chief Privacy Officer's intentions in regards to these unauthorized accesses, were put in a letter that was forwarded to Regional Chief of Staff, to the President and Chief Executive Officer for Vitalité, and to the Vice President of Planning, Quality, Privacy and Human Resources. That letter demonstrated another facet of this case, namely that Medical services would embark on its own investigation into the conduct of Dr. Rojas Lievano regarding disciplinary measures through its own committee.

154. Meanwhile, the Chief Privacy Office at Vitalité continued with its process with a view to notify these patients in this case of multiple privacy breaches. Vitalité solicited our assistance to properly prepare and notify the affected individuals as per the *Act*.

## BREACH NOTIFICATION PROCESS

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

156. 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.

157. 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.

158. 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.

159. In most cases, notification to affected individuals is undertaken at the earliest opportunity.

**Breach Notification in this case**

160. After all of its work to verify the suspected accesses to patient records and the conclusions drawn in January of 2014, it followed that Vitalité and the Hospital could proceed to notify all affected individuals, as per their obligation to do so under section 49 of the *Act*.

161. As stated earlier, when multiple instances of suspected unauthorized access were first discovered in February 2013, Vitalité reported this to the Commissioner shortly thereafter on March 15, 2013. As the matter was on-going and in its early stages in terms of identifying exactly whose files had been accessed, notification to affected individuals did not take place in March of 2013.

162. In the present matter, Vitalité could not proceed sooner until it had verified and confirmed each of the accesses was indeed unauthorized and that Dr. Rojas Lievano had been given an opportunity to provide reasons for each of these questionable accesses, which took place at the end of January of 2014. As explained above, and upon our advice, Vitalité was required to proceed with a full analysis of the accesses and to provide Dr. Rojas Lievano with the opportunity to speak to the questionable accesses before such a determination be made.

163. More importantly, it was agreed by Vitalité and our Office that notification should take place in one single event with preparations in place for Vitalité's Chief Privacy Office staff to answer any calls from the public and from affected individuals about these incidents.

164. While it took a considerable amount of time from the discovery of the accesses to the final determination of those that were indeed unauthorized, we find that the delay in notification in this case was reasonable given all of the circumstances. Moreover, the delay in notification did not in any way diminish the gravity of the situation or the fact that Vitalité took its responsibilities to address the situation seriously.

165. Vitalité notified all individuals affected by the privacy breaches by mail in late February 2014. The notification letter informed the individual of the privacy breach discovered in February of 2013 that was the result of unauthorized access to patient information having occurred at the Hospital between September 6, 2010 and November 30, 2012.

166. Individuals were advised by Vitalité that the information accessed could include, depending on the particular patient file, name, address, Medicare number, and other personal information, but also reasons for referrals, diagnosis, type of tests undergone and results, and more. Individuals were also informed that the accesses were performed from computers located at the Hospital and that corrective action had been undertaken since the discovery to protect patient information. They were also advised of their right to file a complaint with the Commissioner regarding the breach but more importantly, Vitalité encouraged all those who wanted to call with questions or concerns to do so.

167. Of these women notified, over a third of them contacted Vitalité's Chief Privacy Office to obtain further information, including what specific information in their patient files had been viewed by the physician in question, and specifically why – outside that of having poor judgment – had the physician accessed the information. A few asked whether they should fear for their personal safety. Many asked to be advised of the reasons why the accesses were made and of the disciplinary measures that would be imposed.

168. A few of these patients stated that they did not know Dr. Rojas Lievano by name, but when his picture was published in the resulting media coverage, they recognized him as having seen him and interacted with him at their place of work or leisure (restaurants, bars, gyms).

169. The women patients who knew him or had interactions with him stated they found his actions disturbing, but by the same token, they did not believe he had bad intentions or wanted to cause them harm. Of those who did not know him or had ever interacted with Dr. Rojas Lievano, they found the accesses to their patient file also disturbing, a few wondered if they should be worried for their safety, and some wondered if he was selling their information such as to pharmaceutical companies.

170. Some who were employees at the Hospital who received notification letters expressed awkwardness in having to work there. Eleven individuals wanted Vitalité to go back further than 2010 for their particular patient file and Vitalité did so. Of that specific further search and examination, Vitalité found that unauthorized accesses to four additional female patients' files had occurred between 1998 and 2010. For purposes of this investigation, the operative timeline for the incidents examined were those from September 1, 2010 only.

171. Most individuals who called the Chief Privacy Office wanted to find out who was responsible for the breaches and the reasons why accesses to their patient records took place.

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

- *Who is the physician who committed the breach?*
- *How did the breach occur?*
- *Why did the breach occur?*
- *Does the physician in question still work at Vitalité Health Network?*
- *Could the privacy breach result in identity theft?*

173. We referred the question of the identity of the physician who had accessed their file to Vitalité and advised that they could get more details on what aspects of their patient record had been accessed. We assured these individuals that all of the answers to their questions would be contained in our Report of Findings.

## OUR VERIFICATION OF THE UNAUTHORIZED ACCESS

174. As part of our independent role, we examine thoroughly the list of unauthorized accesses that was provided to us by Vitalité. We found two discrepancies on the list; one name that was not part of the notification list and one name that was not on the unauthorized access list. Both these discrepancies were resolved through further clarification by Vitalité in recent weeks. The one name that was not part of the notification list was in fact not a case of unauthorized access, as that patient file access had been cleared to be a justified access. The other name that was included on the notification list but was not included on the unauthorized access list ought to have been; this was found to be a clerical error when Vitalité officials put the final lists together for our review.

175. We note that the final lists provided by Vitalité were derived from the full list of unauthorized accesses presented to Dr. Rojas Lievano on January 24, 2014, less those names of patients whose access were found to be justified. We have already mentioned above that other accesses were recently verified to ensure they were justified and found to be such.

176. As a result, we have been able to verify and confirm that for the audit period between September 1, 2010 and January 18, 2013, Dr. Rojas Lievano accessed 141 patient files as an unauthorized user at the time of the accesses. The verified number of unauthorized accesses was 350 during that same period of time.

177. We also note that the audits carried out by Vitalité for the audit period in question showed that the user was Dr. F. Rojas Lievano, and that was determined through the audit's verification of the access made by a specific user name and passwords, in this case, those that were assigned to Dr. Rojas Lievano during the audit period in question.

178. The audit reports also showed that access to the electronic patient records with Dr. Rojas Lievano's username and passwords, were made from 13 separate computers, all of which were located in the Oncology Centre. One of these computers was specifically assigned to Dr. Rojas Lievano's office at the Oncology Centre.

179. This signifies that Dr. Rojas Lievano was not authorized under the *Act* when he accessed 141 electronic patient files, on 350 separate occasions.

180. In other words, we find that Dr. Lievano committed 350 separate incidents of privacy breaches under the *Act* affecting 141 individual women.

181. Additional observations showed that the files accessed were those of women only. The ages of these women were between 13 and 39. Dr. Rojas Lievano also accessed the same patient files several times over the course of the audit period, from a few times to a considerable number of times. For instance, in one case, Dr. Rojas Lievano accessed the file of one single patient 27 times, namely accessing the same patient record 6 times in the fall of 2010, 14 times in 2011, and 7 times in 2012.

182. We similarly observed that Dr. Rojas Lievano had accessed on the same day, within a few minutes apart, the files of women patients that had the same family name but different first name.

183. The audits revealed accesses that were performed in patterns, patterns of access to only women patient files, of a certain age group, to specific women's file, accesses carried out to the same patient file many times over a period of months and years, and so on. These patterns would be the subject of considerable examination on our part in order to find whether the admitted unauthorized accesses by the physician were the result of an error in judgment, accidental, inadvertent or intentional. Our findings in this regard are reported further below.

## LAW AND ANALYSIS

184. We are often asked to explain what the *Act* is and what it is intended to do.

185. Earlier, we spoke on the purposes of this important legislation found in section 2 that call for individuals to access their own personal health information of individuals and that call upon custodians in the health care industry to handle the information with confidentiality to protect the privacy of these individuals. All of the purposes combined seek to improve the overall health care system in New Brunswick: individuals feel they can be comfortable in sharing their private information knowing that it will be kept confidential and secure while health care providers are better equipped to provide care by using patient information that is more accurate, up-to-date and complete.

186. The *Act* applies to all personal health information ever collected by health care providers and that which is found in their records, including all the information collected before the *Act* came into effect (section 3).

187. More importantly, the *Act* codifies those 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 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.

188. This case is about access to personal health information of patients; what is meant by *access* in terms of the *Act*?

189. Accessing information means retrieving or reading the information, or in other words, handling that information. Handling information is considered using the information, as we find in section 1 of the *Act* that defines 'use' in that very fashion:

> 'use' means to handle or deal with information, and includes reproducing the information but does not include disclosing the information.

190. Accessing information does not necessarily include sharing or communicating the information, as those actions are considered 'disclosure' of the information.

191. This case is therefore about access to patient information and means use of those patients' personal health information.

192. How does the law protect access or use of a patient's personal health information? The law protects access or use of the information by stipulating what are considered *permitted uses*, as in section 34 of the *Act*. Some of these are summarized below, where personal health information may be used foremost with consent, but also in other certain circumstances:

*With consent*

- for the purpose for which the information was first collected or created, and for all functions reasonably necessary for carrying out that purpose, unless the individual expressly instructs otherwise;
- for another use where the individual consents; or,

- to seek the consent of the individual (or substitute decision-maker) where the information is limited to the individual's name and contact information.

*For administrative purposes*

- to prevent or reduce a risk of harm to health or safety of the public;
- to process claims for payment for the provision of health care;
- for risk or error management to improve quality of care or programs or services of the custodian;
- to educate agents of the custodian in the provision of health care;
- for regional health authorities' planning and resource allocation, etc.

*As required in proceedings*

- when authorized by the *Act*, or by another provincial or federal statute;
- where use is permitted by a treaty, agreement or arrangement made under a provincial or federal statute; or
- in legal proceedings where the custodian is expected to be a party or witness, if the information relates to matter at issue in the proceedings.

193. Handling of personal health information with consent is regarded as the golden rule as that has been the established practice throughout the health care industry.

194. In the *Act*, the importance attributed to consent is made evident by an entire portion of the statute having been devoted to explain consent, how best to obtain it, when and how consent can be relied upon lawfully, and so on. These rules surrounding consent are found in Part 3. Under section 19, express consent is required before a custodian can handle personal health information relating to an individual and this would include accessing the individual's health care file.

195. There are special and limited circumstances before the custodian proceeds to collect, use or share the information to perform a health care related task without consent, such as in an emergency to contact a close family member and individual unable to provide consent, or in approved research projects with de-identified information (as stipulated in Divisions A, B, and C of Part 4 of the *Act*.

196. As for Division D of Part 4, it sets out those rules regarding practices, policies, procedures as well as how to maintain the security of the information to uphold the rules regarding the handling of personal health information. In particular, what will constitute a breach of privacy and what to do when a breach takes place, and how to avoid a breach of privacy with security safeguards.

197. Finally, all custodians are mandated by section 50 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*:

- ✓ 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, storage and destruction;
- ✓ require use of:
  - strong passwords, changed on a regular basis,
  - up-to-date encryption software.

198. Administrative safeguards can include policies and procedures regarding the handling of personal health information in the office, training for staff and anyone who will be handling the information on those policies and procedures, confidentiality oaths for staff and others who act for the custodian, secure methods of sharing personal health information in daily tasks (encrypted e-mail, fax, regular confirmation of contact information to minimize misdirected faxes and e-mails, and distinct user and passwords for any individual with access to the personal health information to monitor their use).

199. Technical safeguards are those practices that look to control or limit access of custodians and their staff to only the personal health information needed to do their jobs, including audit logs that show who viewed and/or updated personal health information, document tracking systems, and the like.

200. Physical safeguards are more observable through the use of the physical security of the devices, both paper and electronic, that contain personal health information, such as:

- locked filing cabinets,
- locked filing records areas, even after hours,
- looked storage areas,
- alarm systems,
- keeping mobile devices securely stored when not in use,
- never leaving documents containing personal health information unattended, etc.

201. When any one of these rules or security safeguards is neither implemented, followed, nor respected, custodians are at serious risk to commit what is referred to as a *privacy breach*.

202. As stipulated in the *Act*, a privacy breach is 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, a privacy breach occurs when the information is:

- lost,
- stolen,
- disposed of in an unauthorized manner, or
- is disclosed to or accessed by an unauthorized person.

(Emphasis added)

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

## FINDINGS

204. As stated earlier, this case involves four custodians, Vitalité, the Hospital, the Oncology Centre, and Dr. Rojas Lievano, and 350 multiple incidents of privacy breaches in this case involving 141 separate patients. Also indicated earlier in this Report is that four patients who were affected by these privacy breaches filed formal complaints under the *Act* and they sought answers about the privacy breaches. Our findings for these privacy breaches will provide answers to the complainant's questions while also addressing the accountability of each of the four custodians that were the focus of the investigation in relation to these privacy breaches.

## Findings regarding Vitalité

### *Measures in place at the time of breach*

205. The facts that we have reported on in this investigation have demonstrated that Vitalité as a custodian under the *Act*, has taken its statutory responsibility seriously and has implemented measures by which the rules of the *Act* must be followed, particularly the protection of patients' privacy.

206. These measures are made compulsory to staff as part of their condition of employment, and apply to salaried physicians, i.e., physicians employed by Vitalité.

207. These measures were in place when the breaches took place, in that Vitalité had:

- established a separate Privacy Office specifically created for the implementation and enforcement of its privacy practices;
- implemented overarching policies on Confidentiality and Privacy Breach, with mandatory requirement for all staff to undergo Confidentiality training, including the requisite security safeguards;
- required salaried physicians to adhere to additional privacy practices each year, by signing a Declaration attesting to the fact that they would follow Vitalité's policies;
- required salaried physicians to sign a form in which they promised to respect Vitalité's practices, rules, policies, before having their hospital privileges renewed;
- random audits to monitor any suspicious activity in relation to access to personal health information of patients by authorized users, and these audits applied to physicians' access to patient records;
- a process to notify Clinical services when the alleged privacy breach concerns a physician, that has the power to impose restrictions on physicians' handling of confidential patient information, and in some cases, disciplinary measures;
- a notification process in place to inform the Commissioner and affected individuals of a privacy breach, in accordance with the requirements for doing so under the *Act*.

208. In addition, Vitalité continues to stress the importance of confidentiality as a term of employment or working condition in its facilities, with compulsory awareness sessions on confidentiality.

***Concerns and need for improvement***

209. While it is evident that Vitalité is making its employees aware and training them on how to properly handle patient's personal health information, we have concerns about the monitoring of their actions when handling this confidential information through its audit process.

210. As demonstrated by this case given the length of time it took to discover the multiple unauthorized accesses performed by Dr. Rojas Lievano, the random audit process could be more effective if they were carried out more often. The activities of Dr. Rojas Lievano in this case were only revealed when it came time for the audit committee to include his name on the list of random audits made by physicians, but he had been accessing patient records without authorization for a very long period of time.

211. By instituting more frequent random audits, suspicious activities will be detected more quickly; equally important, more frequent random audits will also serve as a deterrent to all users to only access electronic patient records when authorized. We will recommend that Vitalité continue its process of random audits but that they be conducted on a more frequent basis.

212. Overall, however, we find that Vitalité was not the cause of multiple incidents of privacy breaches that took place in this case in that it met its burden to keep patient information confidential, but for the actions of a physician that went undetected outside the conduct of the audit of his accesses. Our concerns will be addressed in the form of recommendations for additional measures to ensure that future situations of this nature are discovered more quickly.

## Findings regarding the Hospital and Oncology Centre

213. Likewise, we find nothing that would have led either the Hospital or the Oncology Centre to discover the unauthorized accesses and multiple incidents of privacy breaches by Dr. Rojas Lievano. The Hospital and the Oncology Centre as custodians acknowledged and do follow the requirements of the *Act* by seeing to the regular implementation of Vitalité's policies and practices regarding patient privacy.

214. Colleagues and supervisors of Dr. Rojas Lievano had no reason to believe or suspect that he was accessing electronic patient records without consent or authority, and no one

reported issues surrounding Dr. Rojas Lievano's quality of work and treatment of his patients.

215. As reported earlier, physicians enjoy independence given the nature of their work, and this independence includes unlimited access to electronic patient records. In this regard, there is no direct supervision at this level, and no facts showed that the Hospital and the Oncology Centre detected any suspicious activity on the part of the physician, Dr. Rojas Lievano, that would have led them to verify his access to patient records. He acted alone and for this reason, only Dr. Rojas Lievano knew that this was taking place.

216. The random audit function of physicians' accesses performed by Vitalité became for the Hospital and the Oncology Centre the only means to detect this problem. Upon being notified of the privacy breaches in this case, the Hospital and Oncology Centre acted and made staff available to assist in the investigation, including referring the matter to their local and regional Clinical Services committees for follow-up, as we found took place.

217. We are satisfied appropriate steps were taken to secure patient information by imposing restrictions on Dr. Rojas Lievano's access to patient records in the course of his daily practice and on-going monitoring when the suspicious accesses were discovered and being investigated.

218. As such, we have no findings of wrongdoing on the part of either the Hospital or the Oncology Centre in relation to these multiple privacy breaches.

## Findings regarding Dr. F. Rojas Lievano

### *How these privacy breaches occurred*

219. Dr. Rojas Lievano argued of not being aware the existence of Vitalité policies or the law respecting patient privacy that placed limits on his access to their records to only those instances where he was authorized; however, as indicated above in this Report, there is no excuse for any physician or other health care professional to not be aware that patient privacy matters and that patient privacy extends to the protection of personal health information found in their records at all times.

220. The facts show that Dr. Rojas Lievano used his unlimited and unsupervised access to electronic patient records for patients in Vitalité's Zone 1B when clearly not authorized to do so.

221. As stated earlier, we fully examined whether his accesses to these patient records specifically were as a result of error in judgment, accidental, inadvertent, or otherwise justifiable. The facts revealed, however, that the accesses were intentional and could not have been accidental.

222. Patterns of accesses emerged from the analysis of the number and type of electronic patient records performed by Dr. Rojas Lievano. During the audit period, he accessed 141 patients' records, all of which were young women between the ages of 13 and 39, in total, 350 times. None of these individuals were his patients.

223. When confronted about his accesses to these women patient files, Dr. Rojas Lievano denied this being the case. He reported knowing a few of these individuals (co-workers or employees at the Oncology Centre or the Hospital). When asked how he came to look at these specific patient files, Dr. Rojas Lievano stated he had performed random searches in the Meditech system. Dr. Rojas Lievano also said that he had made these accesses without the patients' consent or without authority.

224. The search options for Meditech have been described above, and show that a specific patient file can only be accessed by pulling up lists of patient names, or by conducting searches by patient name. In other words, these searches options are intended to allow the user to find a specific patient file.

225. Furthermore, the details contained in the audit log demonstrated that the accesses could not have been random or inadvertent. As stated above, the audits revealed that he had accessed 141 patients' records, amounting to a total of 350 unauthorized accesses. In some cases, access to the same woman's patient record was made repeatedly by Dr. Rojas Lievano over the course of the entire audit period. For instance, for seven women patients, Dr. Rojas Lievano accessed their records between 6 and 27 times, and for some of these women patients, several times during the same month. We also found that the unauthorized accesses took place multiple times during a short time period.

226. In a single month, Dr. Rojas Lievano accessed without permission many patient records numerous times: for instance, he made unauthorized accesses 38 times in November of 2010 and 28 times during the month of May of 2011. In other instances, Dr. Rojas Lievano was looking at patient records of women with same or similar names within minutes of each other. Two women patients with the same name had their files accessed by him within one minute. Three other women with same or similar names

had their files accessed on the same day at these times 3:25 pm, 3:26 pm, 3:34 pm, and 3:35 pm.

227. We find that the manner in which these accesses were performed could not be accidental or inadvertent, given that none of these women were Dr. Rojas Lievano's patients, and given the frequency of access to their files in the course of a day, month or year. Even if we considered that access to a particular patient record could be inadvertent, namely opening the wrong patient file, we were nevertheless presented with facts that showed that Dr. Rojas Lievano often looked at the patient's different medical information.

228. The audit logs revealed that Dr. Rojas Lievano went into several fields of information and it should have been apparent upon first opening the patient file that he was looking at the wrong patient. Some accesses were for a less than one minute but Dr. Rojas Lievano still clicked on and entered into several modules for many patients, such as their registration information, visit history, radiology reports, care-area administrative data, nursing archive data forms, etc. By spending this extra time in the patient file and clicking on several fields in order to see more of the patient file, we cannot find that Dr. Rojas Lievano's accesses could have been accidental or inadvertent. In addition, there were multiple instances of this level of access to many fields in a single patient file occurring to have been anything but intentional.

229. We also repeat that the facts uncovered in this investigation showed that many of the affected individuals who contacted Vitalité after receiving their notification of the privacy breach recognized Dr. Rojas Lievano and had interactions with him at work or in the community (current or former co-workers, recognized him from local restaurants, fitness clubs, etc.). There were not his patients and these facts demonstrate that he was directing his search of patient files to find these specific women.

230. We find that the accesses performed by Dr. Rojas Lievano were deliberate and intended to look at specific women's patient information while he knew he had no authority to do so, and that he did so without their consent.

231. We find that the facts uncovered in this case clearly demonstrate that Dr. Rojas Lievano committed 337 separate incidents of unlawfully accessing personal health information of 143 individuals, without professional justification or consent.

232. Patient privacy is a right and all those working in the health care sector, including physicians, have a professional and legal obligation to keep patient personal health information confidential at all times. The rules of the *Act* has neither replaced nor changed the essential practices that have been integral to the health care industry for years. Those rules and principles alike are imposed on health care providers, known as custodians under the *Act*. Any health care professional or custodian who claims being unaware of the existence of the *Act* is in effect claiming ignorance of one's professional and ethical obligation to protect patient privacy.

233. In this case, Dr. Rojas Lievano is a duly licensed physician, employed by Vitalité under whose direction is required to be familiar about its policies and practices, including policies GEN.6.30.15 CONFIDENTIALITY and GEN.6.30.20 PRIVACY BREACH regarding patient privacy and his obligations that flow therefrom. In addition, Dr. Rojas Lievano signed for each year of this audit period a *Declaration* attesting to the fact that he was familiar with and accepted to abide by Vitalité's administrative policies and regulations in order to have his working privileges renewed, including his unlimited access privileges to Meditech database.

234. We find that the use of these patients' personal health information by Dr. Rojas Lievano, a custodian, is in contravention of the *Act* as per Part 4, Division B (sections 32 to 34). Moreover, we find that Dr. Rojas Lievano's accesses to these patient records, namely using the patients' personal health information without their consent or lawful authorization, constitute offences under paragraph 76(3)(a) of the *Act* :

> 76(3) A custodian or information manager commits an offence if the custodian or information manager
>
> (a) collects, uses, sells or discloses personal health information contrary to this *Act.*

235. The matter of whether discipline should be imposed in relation to these offences and that remain within the role of the employer, Vitalité in this case. We will, however, recommend that such measures be considered. Likewise, we do not determine the sanctions that may flow from these offences, that remaining within the realm of court process under the *Provincial Offences Procedures Act*.

***Why these privacy breaches occurred***

236. The question as to why Dr. Rojas Lievano committed these breaches of patient privacy was answered by explanations he provided directly to Vitalité during the course of this investigation, out of personal interest and in wanting to find out their ages. These reasons are sufficient for us to establish that Dr. Rojas Lievano knew what he was doing when he accessed the patient files without their consent and without lawful authority.

237. Dr. Rojas Lievano admitted and recognized when asked for each of the 350 separate incidents of access to patient files that he had no permission, consent or that the access was not otherwise justified. We wish to point out that the investigation did not uncover any evidence to suggest that Dr. Rojas Lievano shared or otherwise communicated the personal health information of these patients, or that he accessed for any other purpose than for personal interest. Vitalité uncovered no evidence leading it to believe that any of these 141 patients were at risk because of the physician's unauthorized accesses.

***Unauthorized access to patient information and identity theft***

238. Another concern brought to our attention was the risk of identity theft due to Dr. Rojas Lievano's unauthorized accesses to personal health information of the complainants, and others who contacted our Office with such a question. Again, we verified all of the facts of this case thoroughly and we did not uncover any evidence to suggest that Dr. Rojas Lievano accessed the patients' records to use or share their personal information, to steal or sell their identities to third parties, or even set up lists and sell them to pharmaceutical companies. Nothing we found led us to believe that Dr. Rojas Lievano was mining the identities of these patients for fraudulent purposes.

239. 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 these comments.

240. 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.

241. 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*).

### *Is Dr. Rojas Lievano still working for Vitalité Health Network?*

242. The salaried physician in this case violated the *Act* and committed offences on several occasions that he admitted were performed without permission and therefore deliberate.

243. Where serious wrongdoing has been established, the Commissioner will not recommend that disciplinary measures be imposed but instead recommend to Vitalité, a custodian and the physician's employer in this case, that such measures be considered to ensure the integrity and security of patients' personal health information at all times.

244. Dr. Rojas Lievano actions were not justified. The facts are of sufficient severity and of such scale that action should be taken to demonstrate that unauthorized access to personal health information will not be tolerated in New Brunswick. These actions

could include the possible laying of *informations* for having committed multiple violations of the *Act* under the offences provisions found in section 76.

245. We have been asked if Dr. Rojas Lievano is still working, and that question was also asked of Vitalité. Shortly after the extent of the breaches became known, Dr. Rojas Lievano was permitted to continue to work at the Oncology Centre but with important limits and restrictions for his access privileges to patient files and with on-going monitoring of his accesses to patient databases.

246. In the context of these findings for privacy breaches committed under the *Act*, we are not aware of Dr. Rojas Lievano's current work status with Vitalité. That question rests with Vitalité as the physician's employer.

## CONCLUDING COMMENTS

247. 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 handled only when necessary and as 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.

248. Snooping in medical records is quickly becoming one of the most reported and publicly reproachable actions on the part of custodians who handle patient information to work in the health care industry throughout Canada.

249. In the Province of Saskatchewan, a recommendation has been made by the recently retired Information and Privacy Commissioner that snooping be made an express offence under the law. A physician in Alberta who was caught snooping was found guilty of unprofessional conduct by the College of Physicians and Surgeons of Alberta and suspended for at least a month for having accessed the electronic health records of three people without having a patient/physician relationship with those people.

250. 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 staff of the Office of the Information and Privacy Commissioner stemming from complaints received by the Office that both individuals had allegedly improperly accessed the personal health information of a number of patients.

251. It is unfortunate that we are seeing this trend across the country and regrettably, it has occurred here in New Brunswick.

252. This case illustrates the ease with which one can open and read patient information in electronic files when a health care professional is granted an unlimited level of access. Being able to browse through medical records as was demonstrated in this matter by the physician responsible causing several hundred privacy breaches is the main reason why we will recommend that Vitalité Health Network undertake a much stricter surveillance by performing random audits of access to computer systems.

253. Evidenced by the high number of individuals who contacted Vitalité to ask questions and share their concerns, in our view, this demonstrated the impact it had had in their lives. Unlawful access to one's personal health information impacts those to whom the information belongs; it is a violation of their privacy.

254. This case presented many challenges to all those affected by it, due to its nature, involving serious breaches of privacy, for a very large number of individuals, over an extended period of time, by a physician. As with all cases, this investigation was carried out over the last 17 months by not only taking into consideration all of the relevant facts and its particular circumstances, but also by maintaining a proper balance between the obvious impacts it has had upon those affected and the physician himself.

255. The case has been the subject of much media coverage, raising its profile and putting into sharp focus both the implication of the *Act* as well as the impact upon all those affected and the physician in question.

## RECOMMENDATIONS

256. In view of all of the above findings, the Commissioner recommends corrective measures, intended to prevent future recurrences of unlawful accesses to electronic patient records and equally serve as a deterrent to all those who work in Vitalité's public health care institutions by ensuring that:

- the frequency of random audits be increased,
- actions be undertaken more quickly when suspicious activities are discovered to limit or restrict access,
- to continue the limits, restrictions and on-going monitoring imposed on Dr. Rojas Lievano's access to patient files,
- Vitalité consider imposing disciplinary measures on Dr. Rojas Lievano, and
- Vitalité consider whether charges under the *Provincial Offences Procedures Act* would be appropriate in this case.

## Recommendations issued to Vitalité

257. The Commissioner issues the following recommendations to Vitalité Health Network:

**Recommendation 1** The Commissioner recommends that within the next six months of the date of this Report of Findings, Vitalité implement a process and ensure that adequate resources are allocated to permit the undertaking of more frequent and regular random audits of accesses to Meditech patient databases that currently exist. These more frequent and regular random audits must include physicians and all other professional health care providers employed by Vitalité.

Vitalité will be required to provide the Commissioner a status update on the implementation of **Recommendation 1** by October 24, 2014.

**Recommendation 2** The Commissioner recommends that Vitalité continue with its practice to limit and restrict the access privileges of any custodian in its employ whose suspicious accesses to electronic patient records as soon as those accesses are determined by Vitalité to have been unjustified. The Commissioner further recommends, in such a case, Vitalité must impose regular and on-going monitoring of the accesses to be performed by the employee-custodian until a final outcome of the case. The Commissioner further recommends that Vitalité add these practices to its audit process and inform its entire professional staff of such.

Vitalité will be required to provide the Commissioner with a confirmation of the implementation of **Recommendation 2** by October 24, 2014.

**Recommendation 3** Given the multiple incidents of privacy breaches that have been established in this case, and to continue to protect personal health information of patients housed in the Meditech patient database, the Commissioner recommends to Vitalité that the limits, restrictions and monitoring currently imposed upon Dr. Rojas Lievano's access privileges to Meditech continue for a period of no less than 24 months from the date of this Report of Findings. At the end of this period, when his access privileges are restored, the Commissioner further recommends that Vitalité conduct random monthly audits of Dr. Rojas Lievano's accesses to Meditech for a period of no less than 12 months and to immediately report to the head of the Regional Medical Services of Zone 1B any suspicious activity.

**Recommendation 4** Given the multiple incidents of serious wrongdoing that has been established in this case and to ensure that the integrity and security of patients' personal health information remains a fundamental requirement for Vitalité's professional staff at all times, the Commissioner strongly recommends that Vitalité consider imposing disciplinary measures on Dr. Rojas Lievano.

**Recommendation 5** Given the scale of unlawful accesses committed by Dr. Rojas Lievano, the multiple offences committed under subsection 76(3) of the *Act*, and that it be demonstrated that unauthorized access to personal health information will not be tolerated in New Brunswick, the Commissioner strongly recommends that Vitalité consider the possibility of laying charges against the physician in question under the *Provincial Offences Procedures Act*.

258. The Commissioner's Office will follow up with Vitalité in the course of the coming weeks and months regarding the implementation of these recommendations.

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

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