OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
for
Prince Edward Island

Breach Report HI-18-005

Custodian: Health PEI

Prince Edward Island Information and Privacy Commissioner
Karen A. Rose

December 12, 2018

Summary: During a regular audit process, a Health PEI manager investigated further, and discovered that an employee had inappropriately accessed personal health information on the Clinical Information System database (the CIS).

The Commissioner agreed with Health PEI's conclusion that there were unauthorized accesses to personal health information of 353 individuals (snooping).

Snooping prevention
With regard to breach prevention, the Commissioner found that Health PEI had established reasonable information practices to prevent snooping. However, the Commissioner found that the scope of personal health information accessed by the breaches would have been less, if established information practices had been implemented by Health PEI relating to user access credentials. The employee's user access credentials should have been changed from that of an LPN to that of a PCW. The Commissioner found that Health PEI has taken reasonable steps to remediate this shortcoming, to avoid such a failure to implement in future.

With regard to automatic logout periods for inactivity on the CIS, the Commissioner recommended that Health PEI review their logout standards, with a view to what time period is appropriate for the level of sensitivity of the personal health information to be protected, in accordance with subsection 39(2) of the *HIA*.

Snooping detection
This breach, and others recently investigated by Health PEI, indicate that snooping is not a one-time event in the health care system. Given the risk of snooping in electronic databases, the Commissioner found that Health PEI's use of random auditing was a positive and proactive step to detect snooping. However, current random auditing alone had not been able to detect this snooping breach over a three year period. Therefore, the Commissioner found that Health PEI has not yet established reasonable information practices to detect snooping. The Commissioner encouraged Health PEI to follow through with auditing improvements it has already planned, and the Commissioner also recommended that Health PEI analyze their processes for detection of snooping activity, including auditing and management training, with a view to establishing and implementing more robust detection methods.

Breach response
The Commissioner found that Health PEI responded reasonably once the breaches were discovered, including timely and appropriate notification to affected parties and to the Commissioner, reasonable steps to contain the breach, a thorough investigation, and reasonable measures to remediate with training and education. However, the Commissioner recommended improvements to breach detection methods, as noted above.

In most circumstances individuals who interact with a health care provider should know who is accessing their personal health information. In cases of CIS snooping, affected individuals have a heightened need to know the identity of the snooper, for various reasons, but primarily to identify whether the snooper is someone with malicious intentions. The Commissioner recommended that, for any future cases of CIS snooping, Health PEI should proactively provide a copy of an excerpt of the log of accesses to an affected party's electronic personal health information on the CIS, highlighting the dates(s) and the name of the snooper.

Statutes Considered: *Health Information Act*, SPEI 2014, cap 31, ss. 1(r) and (t), 10, 22, 34, 36, 37(1)(r), 39, 75.

Reports Cited: Breach Report HI-18-001, *Prince Edward Island (Health) (Re)*, 2018 CanLII 83554 (PE IPC)

I. BACKGROUND

[1] In order to fully understand the circumstances leading up to this Breach Report, it is necessary to describe the electronic medical records system of Health PEI, and Health PEI's audit capacity and practices.

The Clinical Information System

[2] Health PEI has an electronic medical records system, often referred to by the name of the supplier, Cerner, or as the Clinical Information System ("the CIS"). This system digitally stores personal health information of patients.

[3] Health PEI protects the personal health information in the CIS with a number of administrative and technical safeguards, including:

a. The system administrator creates user accounts for individuals to access and use the CIS. The system administrator provides each user a unique username and initial password, which users re-set to their own personalized passwords.
b. Health PEI has a procedure to advise the system administrator if an individual leaves work (permanently or temporarily), so that the individual's user account may be revoked.
c. Health PEI recently reviewed and disabled user accounts that had been inactive for more than 18 months.
d. The scope of personal health information a user may access or use is electronically limited, depending on an employee's staff position within Health PEI. The system administrator permits a user to view, add, or change various fields of an electronic medical record, based on the defined roles of an employee in that position. For example, if an employee's role includes viewing, but not recording a patient's weight, then that field is visible, but

the field is locked and the user is not permitted to enter or change the patient's weight in the electronic medical record.

e. Every time a user accesses, adds, or amends personal health information in the CIS, a new record is created, detailing who accessed the personal health information (by their username), when the personal health information was accessed (date, time), to whom the personal health information belongs (name and Provincial Health Number of the patient), and what personal health information was added. This is sometimes called a digital footprint, an audit trail, or an electronic log book.
f. Users are required to be trained in confidentiality and the acceptable use policies of Health PEI, with training supported by a confidentiality agreement. While annual retraining is not currently part of Health PEI's practice, users require retraining when they return to work following an extended leave of absence.
g. Access to the CIS is timed out automatically after a period of inactivity.
h. Health PEI monitors compliance with their policies by conducting routinely scheduled audits of randomly selected users and patients, and audits on request.

Audits

[4] The Senior Information Security Specialist initiates audits, by compiling a record of every access made by a randomly selected pool of users, and compiling a separate record of every user who accessed a randomly selected pool of patients, within a set time range.

[5] The audit of a user shows all of the patient records that the user accessed within a certain time period. The direct managers of the user interpret the audit reports, as they would know which patients the user was caring for and treating, and are best able to identify unauthorized access.

[6] An audit of a patient shows all of the users who accessed that patient's electronic medical record within a certain period. At the Queen Elizabeth Hospital ("the QEH"), the nurse manager of the unit in which the selected patient was resident, interprets the audit report, as they would best know which employees were caring for and treating the patient, and are best able to identify unauthorized access.

[7] In addition to these regularly scheduled audits, a manager may request an audit with respect to a certain individual patient or user. Health PEI calls these 'trigger audits'.

Facts Giving Rise to this Breach Notification

[8] In the course of reviewing an audit of a patient's electronic medical record, a nurse manager at the QEH checked the patient's electronic medical records to review the list of users who had worked with this patient.

[9] The nurse manager observed that an employee ("the Employee") had accessed the patient's records, but that the Employee was not a caregiver for this patient. The Employee was a personal care worker (PCW) who, the nurse manager knew, works in the role of providing constant care.

[10] Constant care is assigned for patients who are at risk for certain hazards, including falls or flight. A patient receiving constant care has one-on-one supervision; usually a PCW provides this service and remains with the patient at all times.

[11] The nurse manager recalled that this patient did not require constant care. In addition, the nurse manager does not expect any employee providing constant care to access the CIS because, at the QEH, constant care PCWs do not need to access or input personal health information in the CIS. They are given the medical information they may need to perform their duties by the nursing team, and do not enter data into the CIS. They fill out a paper chart during their shift, a "Behaviour Flow Record", which is kept by the patient's bedside and filled in periodically during the shift.

[12] Because the nurse manager recalled that the Employee usually works to provide constant care, the nurse manager requested a trigger audit of the Employee for the previous year.

[13] The trigger audit confirmed that the Employee had accessed personal health information of multiple patients within given shifts, and personal health information of some hospital staff.

[14] The nurse manager advises that they had previously twice observed the Employee at work at a computer, and on both occasions had instructed the Employee not to use the computer while at work. The nurse manager thought the Employee was using the computer for personal use, and had no suspicions that the Employee had been accessing patients' personal health information on the CIS.

[15] This trigger audit prompted further investigation by the Employee's manager. The nurse manager who requested the audit was no longer involved in the investigation.

II. THE INVESTIGATION

[16] The Employee's manager determined that many incidences of the Employee's access to personal health information in the CIS, were not authorized.

[17] The Employee's manager also observed that the scope of the Employee's user access to view, enter and change personal health information in the CIS was as a Licensed Practical Nurse (an "LPN"). The province had amended the educational qualifications for those working as an LPN effective April 1, 2014. The Employee had been an LPN until April 1, 2014, when the statutory education qualifications for an LPN came into effect. The Employee had not obtained the education requirements and continued to work as a PCW. While PCWs do have access to the CIS, the scope

of information they can access is more limited. However, the scope of the Employee's user access to personal health information had not been changed to reflect the change in the Employee's role.

[18] The Employee's manager ordered an audit from April 1, 2014 forward, which showed the Employee had accessed the personal health information of 353 patients, without the need to do so.

[19] The Employee's manager interviewed the Employee, who admitted to the unauthorized access of personal health information. The Employee did not initially provide an explanation for the incidents of access to personal health information.

[20] Health PEI conducted further audits to assess whether the Employee had added, changed, or printed any personal health information. It is not possible to delete personal health information in the CIS, so Health PEI is not concerned about deleted information. Audits showed that the Employee had modified some charts, adding information related to vital signs, activities of daily living and dietary orders. The audits did not indicate that the Employee had changed, or printed any personal health information.

[21] Once it was determined that the Employee had accessed the CIS without authorization, Health PEI immediately revoked the Employee's access to personal health information, and cancelled all of the Employee's scheduled shifts.

[22] Health PEI notified the Charlottetown Police, which investigated, and found no evidence of offences under the *Criminal Code*.

[23] Health PEI notified the Information and Privacy Commissioner, notified the public via a press release, and notified by mail the affected individuals who were not deceased, within 10 days of discovering the unauthorized access. Health PEI also set

up a hotline for the notified individuals to respond to any questions. Health PEI advises that some of the notices were not delivered (returned).

[24] Health PEI no longer employs the Employee. There is no opportunity for continuing coaching of this particular Employee. However, Health PEI has taken steps to remediate this breach.

Input from Affected Parties

[25] This Office provided an Investigation Summary to the individuals who are affected by this breach, setting out the facts described above, and inviting them to contact this Office with representations, questions, or concerns they may have.

[26] We received 12 responses from either an affected party, or their representative. In two cases, the communication was for the purpose of advising that the affected party was deceased. The concerns which were raised involved the following questions:

- When did the breach occur, and how many times?
- Who accessed the personal health information, and what information did they access?
- How do I know for sure that the personal health information was not disclosed to others?
- For what purpose did the Employee breach this personal health information?
- Are such breaches included in an employee's personnel records, or references?
- How did the Employee have access to the CIS, and how was their breach not detected?
- What is the length of the logout period on the CIS?

[27] When affected parties asked questions relating to the first two bullets above, this Office suggested that they contact Health PEI to address some of their questions. In addition, this Office requested Health PEI to respond to all of the above questions.

[28] Three affected parties stated that they did not receive the Breach Notification letter from Health PEI, which was sent by Health PEI to all affected parties in October, 2017. This Office also asked Health PEI to address this issue. This question, and the bulleted questions listed at paragraph [26] above, are addressed later in this Report, in the discussion of Issue Three.

III. ISSUES UNDER REVIEW

[29] The issues which I will be addressing in this review are:

> Issue One: Was personal health information compromised in a manner described at clause 36(1)(c) of the *Health Information Act*?
>
> Issue Two: Did Health PEI establish and implement reasonable information practices to protect personal health information from access by an unauthorized person?
>
> Issue Three: Did Health PEI respond reasonably?

Issue One: Was personal health information compromised in a manner described at clause 36(1)(c) of the *Health Information Act*?

[30] Health PEI notified the Commissioner on the basis of clause 36(1)(c)(iv), that personal health information had been accessed by an unauthorized person. Clause 36(1)(c) of the *Health Information Act* ("the *HIA")* states:

36. Duties of custodian
(1) A custodian shall
….
(c) notify the individual to whom the personal health information relates and the Commissioner in writing at the first reasonable opportunity if personal health information is
(i) stolen,
(ii) lost,
(iii) disposed of, except as permitted by this Act, or
(iv) disclosed to or accessed by an unauthorized person.

[31] Health PEI's trigger audits of the CIS confirmed that the Employee accessed electronic medical records of 353 individuals, and that the access was not necessary for the Employee's job.

[32] The *HIA* defines "personal health information" to include any identifying information about an individual in oral or recorded form that relates to the provision of health care to the individual (Subsection 1(t) of the *HIA*). I agree that the information accessed in the CIS by the Employee of Health PEI, satisfies the definition of personal health information at subsection 1(t) of the *HIA*.

[33] Health PEI does not permit employees to use their access credentials (username and password) to look up information in the CIS about anyone, unless it is related to the employee's work. The limits which custodians place on employees, with regard to accessing personal health information, are based on protection of patient and client privacy. Health PEI's policies, procedures, and safeguards against unauthorized access to personal health information, are consistent with Health PEI's obligations under the *HIA*. Section 22 of the *HIA* sets out limits on the use of personal health information. It states in part:

22. Use of personal health information

(1) A custodian shall not use personal health information except as authorized under this section.

Limitation on use of personal health information
(2) Every use by a custodian of personal health information shall be limited to the minimum amount of personal health information necessary to accomplish the purpose for which it is used.

Idem
(3) A custodian shall limit the use of personal health information it maintains to those employees and agents of the custodian who need to know the personal health information to carry out the purpose for which the personal health information was collected or received or to carry out any of the permitted uses authorized under this section.

[34] Subsection 22(5) lists circumstances that are authorized uses of personal health information. None of those circumstances apply to the Employee's use of the personal health information of the 353 affected individuals. Although the Employee made chart modifications to the electronic charts of 105 patients (totaling 835 modifications), such modifications would only have been permitted if the Employee were acting in the capacity of an LPN. The Employee also accessed charts of patients who had not been assigned to them, including one patient whose personal story had been covered in the media, at least three physicians, and at least three possible colleagues of the Employee. None of these individuals had been patients to which the Employee was assigned. In addition, as a PCW who provided constant care at the QEH, the Employee was not authorized to use the CIS at all.

[35] Because the Employee did not need to access the personal health information of these 353 individuals for duties of employment, I find that these are accesses to personal health information by an unauthorized person, the Employee, pursuant to clause 36(1)(c)(iv) of the *HIA*.

Issue Two: Did Health PEI establish and implement reasonable information practices to protect personal health information from access by an unauthorized person?

[36] Clauses 36(1)(a) and (b) of the *HIA* set out certain duties of a custodian to manage the personal health information in their custody or control:

> 36. **Duties of custodian**
> (1) A custodian shall
> (a) establish and implement information practices to facilitate the implementation of, and to ensure compliance with, this Act;

[37] The expression "information practices" in clause 36(1)(a), is defined in the *HIA*:

> 1. Definitions
> In this Act
> . . .
> (r) "information practices", in relation to a custodian, means the policies of the custodian governing actions in relation to personal health information, including
> (i) when, how and the purposes for which the custodian routinely collects, uses, modifies, discloses, retains, destroys or disposes of personal health information, and
> (ii) the administrative, technical and physical safeguards and practices that the custodian maintains with respect to the personal health information;

[38] Section 39 of the *HIA* requires that a custodian's information practices be reasonable. Subsections 39(1) and 39(4) are particularly relevant to this breach investigation:

> 39. Protection of personal health information
> (1) A custodian shall protect personal health information by adopting information practices that include reasonable administrative, technical and physical safeguards that ensure the confidentiality, security, accuracy and integrity of the information.

. . .

> Controls and safeguards
> (4) Without limiting the generality of subsection (1), a custodian shall
>
> (a) implement controls that limit the persons who may use personal health information maintained by the custodian to those specifically authorized by the custodian to do so, including where appropriate the restriction of access to an individual's personal health information by an employee, agent, contractor or volunteer of the custodian or by a health care professional who has the right to treat persons at a health care facility operated by the custodian to only that personal health information that the employee, agent, contractor, volunteer or health care professional requires to carry out the purpose for which the personal health information was collected or will be used;
>
> (b) implement safeguards and controls to ensure that personal health information maintained by the custodian cannot be used unless
> (i) the identity of the person seeking to use the personal health information is verified as a person the custodian has authorized to use it, and
> (ii) the proposed use is verified as being authorized under this Act;
>
> . . . .

[39] As noted above, Health PEI has put in place policies and procedures relating to access to personal health information, which help to ensure conformity with its obligations under the *HIA*. These policies and procedures include the following technical safeguards:

- Unique username and passwords for each user of the CIS;
- Well-defined limits on access to personal health information in the CIS, depending on an employee's job description;
- Access to the CIS is logged out automatically after a period of inactivity; and
- The creation of an electronic record each time a patient's personal health

information is accessed.

[40] Health PEI's policies and procedures also include the following administrative safeguards to protect personal health information:

- Revoking inactive user accounts;
- Training for all staff;
- Limiting access to personal health information in the CIS, depending on an employee's job duties, and the institution in which the employee works;
- Conducting proactive routine audits, and trigger audits;
- Requiring an oath of confidentiality by employees;
- Supervising employees in the performance of their job duties; and
- Prior to being provided with access to an electronic information system, all staff must review and sign the ITSS Acceptable Use of Government Provided Computer Technology Agreement, which outlines conditions for access which includes limiting staff to using systems and the information contained within them only as authorized.

[41] In addition to the foregoing safeguards, additional administrative safeguards were put in place in July, 2017, with the proclamation of the *HIA*. Health PEI underwent an updating project on its privacy policy to bring the policy in line with privacy best practices and policies in place in other jurisdictions. The new *Privacy and Protection of Personal Health Information Policy* specifically limits access to personal health information to only what is necessary for the performance of job duties. Additional policies address the use of the CIS more specifically, such as the *CIS Security and Access Policy* and the *Appropriate Use of Patient Records in the Clinical Information System Policy*. The S*ecurity and Access Policy* establishes safeguards to protect the information collected in the CIS and includes a provision expressly stating that users may only access information in the CIS as authorized for the performance of their job duties. The *Appropriate Use* policy outlines appropriate and acceptable use of

patient information by staff and includes detailed provisions regarding access to patient charts for the purpose of provision of care. In addition, the *QEH Level of Observation and Behaviour Flow Record Policy* guides staff who are providing constant care in the specific types of personal health information to collect.

Breach Prevention and Minimization

[42] Subsection 39(1) of the *HIA* requires custodians to adopt information practices to ensure the security of personal health information. Health PEI's policies and practices, when taken together, and if implemented consistently, contribute to a strong and well-woven safety net to fulfill the obligations of this subsection, for the prevention of breaches of personal health information. I find that Health PEI has established reasonable information practices for the prevention of accesses to personal health information by unauthorized individuals.

[43] As noted above, one technical safeguard of the CIS is an automatic logout after a period of inactivity. One affected individual asked about the length of time that can pass before the CIS automatically logs out a user for inactivity. Although logout time was not a factor in this particular breach, it is an important information practice for the purpose of breach prevention, in compliance with the duty to ensure security of personal health information under subsection 39(1) of the *HIA*. Therefore, Health PEI responded as follows:

> Users of the clinical information system ("CIS") are logged out of the system automatically after 30 minutes of inactivity. There are a limited number of exceptions to this rule that have been created after an assessment of the balance between risks and workflow for the purposes of patient care. One example of such an exception is physicians working in hospital emergency departments, whose accounts are set to log out automatically after 60 minutes of inactivity. This safeguard is strengthened by educating all staff on the importance of logging out when leaving a workstation (as part of core CIS training) and

through periodic reminder communication distributed to all CIS users.

[44] Health PEI's automatic logout periods for the CIS range from 30 to 60 minutes. One important factor in determining appropriate automatic logout periods is the sensitivity of the personal health information accessible on the electronic database. I make no finding regarding the reasonableness of the 30 minute automatic logout set by Health PEI for the CIS. However, subsection 39(2) of the *HIA* requires that Health PEI base their information practices on nationally or provincially recognized standards, and processes that are appropriate for the level of sensitivity of the personal health information to be protected. I recommend that Health PEI review such standards, with a view to what is appropriate for the level of sensitivity of the personal health information to be protected, in accordance with subsection 39(2) of the *HIA*.

[45] This type of unauthorized access to personal health information of patients, is often described as "snooping". For some individuals, the accessibility of others' personal health information is too great a temptation to resist. Although the policies against accessing electronic databases for anything other than work purposes are clear, and although there are penalties for unauthorized access, a small percentage of individuals will snoop anyway. For this reason, it is important to limit the access that employees may have, to only what they need to carry out their duties of employment.

[46] Subsection 39(4) of the *HIA* further requires that custodians implement controls that limit the personal health information available to various categories of individuals, including employees. Although a PCW has technical access to the CIS, such access is further limited by the policies of the institution in which they work. For example, a PCW at a long term care facility may be required to use the CIS for their job, whereas a PCW providing constant care at the QEH does not. Health PEI advises that, in April

2014, fifty-five LPNs chose not to seek licensing under the new requirements but continued to work for Health PEI as PCWs. Only 3 of these PCWs were identified to be working exclusively in constant care assignments. Health PEI confirmed, via audit, that two of these employees had followed administrative policies, and had not accessed the CIS from April 1, 2014 forward. In contrast, during this time the Employee frequently accessed the CIS, and was acting as an LPN in their use of the CIS. In fact, the Employee was inputting vital signs of patients, which is a task of an LPN, but not a task of a PCW doing constant care at the QEH.

[47] In the circumstances of this breach, one of Health PEI's administrative safeguards was not actually implemented. Safeguards are not only used to prevent breaches, but are also used to minimize the personal health information which may be at risk. This minimization of risk is consistent with subsections 39(1) and (4) of the *HIA*, set out above. In this case, an established technical safeguard was not put to use. Health PEI advises that in April, 2014, the QEH Human Resources office was notified by the LPN Association of PEI of the names of all LPNs who chose not to complete the new licensing requirements. The Employee's position changed from LPN to PCW. However, the process for changing access to the CIS is separate from the Human Resources process, and is administered by Information Technology Shared Services ("ITSS"). Management is responsible for submitting an ITSS Employee Change Request Form to ITSS. In this case, no request to change the scope of personal health information available was submitted. For the ensuing years, the Employee kept their LPN credentials to sign into the CIS.

[48] The scope of the Employee's technical access to view, enter and change personal health information was as an LPN. LPNs are able to gain CIS access to personal health information which includes the following: lab and diagnostic imaging results, nursing progress notes, physician orders, medications, diet orders, problems and diagnoses and care plans. LPNs are not able to gain access to personal health information which includes scheduling appointments, discharge information,

procedures and tasks assigned or completed by allied health (home care, mental health crisis response, palliative care, infection control, social work, occupational therapy, etc).

[49] If the Employee's access to the CIS had been changed to that of a PCW, they would have had access to less personal health information. Health PEI also provided a copy of spreadsheets indicating the scope of personal health information technically available to a PCW. Generally, an LPN has a greater ability to view and change orders, as well as greater access to medication information of a given patient.

[50] Health PEI's failure to implement a technical safeguard put additional personal health information at risk. It is much more difficult to snoop on the CIS if the snooper does not have technical access. Similarly, the more limited the snooper's access is, the less personal health information will be available to them. Health PEI had an opportunity, in 2014, to limit the Employee's access to personal health information, by changing their position code in the CIS to PCW, rather than LPN. Health PEI missed their opportunity to minimize this breach. For these reasons, I find that Health PEI failed to implement an information practice which they had established, in contravention of section 39 of the *HIA*.

Breach Detection

[51] As noted above, Health PEI has reasonable policies and procedures in place to prevent privacy breaches of this nature. The policies and procedures are meant to prevent privacy breaches; a secondary goal, if a breach occurs despite these measures, is to minimize any breach which may arise. This goal is accomplished by limiting the amount of personal health information available to a user of the CIS, consistent with their needs. A third goal, which is vitally important, is detecting a breach once it has occurred. A question arises as to whether Health PEI has reasonable information practices in place to detect such breaches, once they have occurred.

[52] In this case, once the breach was discovered, the Employee did not immediately offer an explanation for their snooping. However, other snoopers, in other jurisdictions, often state that they snooped because they were bored, or simply curious. To the victims of a privacy breach, such reasons provide no comfort. The Employee was entrusted with access to personal health information, and the Employee abused that trust. Health PEI understands that such actions are not acceptable, which is why it expends such effort implementing the preventative information practices described above.

[53] A person who is intent on snooping can also be difficult to detect. In a perfect world, all users of electronic databases would follow the information practices which protect the personal health information accessible by them. However, Health PEI realizes that snooping may occur despite its best efforts, which is one of the reasons that Health PEI has an auditing process. Access to the CIS must be monitored to detect possible breaches.

[54] With all of the safeguards Health PEI has in place, an affected party asked how these breaches were not detected earlier. Health PEI states that the primary reason that the Employee's unauthorized access went undetected over a period of more than three years was that no triggers occurred to bring unauthorized accesses to the attention of Health PEI management. The Employee was never selected for a random audit. Other auditing activities completed during this time, including system clean-up projects to terminate any users with no activity, and reviews/updates to user role definitions, had not flagged the Employee's access as unusual. Although the Employee's Nurse Manager recalled observing the Employee using a computer in the workplace, this on its own would not be unexpected as the Employee had network access, as all staff do, for the purpose of accessing email, intranet sites (for communication purposes), and shared drives. The Nurse Manager assumed that the Employee's use was for the purposes of playing games or personal use, and had

directed the Employee to stop.

[55] The facts are that the Employee did access the personal health information of 353 patients over a three year period, and inputted information into the CIS in 835 instances, but was never detected. This is not a criticism of the Nurse Manager, who was astute enough to recognize the name of the Employee when reviewing a patient audit, which ultimately led to the discovery of 353 incidents of snooping.

[56] The circumstances of this breach are unusual in that the Employee has snooped into the personal health information of many patients. Snooping itself, however, is not a unique event. Since July 1, 2017, this office has received 5 breach notifications relating to cases of snooping, 3 of which were from Health PEI. I find that Health PEI's use of regular random auditing is a positive and proactive step in breach detection. However, its random auditing was unable to detect this breach for three years. It is incumbent on Health PEI, in these circumstances, to carefully analyze its auditing processes; Health PEI plans to take steps in this regard, which is discussed in the analysis of Issue Three, below, under remediation. It is also advisable that management training processes include tools to detect snooping.

Conclusions relating to Issue Two

[57] With regard to breach prevention, I find that Health PEI has reasonable information practices established to prevent this breach. However, Health PEI failed to implement one of their information practices. In particular, Health PEI failed to limit the Employee's access to the CIS, by changing their credentials to that of a PCW, in contravention of section 39 of the *HIA*.

[58] With regard to breach detection, I find that Health PEI has not yet established reasonable information practices to detect accesses to personal health information by unauthorized individuals. While Health PEI conducts regular random audits, these audits alone were not able to detect snooping which occurred over a period of

more than three years, for 353 patients, by an employee who was not entitled to access the CIS for their job duties. My recommendations to Health PEI will be discussed below, under Issue Three, remediation.

Issue Three: Did Health PEI respond reasonably to the 353 accesses to personal health information by an unauthorized person?

[59] When assessing Health PEI's response to this privacy breach, I will consider the following, outlined in *Privacy Breach Reporting Guidelines* (available at www.oipc.pe.ca):

- Breach Notification;
- Breach Containment;
- Breach Investigation; and
- Remediation.

Breach notification

[60] Custodians are required to notify the individual to whom the personal health information relates, and the Commissioner, at the first reasonable opportunity following an access to personal health information by an unauthorized person. This requirement is set out at clause 36(1)(c) of the *HIA*.

[61] The accesses to personal health information of 353 individuals occurred over more than a three year period, most of which occurred before the *HIA* was proclaimed on July 1, 2017. Although those unauthorized accesses to personal health information would have been considered an unauthorized use of personal information under the *Freedom of Information and Protection of Privacy Act*, there is no requirement to notify regarding breaches which occurred prior to July 1, 2017. Health PEI exceeded the requirements of the *HIA* by taking the initiative to notify all living affected parties, whether the breach occurred before or after July 1, 2017.

Timing of Notifications

[62] Ninety-five individuals whose personal health information was accessed by the Employee, were deceased by the date of the discovery of the breach. Health PEI did not notify the estate or family of deceased patients whose personal health information was accessed by the Employee without authorization. Once addresses were validated, 252 letters of notification were sent by Health PEI ten days following its confirmation that the personal health information had been compromised. Health PEI also notified this Office of the breach.

[63] Health PEI gave careful consideration to whether to notify family members of deceased individuals. At the time of Health PEI's decision, section 36 of the *HIA* required notification to individuals affected by a breach unless it is reasonable to believe that the breach will not (a) have an adverse impact on provision of care to the individual, (b) have an adverse impact on the health, economic or social well-being of the individual, or (c) lead to the identification of the individual. In weighing these criteria for notification, Health PEI concluded that the breach could not impact the provision of care, under clause 36(2) of the *HIA*, where the affected individual is now deceased. Additionally, no evidence was found to indicate that the personal health information accessed in this breach was used or disclosed for any purpose; therefore, there was no reason to believe that there would be adverse impact to the well-being of the deceased individuals, under clause 36(2)(b) of the *HIA*.

[64] Health PEI identified two options for notification that could be pursued where the affected individuals were deceased, either sending letters to "The Estate of…" or notifying the individual's next of kin. As a custodian, Health PEI must continue to protect the privacy of deceased individuals. The risks of the first option include the address on file being no longer valid for the estate and the letter being opened by an unauthorized person, further breaching the affected individual's privacy. The risks

of the second option include the accuracy of the next of kin information on file (as provided by the individual at their last encounter with acute care) and breaching of the affected individual's privacy by contacting the next of kin to confirm they are the correct party to receive the notice and obtain address. Health PEI sought advice from this Office. There is no clear guidance available in the *HIA*. I recommended that Health PEI reach a decision based on the objectives of eliminating further risk to the privacy of the personal health information of the deceased, and ensuring sensitivity to the loved ones of the deceased.

[65] As a result of their assessment, Health PEI decided not to send notifications of privacy breach to deceased individuals. Health PEI decided that the issue would be revisited if any evidence of use or disclosure of the breached information were discovered indicating that there may be an adverse impact to the well-being of the deceased.

[66] Based on the practical limitations of identifying the appropriate individual and address, and resulting risk to privacy based on unreliable delivery information, I find Health PEI's decision not to send notifications to representatives of those affected individuals whom their records show to be deceased, is reasonable. Subsection 36(2) of the *HIA* has since been amended. These amendments were not applicable at the time Health PEI made its decision; however, I find that Health PEI's decision would nonetheless be reasonable under the amended subsection 36(2) of the *HIA*.

[67] With regard to timing, Health PEI was required to prepare individualized letters for 252 patients, indicating the number of unauthorized accesses, and the date on which the last access occurred. They also set up a toll free hotline during this time, and notified the media of the breaches. In the circumstances, I find that the timing of the notifications, ten days following discovery of the breaches, is reasonable.

Content of Notifications

[68] A letter from the Acting CEO of Health PEI was mailed out to 252 affected individuals to advise them of the breach, offer an apology, provide information based on their preliminary investigation, and outline the next steps they would take in managing the breach.

[69] The notification letters sent to the individuals whose personal health information had been accessed by the Employee, included the following information:

- The number of times the patient's personal health information was accessed by the Employee, and the date of the most recent access;
- The type of personal health information which was accessed by the Employee;
- That the access to their personal health information by the Employee was in violation of Health PEI policy;
- That the Information and Privacy Commissioner had been notified; and
- A toll-free phone number to contact Health PEI with any questions or concerns.

[70] Health PEI received 32 messages on their toll-free line. All messages were returned. The most common question received from affected individuals was to know the name of the employee responsible for the breach. After careful consideration, Health PEI determined that the best approach to responding to this question would be to follow an established process to provide, upon request, an audit report showing the names and positions of all staff who have accessed an individuals' electronic patient chart. All fourteen affected individuals who asked for the identity of the Employee, were provided with an audit report covering the time period of April 1, 2014 to October 2017 with the access(es) subject of this breach investigation highlighted.

[71] In comments made to this Office, some affected individuals asked the dates the breaches occurred. While the letter from Health PEI did state how many times the individual's personal health information was accessed, it only stated the date of the most recent access. Some affected individuals also asked the name of the Employee who accessed their personal health information. This information was not contained in the notification letter but, as noted above, is contained in the electronic log required to be maintained by Health PEI, which was requested by 14 individuals who contacted Health PEI.

[72] Subsection 34(2) of the *HIA* requires custodians to maintain an electronic log of all accesses to personal health information in an electronic database such as the CIS. The electronic log must record the unique user i.d. of the individual accessing the personal health information, the date and time of access, and a description of the personal health information accessed or that could have been accessed. The person to whom the personal health information relates, is entitled to access to this electronic log, as it is their personal health information. In most circumstances individuals who interact with a health care provider should know who is accessing their personal health information. In the case of a snooper, citizens have a heightened need to know the identity of the snooper, for various reasons, but primarily to identify whether the snooper is someone with malicious intentions. Such access to the individual's own electronic log may be refused by a custodian if any of the circumstances listed at section 10 of the *HIA* apply. I have reviewed section 10, and none of these exceptions apply to the circumstances of this breach.

[73] While Health PEI offered an electronic log to those affected individuals who sought the name of the Employee and/or the dates of each unauthorized access to their personal health information, they did not offer to provide the electronic log, nor did they mention the electronic log, in their 252 notification letters. As this was the first case of multiple incident snooping that Health PEI has dealt with, and it was only

months after the proclamation of the *HIA*, they may not have been prepared for the question that most victims of snooping have at the top of their minds; who snooped, and how often. I recommend that, in future, Health PEI reference the electronic log in their notification letter, and enclose a copy of an excerpt from the electronic log which applies to the affected individual, highlighting the access(es) which reflect the breach, including the date(s) and the name of the snooper.

[74] In these circumstances, I find that Health PEI notified the patients, and this Office, of these privacy breaches at the first reasonable opportunity. I do, however, recommend the above-noted change to the content of the notification letter, where the breach involves snooping.

Notification letters not received

[75] Three affected individuals advised our Office that they did not receive their letters of notification, which were sent by Health PEI to all affected parties in October 2017. It was, therefore, surprising to them when they received a summary of the facts of this investigation, from this Office. This Office asked Health PEI to address this issue.

[76] Health PEI advises that, for the purpose of notifying affected individuals, mailing addresses recorded in the CIS were used. The specific addresses used reflected the address that each affected individual would have been asked to validate at their most recent admission to hospital or visit to an Emergency Department. A label reading "CONFIDENTIAL: If undeliverable, DO NOT OPEN and return to sender" was affixed to each envelope and a total of 14 letters were returned to Health PEI as undeliverable.

[77] Section 75 of the *HIA* permits mailing notices to an individual's last known address. Nonetheless, Health PEI investigated each of the undelivered notifications. They confirm that all three were included in their mailing list and none of the three

letters were returned to them as undeliverable. Further, they point out that, since this Office used the mailing list provided by Health PEI, this serves to validate that the addresses used for these individuals were correct. Health PEI submits that no available source of mailing address information could have guaranteed 100% accuracy when sending correspondence to over 250 individuals, as people do not always update their addresses with Health PEI programs and services when they move.

[78] Health PEI expressed concern that these three notifications had not reached their intended recipients, and further, that they were not returned to Health PEI. They provided a copy of each of the three notifications to this office, signed. Given that 252 letters were sent to affected individuals, I find that Health PEI made their best efforts to notify the affected individuals, and took a reasonable approach in sending these notifications by the mailing methods which they describe.

Breach Containment

[79] Containing a privacy breach means ensuring that the personal health information is not subject to further risk of unauthorized access, use or disclosure, requiring quick action by a custodian.

[80] Upon the Nurse Manager's discovery of this breach on October 11, 2017, Health PEI ensured that the Employee did not have further access to any personal health information while its investigation was ongoing. As the Employee worked on a casual basis, no further shifts were offered to them. The following day, on October 12, 2017, Health PEI met with the Employee to describe their findings. At that meeting, the Employee admitted to accessing patient charts on the CIS without authorization. As the employment relationship between the Employee and Health PEI then ended, the Employee had no further access to the CIS.

[81] As noted above, some affected individuals asked how they can be certain that their personal health information was not disclosed to others. Health PEI also investigated whether personal health information had been disclosed to anyone by the Employee. In two separate interviews with Health PEI, the Employee expressed great remorse, and stated that they had not disclosed any personal health information. Health PEI notified police services, who also interviewed the Employee. Health PEI has received no complaints relating to disclosure of any of the personal health information at issue. Their audit determined that the Employee had not printed any information from the CIS. Further, following discovery of the breach, the Employee signed an undertaking stating that the Employee had not disclosed the personal health information to anyone, and agreeing that the Employee will not disclose any in future. Health PEI has found no evidence, and has been provided with no evidence, that any of the personal health information of the affected parties was disclosed.

[82] I find Health PEI's conclusions regarding disclosure to be reasonable in these circumstances. While we cannot conclude with 100 percent certainty that none of the personal health information accessed by the Employee was disclosed, no evidence of disclosure has been found. Given the reasons the Employee likely had for accessing the personal health information, described below, disclosure was not likely the Employee's intention.

[83] As Health PEI took action to prevent further unauthorized access, use or disclosure of personal health information, I find that Health PEI took reasonable steps to contain the breach.

Breach Investigation

[84] Custodians should conduct internal investigations, to determine the root cause(s) of a breach. Without such investigations, it is not possible to prevent future similar

breaches.

[85] Once the breach was discovered, Health PEI conducted a thorough audit, covering a period of more than three years, to determine all accesses to the CIS by the Employee. This initial audit disclosed unauthorized access to 353 patient charts. Health PEI conducted further audits to assess whether the Employee had added, changed, or printed any personal health information. An additional audit report found that the Employee made 835 chart modifications to the charts of 105 individuals over more than three years. Health PEI also reviewed a random sample of 31 individuals affected by the breach, to determine whether they had a constant care assignment. This paper-based audit determined that 9 of the sample had a constant care assignment which matched the dates of access to the CIS by the Employee, but that 22 had no record of a constant care assignment.

[86] As noted above, some affected individuals asked for what purpose the Employee breached their personal health information. This is an understandable question, as the reasons for snooping may indicate a malicious intent. As part of their investigation, Health PEI attempted to determine the Employee's reasons. Health PEI interviewed the Employee twice. Although the Employee admitted to the unauthorized accesses, they did not provide much information regarding their reasons for snooping. However, Health PEI drew some conclusions based on the evidence.

[87] The investigation confirmed that some of the accesses to electronic patient charts by the Employee were related to constant care assignments. It appears as though the Employee was conducting themselves as an LPN, although that was no longer their role. This is consistent with a statement made by the Employee to the Nurse Manager that the Employee wanted to do charting (the Nurse Manager reminded the Employee that their position did not require electronic charting). The modifications made to the charts of some of the affected individuals show no

evidence of malicious altering of information, but rather reflect that the Employee most likely continued the charting practices that they had established in their previous role as an LPN. The modifications are limited to documenting patients' personal health information; however, as this documentation on the electronic chart was in violation of QEH policy related to constant care, it is still an unauthorized access by the Employee.

[88] In a random sample audit of 31 accesses, Health PEI found no evidence of a constant care assignment for 71% of the patients. This supports a conclusion that there were other reasons for the Employee's unauthorized access. Health PEI explains as follows:

> Although no definitive reason for the access was given by the Employee, some of the information uncovered in the investigation suggests possible motivations. The patterns of access found on some dates, where the Employee accessed multiple patient charts within a very short time frame at a time of day when [their] shift would have been starting, could suggest that the Employee may have been reviewing patients on the constant care assignment list to identify if any individual would be a more preferable assignment than others. The inclusion of physicians and staff of the QEH in the list of affected individuals may suggest that the Employee was accessing the charts of colleagues out of curiosity.

[89] The evidence supports the conclusion that the Employee had various reasons for accessing the personal health information in the CIS, without authorization: to continue performing LPN tasks, to choose the more preferable patients to provide constant care, and out of simple curiosity. An additional reason that was offered by the Employee was to look up room numbers of people who were in hospital. I find that Health PEI's conclusions, relating to the possible reasons for the Employee snooping, are reasonable based on the evidence. I also agree with Health PEI that none of these reasons are the basis of authorized use of personal health information.

[90] In addition to Health PEI's extensive initial investigation, it further investigated in response to queries from this Office, and in response to the concerns raised by affected individuals. Based on all of the circumstances, I find that Health PEI adequately investigated the unauthorized access to personal health information by the Employee.

Remediation

[91] Good information practices are the key to successful remediation of a privacy breach. Remediation involves finding solutions to reduce the risk of a similar breach occurring in future. Remediation may involve, for example, a technical solution, staff training and education, or a change in administrative practices.

Training and Education

[92] Health PEI advises that, immediately following the discovery of this breach, it circulated a memo to inform all staff of the incident. The memo included reminders of privacy and confidentiality expectations and encouraged all staff to review applicable policies and the pledge of confidentiality they signed at the time of hire.

[93] New employee orientation at Health PEI includes a review of privacy and confidentiality expectations. The CIS was implemented in 2008 and all staff received training on the system as part of go-live preparations. This initial training and all training sessions since implementation focus heavily on privacy, including a review of acceptable use of personal health information in the CIS and informing staff of the auditing program. Health PEI advises that they recently conducted a system-wide initiative to educate staff on the *HIA* and to provide refresher privacy training. A staff education toolkit was developed and made available to managers and supervisors for the purpose of educating their teams. A key message common to the privacy training is that the use of personal health information must be limited to

accessing only the information that is required for the purposes of an employee's job duties.

[94] Health PEI advises that Human Resources will conduct an education campaign targeted at all managers across Health PEI. The key messages will include information on the process in place to change or terminate system access, manager responsibilities when staff change roles or positions, and a reminder on how to request CIS audits if unauthorized access is suspected. Some of the communication activities planned as part of this campaign include a presentation at the next full leadership meeting and the distribution of a memo to all managers. Human Resources will also explore options for moving to an electronic process for HR forms, with a checkbox and/or automated link to relevant ITSS forms. They will also explore the creation of a position change report. The report would list all staff terminations and position changes for a unit or program area over a designated time period and would be sent to the manager for validation that any required system access changes have been requested. I find that these described plans are reasonable steps to remediate the error in failing to change the Employee's CIS access credentials from those of an LPN, to those of a PCW. In my view, all of these plans will help to prevent, and sometimes detect, future breaches.

[95] Health PEI did not identify any necessary policy changes as a result of the investigation. However, increased awareness of policies pertaining to privacy, ITSS and CIS will be one of the areas of focus for education and communication to staff, described immediately below.

[96] Health PEI plans to conduct an education campaign to all staff to share lessons learned through the investigation and provide reminders on privacy policy and expectations. The primary communication activity will be a memo to all staff from the Interim CEO. Additionally, Human Resources will explore options for better

integrating a review of policies by staff into the annual performance appraisal process.

[97] In a recent breach report, HI-18-001, *Prince Edward Island (Health) (Re)*, 2018 CanLII 83554 (PE IPC), I observed that there may be a temptation to use the CIS for personal use. I recommended that Health PEI remind all users of the CIS that electronic medical records are not to be accessed for purposes not related to the duties of their employment. Health PEI followed this recommendation, and has focused further on training and education, all with a view to prevent breaches such as this. It is imperative that all employees of Health PEI not only know this, but apply it to their daily work lives. The privacy of personal health information is of utmost importance. Individuals expect that they, and their loved ones, will enjoy the most responsible protection of their personal health information that custodians can offer.

[98] The *HIA* has been in force since July 1, 2017. With this law comes new obligations of health custodians, and potential consequences for activities such as snooping. In these circumstances, Health PEI has taken the initiative to retrain, reeducate, and refamiliarize staff with the limits to their access to patient personal health information. I consider such training to be a reasonable step of remediation relating to this breach, as it is likely to considerably help to reduce the risk of snooping in future. I find that Health PEI's training and education efforts to be robust.

Auditing

[99] Health PEI advises that no new technical safeguards or changes to existing technical safeguards were identified as a result of the investigation. However, with regard to administrative safeguards, Health PEI advises that they will increase the frequency of user account maintenance audits to quarterly and will reduce the period of user inactivity that results in de-activation of an account to 6 months. These are positive steps of remediation. The CIS team and Human Resources will also explore the

creation of a user role audit report. This report would list all staff working within a unit or program area with their CIS user role identified and would be sent to the manager for validation.

[100] Health PEI also states that, as of October 2018, the CIS team is testing new auditing functionality that is expected to provide a greater level of detail regarding sections of a patient's chart that are accessed by users. If this testing is successful, the detailed audits will be available on a go forward basis as an audit investigation tool. I encourage Health PEI to follow through with these auditing improvements. As noted above, management has also received refresher training regarding how to request CIS audits if unauthorized access is suspected.

[101] Not only did the Employee access the personal health information of 353 patients, and inputted information into the CIS in 835 instances, but the Employee was not detected until more than three years had passed. Snooping is a risk of electronic health databases, and there must be effective auditing mechanisms in place to detect snooping. I appreciate that Health PEI plans to take steps to improve their auditing capabilities, and I encourage Health PEI to move forward with these plans. However, I have further recommendations below.

Prevention targeted at the Employee

[102] Some affected individuals asked whether this type of privacy breach is included in an employee's personnel records or references. As the Employee is no longer employed with Health PEI, there was no opportunity to take disciplinary, performance management or re-education actions. However, all hiring for Health PEI is completed by the Public Service Commission. Health PEI has notified the Public Service Commission of this breach and identified the Employee to them, for the purpose of flagging concerns if the Employee were to apply for future employment.

Risk of Identity Theft

[103] Health PEI assessed the level of risk for identity theft if the personal health information accessed by the Employee were to be disclosed. Firstly, there is no evidence to suggest that the personal health information was disclosed to anyone, and the Employee signed an undertaking confirming this. Information typically targeted for the purposes of identity theft and fraud, for example financial and banking information and social insurance numbers, is not recorded in the CIS. Personal health numbers are not, in this province, considered to be a piece of foundation identification that could be accepted as proof of identity and, therefore, used for the purposes of identity theft. For these reasons, Health PEI found the risk of identity theft resulting from this breach to be low to nil and concluded that it was not necessary to advise affected individuals to take any preventative measures. I find this conclusion to be reasonable.

[104] In responding to this privacy breach, Health PEI has shown an understanding of the consequences of snooping into patients' electronic health records. Further, the actions of Health PEI to remediate this breach have been thoughtful, and their efforts at training and education are reasonable. However, in consideration of all the circumstances, I recommend that Health PEI conduct a careful analysis of its auditing processes with a view to improved detection of unauthorized access. I further recommend that Health PEI take steps to ensure that management is adequately trained in how to detect snooping activity of employees.

IV. SUMMARY OF FINDINGS

Issue One: Was personal health information compromised in a manner described at clause 36(1)(c) of the *Health Information Act*?

[105] I find that the Employee accessed the personal health information of 353 individuals, without authorization. Because the Employee did not need to access the personal

health information of these individuals for their duties of employment, I find that these are accesses to personal health information by an unauthorized person, under clause 36(1)(c)(iv) of the *HIA*.

Issue Two: Did Health PEI establish and implement reasonable information practices to protect personal health information from access by an unauthorized person?

[106] I find that Health PEI has established reasonable information practices for the prevention of accesses to personal health information by unauthorized individuals. Health PEI's policies and practices, when taken together, and if implemented consistently, contribute to a strong and well-woven safety net for breach prevention. However, by failing to change the Employee's CIS access status to that of a PCW, from that of an LPN, Health PEI failed to implement an information practice which they had established, in contravention of section 39 of the *HIA*.

[107] I find that Health PEI has not yet established reasonable information practices to detect accesses to personal health information by unauthorized individuals, which have already occurred. While Health PEI conducts regular random audits, these audits alone were not able to detect snooping which occurred over a period of more than three years, for 353 patients, by an employee who was not entitled to any access to the CIS for their job duties. I encourage Health PEI to carry through with proposed changes to their auditing program, as part of my recommendations set out below.

Issue Three: Did Health PEI respond reasonably?

[108] I find Health PEI's decision not to send notifications to representatives of those affected individuals whom their records show to be deceased, is reasonable. I further find that Health PEI notified the individuals to whom the personal health information relates, and the Commissioner, at the first reasonable opportunity

following discovery of the breaches, and that their notification by mail was reasonable.

[109] I find that Health PEI took reasonable steps to contain this breach. I further find that Health PEI's conclusion that the personal health information was not disclosed by the Employee, is reasonable in these circumstances. While it cannot be concluded with 100 percent certainty that none of the personal health information accessed by the Employee was disclosed, no evidence of disclosure has been found.

[110] I find that Health PEI adequately investigated the accesses to personal health information by an unauthorized person. I also find that Health PEI's conclusion that the risk of identity theft resulting from this breach is low to nil, and it was not necessary to advise affected individuals to take any preventative measures, is reasonable in the circumstances.

[111] I find that Health PEI has taken reasonable measures to remediate the unauthorized access of personal health information by the Employee, by implementing appropriate training and education. However, given that random audits have not detected incidents of snooping, I find that remediation, as it relates to auditing and management training in snooping detection, is not adequate. Therefore, I have made recommendations for further remediation below.

V. RECOMMENDATIONS

[112] Snooping into the electronic health records of patients violates the *HIA*, and is unacceptable to even the most basic ideals of privacy. This breach, and others recently investigated by Health PEI, indicate that snooping is not a one-time event in the health care system. While Health PEI conducts regular audits of the CIS, there is room for improvement in their auditing process, for better detection of snooping. In

addition, victims of snooping are entitled to proactive disclosure of their electronic log. Further, as automatic logout periods on an electronic database are crucial to the security of personal health information, this is a practice that is deserving of review. As a result of the foregoing, I make the following recommendations:

a. I RECOMMEND that Health PEI carry forward with changes proposed to its auditing program, and further analyze its current CIS auditing process with a view to establishing and implementing improvements in methods for the detection of snooping.
b. I RECOMMEND that Health PEI ensure that management is adequately trained in how to detect snooping activity in the CIS.
c. I RECOMMEND that, in the event of future CIS snooping breaches, Health PEI reference the log of accesses to the electronic database in their notification letter, and enclose a copy of an excerpt of the electronic log which applies to the affected individual, highlighting the accesses which reflect the breach, including the date(s) and the name of the snooper.
d. I RECOMMEND that Health PEI review their automatic logout standards for the CIS, with a view to what is appropriate for the level of sensitivity of the personal health information to be protected, in accordance with subsection 39(2) of the *HIA*.

[113] I thank Health PEI for carrying out its responsibilities in a forthright manner, and I appreciate its cooperation throughout this investigation.

_____

Karen A. Rose
Information and Privacy Commissioner