



**OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
for
Prince Edward Island**

Breach Report HI-19-002

Custodian: Health PEI

**Prince Edward Island Information and Privacy Commissioner
Karen A. Rose**

May 30, 2019

Summary: After obtaining an electronic log of accesses to their personal health information, an individual noticed that a named employee had accessed their personal health information multiple times on the Clinical Information System database. The affected individual reported this discovery to Health PEI, who investigated.

The Commissioner agreed with Health PEI's conclusion that there were unauthorized accesses of personal health information of the affected individual by the employee.

Breach response

The Commissioner found that Health PEI responded reasonably once the breach was discovered, including timely and appropriate notification to the affected individual and to the Commissioner, reasonable steps to contain the breach, and a thorough investigation.

The affected individual wished to know what discipline measures Health PEI had imposed on the employee as a result of the privacy breach. Health PEI refused to disclose this information.

The Commissioner found that Health PEI was not required to disclose the precise discipline. However, the Commissioner found that Health PEI is required to provide assurances that personal health information will be protected from unauthorized access. The Commissioner recommended that Health PEI introduce regular auditing of the employee's access to electronic records, with particular attention to the personal health information of the affected individual.

Statutes Considered: *Health Information Act*, SPEI 2014, cap 31, ss. 1(t), 22, 34(2), 36, 39(4)(a).

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

Breach Report HI-18-005, *Re: Health PEI*, 2018 CanLII 130517 (PE IPC)

Order HO-010, *Re: Ottawa Hospital* (ON IPC)
<https://decisions.ipc.on.ca/ipc-cipvp/hipa/en/item/135125/index.do>

I. BACKGROUND

- [1] In order to fully understand this Breach Report, it is necessary to describe the facts preceding discovery of the breach.
- [2] On March 2, 2018, Health PEI received an inquiry from an individual (“the Affected Individual”) regarding access to personal health information in their electronic patient chart in the Clinical Information System (“the CIS”). This system digitally stores personal health information of patients.
- [3] Subsection 34(2) of the *Health Information Act* (“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

identification 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 a copy of this electronic log, as it is their personal health information.

- [4] The Affected Individual had received an electronic log of all accesses to their personal health information within a specified time period, as part of the follow up to a separate, unrelated privacy breach. Upon review of the log report, the Affected Individual noticed that an employee who is known to the Affected Individual (“the Employee”) had accessed the Affected Individual’s chart numerous times, including dates when the Affected Individual was not admitted to hospital.
- [5] On April 30, 2018, the Affected Individual again contacted Health PEI to inquire about access to their personal health information noted in the electronic log by another employee (“the Second Employee”), whom the Affected Individual believed did not work at the Queen Elizabeth Hospital (“the QEH”) where they had been a patient, but rather at another health care facility.
- [6] The Affected Individual did not remember seeing either the Employee or the Second Employee at the Affected Individual’s bedside or receiving care directly from them.

Custodian’s Investigation of the Employee

- [7] At the time of receipt of the inquiry, the Employee was on a leave of absence from their position and did not have access to personal health information. For this reason, Health PEI determined it was not necessary to take any additional action to contain the alleged breach during their investigation into the matter.

- [8] The Information and Privacy Commissioner (“the Commissioner”) received notification of the breach from Health PEI on June 11, 2018. Health PEI states that the time between receipt of the Affected Individual’s inquiry and submission of the notification to the Office of the Information and Privacy Commissioner reflected the time required for Health PEI to investigate the accesses to personal health information, to determine if unauthorized access had occurred.
- [9] Health PEI conducted additional auditing as part of its investigation. These audits confirmed that no additional access by the Employee to the Affected Individual’s patient chart occurred outside of the time frame covered by the electronic log previously provided to the Affected Individual. It was also confirmed that the Employee at no time modified personal health information in the Affected Individual’s electronic chart.
- [10] The Employee works at the QEH. The Employee’s responsibilities include providing advice and consultation to health care professionals, as well as assessing patients directly at the bedside and/or through reviewing information in their electronic patient charts, such as lab test results. The role also involves surveillance and outcome reporting, which can require the Employee to access follow up information from patient charts post-discharge.
- [11] The Affected Individual noted that some of the accesses by the Employee occurred after the Complainant had been discharged from hospital. The Employee’s Manager advises that this is not necessarily outside of the scope of the Employee’s job duties. In some cases, employees who work in this service would be required to access patient charts post-discharge for follow up or for quality assurance purposes. Also, it is not unusual for employees in this service to complete their work “behind the scenes” and for them not to have any direct contact with the patients. The service they provide is consultative in nature and duties include assessment and recommendation based on information in the patient’s chart.

[12] The Employee's Manager conducted a chart review. Based on the results of the audits and chart review, the Manager determined that some, but not all, of the accesses to the Affected Individual's chart were consistent with the performance of the Employee's job duties. The Manager's chart review may be described as follows:

- For the investigation, the Manager compared the chart access dates to other information in the patient's chart, to confirm or rule out reasons for accessing the patient's chart.
- There were times when the patient's chart was accessed, which were likely when the Employee was checking to determine if results had been posted to the electronic health record.
- There were 16 times the Employee accessed the chart where the Manager could not link the access to work-related duties. Out of those 16 accesses, there were 10 which occurred when the patient was not admitted to the QEH. The accesses at times occurred closely together (i.e. 1202 hrs, 1333 hrs and 1347 hrs on the same day). The Manager could not determine if the Employee was doing work related tasks or if they could have completed their tasks within one access instead of three.
- For the times the chart was accessed and the patient was not admitted, the Manager could not identify any reason why the Employee would have accessed the patient's chart.

[13] Health PEI held a meeting with the Employee on May 18, 2018 to review the allegation and the results of the audits and chart review. The Employee stated that all of their access to the Affected Individual's personal health information was for professional reasons. They indicated that there is a long history of a volatile

relationship between the Employee and the Affected Individual and the Employee was concerned that the privacy complaint was made with malicious intent.

[14] Health PEI concluded that the Employee had accessed the Affected Individual's personal health information without authorization. Health PEI concluded that, at a minimum, some of the accesses to the Affected Individual's personal health information by the Employee were not authorized. This conclusion was based on the findings of the Manager's chart review where they could find no evidence of a need to access the information for the purposes of the Employee's duties in several instances. Additionally, the Employee was given the opportunity to respond to the findings of the Manager's audit and, although the Employee maintained that all accesses to the Affected Individual's chart were for professional reasons, the Employee could not provide any additional detail to substantiate that claim in regards to the unexplained accesses identified in the Manager's chart review.

[15] Health PEI concluded that there was unauthorized access by the Employee to the Affected Individual's personal health information. Health PEI established a performance management plan for the Employee. This plan includes disciplinary measures, not including termination, according to Health PEI policies. There are currently no plans to restrict access to the CIS by the Employee based on this breach, as such restrictions would impact the Employee's ability to complete the duties of their employment. The Employee's access to the CIS will be subject to the routine auditing planned for Program staff.

[16] Additional measures are underway to improve privacy awareness and compliance with policy within the service in which the Employee is employed. The staff in this service have recently been brought together as a provincial team with a single Manager. Prior to this change, staff reported individually to the hospitals in which they were assigned to work. The Manager plans to conduct privacy refresher

training and implement random auditing of access to the CIS from where the electronic charts are accessed.

[17] A meeting was held with the Affected Individual, and a relative, on May 31, 2018. At this meeting, the Manager provided information on the job duties of employees of their service and the findings of the investigation were shared with the Affected Individual. The Affected Individual was informed of the measures planned for the service to improve privacy awareness and compliance and advised that a performance management plan, which included disciplinary measures, had been established for the Employee.

[18] On July 18, 2018, Health PEI sent a letter to the Affected Individual outlining all their findings, and offering an apology for the unauthorized access.

Custodian's Investigation of the Second Employee

[19] The Affected Individual's second inquiry was related to access to the Affected Individual's personal health information in December, 2014 by the Second Employee, whom the Affected Individual did not believe worked at the QEH. It was determined that the Second Employee had accessed the Affected Individual's chart six times over the course of three dates.

[20] Upon investigation, Health PEI found that the Second Employee's home position at the time in question was indeed at another health care facility. However, payroll records indicate that the Second Employee picked up additional shifts at the QEH on the dates of access to the Affected Individual's personal health information. Payroll records confirm that all accesses to the Affected Individual's chart occurred during the hours that the Second Employee was working at the QEH and not during shifts at the Second Employee's home position/facility.

[21] Health PEI also confirmed through an audit that the Second Employee did not modify any information in the Affected Individual's chart.

[22] Health PEI concluded that the Second Employee was authorized to access the Affected Individual's personal health information. Therefore, no remedial action was taken with respect to the Second Employee.

Input from the Affected Individual

[23] The Commissioner provided an Investigation Summary to the Affected Individual, setting out the facts described above, and inviting them to contact the Commissioner with representations, questions, or concerns they may have.

[24] The Commissioner received a response from the Affected Individual, who disagreed with the Employee's statement that the Affected Individual had any malicious intent. The Affected Individual advised that they would be concerned no matter who had accessed their personal health information without authorization. The Affected Individual also requested that they be advised of the specifics of the discipline measures which were imposed upon the Employee.

[25] The Commissioner requested that Health PEI respond to the Affected Individual's concerns. Health PEI gave detailed submissions on this issue. The Affected Individual was provided with an opportunity to respond.

II. ISSUES UNDER REVIEW

[26] 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*?

[27] On June 11, 2018, 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.

[28] Health PEI concluded that the Employee accessed the Affected Individual’s personal health information without authorization. This conclusion was based on the findings of audits and a chart review. In addition, the Employee could not provide an explanation for the questionable accesses identified in the Manager's chart review.

[29] 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 by the Employee on the CIS, satisfies the definition of personal health information at subsection 1(t) of the *HIA*.

[30] Health PEI does not permit employees 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 individual 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.

...

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.

[31] Subsection 22(5) lists circumstances that are authorized uses of personal health information, including clause 22(5)(a), using it for the purpose it was created. Health PEI's investigation determined that the Employee's job duties required them to access the chart of the Affected Individual. However, Health PEI concluded that some of the accesses were not necessary for the Employee's job. Because the Employee did not need to access the personal health information of the Affected Individual on each occasion, for duties of employment, I find that there were accesses to personal health information by an unauthorized person, the Employee, pursuant to clause 36(1)(c)(iv) of the *HIA*.

[32] Health PEI concluded that the Second Employee was authorized to access the Affected Individual's personal health information. This conclusion was based on Health PEI's confirmation that the Second Employee had worked at the QEH on the three dates that the chart had been accessed, contrary to the initial belief of the Affected Individual. I find Health PEI's conclusion relating to the Second Employee, to be reasonable. The pattern of access was consistent with the Second Employee's duties, and the Affected Individual's health care.

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

[33] Clause 36(1)(a) of the *HIA* requires a custodian to establish and implement information practices to facilitate the implementation of, and to ensure compliance with the *HIA*.

[34] "Information practices" 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;

...

[35] Section 39 of the *HIA* requires that a custodian's information practices be reasonable. Clause 39(4)(a) requires a custodian to 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.

- [36] As I have found previously in Breach Report HI-18-005, *Re: Health PEI*, 2018 CanLII 130517 (PE IPC), Health PEI has established reasonable information practices for the prevention of accesses to personal health information in the CIS by unauthorized individuals. Health PEI has detailed policies and procedures relating to access to personal health information, which conform with their obligations under the *HIA*. These include requirements of unique usernames and passwords for each user of the CIS, and creation of an electronic record each time a patient's personal health information is accessed. Health PEI also has administrative safeguards to protect personal health information, including training, supervision and audits of staff, and limiting access to personal health information in the CIS, depending on an employee's job duties.
- [37] Health PEI also uses regular random auditing to detect privacy breaches. As noted in Breach Report HI-18-005, *supra*, Health PEI has advised that they will 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. As of October 2018, the CIS team is also testing new auditing functionality, expected to provide a greater level of detail regarding sections of a patient's chart that are accessed by users. Management has also received refresher training regarding how to request CIS audits if unauthorized access is suspected.
- [38] In addition to the above proactive steps by Health PEI, the Commissioner made further recommendations in Breach Report HI-18-005, *supra*, to which Health PEI has responded positively.

Conclusions relating to Issue Two

[39] Based on the foregoing, I find that Health PEI has established reasonable information practices to protect personal health information from access by unauthorized persons. Issue Three will focus on Health PEI's response to this particular breach, including whether additional safeguards should be implemented in these circumstances.

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

[40] 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

[41] 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*.

[42] The Commissioner received notification of the inquiry on June 11, 2018. Health PEI advises that the time between receipt of the Affected Individual's inquiry, and

notification to the Commissioner reflects the time required for Health PEI to investigate and determine if unauthorized access had occurred.

[43] The Affected Individual had reported the potential breach to Health PEI in March, 2018. Health PEI kept the Affected Individual informed of their investigation, and also reported the details of the outcome of their investigation in July, 2018.

[44] Health PEI did not detect the privacy breach when they provided the electronic log to the Affected Individual. The unauthorized accesses were among a large number of authorized accesses. Without any suspicion of unauthorized access, Health PEI had no reason to investigate at that time.

[45] Once a potential breach was brought to their attention, Health PEI prudently investigated the allegations of the Affected Individual, before they could draw conclusions regarding whether a privacy breach had occurred. Once Health PEI had enough information to make such a conclusion, they notified both the Commissioner, and the Affected Individual. In addition, Health PEI offered an apology to the Affected Individual, and advised how they would be responding to the breach.

[46] In these circumstances, I find that Health PEI notified the Affected Individual, and the Commissioner, of this privacy breach at the first reasonable opportunity.

Breach Containment

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

[48] Upon receipt of the report of this potential breach, Health PEI advises that the Employee was on a leave of absence from their position and did not have access to

personal health information. Health PEI determined it was not necessary to take additional action, as they would normally do, to limit an employee's access to personal health information during their investigation. In these circumstances, I find that Health PEI took reasonable steps to contain the breach.

Breach Investigation

- [49] Custodians should conduct internal investigations, to determine the root causes of a breach. Without such investigations, it is not possible to prevent future similar breaches.
- [50] Once the breach was confirmed, Health PEI conducted additional auditing, beyond the time frame covered by the electronic log. Their audit included whether the Employee had modified personal health information in the Affected Individual's electronic chart. A chart review was also done, upon which it was determined that some of the accesses to the Affected Individual's personal health information was consistent with the performance of the Employee's job duties.
- [51] Health PEI also met with the Employee to review the allegation, and the results of their audits. Health PEI provided the Employee with an opportunity to explain the accesses to the Affected Individual's personal health information.
- [52] Based on their investigation, Health PEI was able to determine that the Employee accessed personal health information of the Affected Individual, on several occasions, without authorization to do so. These accesses were contrary to the policies of Health PEI under which the Employee works. As a result, Health PEI subjected the Employee to discipline.
- [53] In addition to Health PEI's internal investigation, they further responded to queries from the Commissioner, and to concerns raised by the Affected Individual.

[54] Based on all of the circumstances, I find that Health PEI adequately investigated the unauthorized access to personal health information by the Employee.

Remediation

[55] 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, or a change in administrative practices.

Staff Training

[56] In Breach Report HI-18-001, *Re: Health PEI*, 2018 CanLII 83554 (PE IPC), 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, for the purpose of preventing breaches such as this.

[57] Following discovery of this breach, Health PEI advised that they would provide all staff in the Employee's area with privacy refresher training. As was discussed in Order HI-18-005, *supra*, new employee orientation includes a review of privacy and confidentiality expectations. CIS training has also focused heavily on privacy, since its introduction in 2008. A key message common to 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.

[58] I find Health PEI's training response to be a reasonable step of remediation.

Discipline of the Employee

[59] The Employee was disciplined, but not terminated. This is the extent of the

information provided by Health PEI with regard to the discipline of the Employee, to the Commissioner and to the Affected Individual. The Affected Individual would like more information.

[60] Health PEI's submissions indicate that they carefully considered the discipline measures which would ultimately be applied to the Employee. Relevant circumstances included:

- The nature of the misconduct, including the Employee's cooperation with the investigation;
- Health PEI policies;
- The applicable Collective Agreement, which has provisions addressing discipline, and for which interpretation is based on arbitral and court case law;
- The Employee's work and disciplinary history; and
- Health PEI's past practice regarding discipline in similar matters.

[61] Health PEI states as follows:

Taking into account all of this information, and its prior experience, HPEI then imposed the disciplinary penalty it felt was warranted in this situation.

[62] Health PEI submits that the Commissioner's role does not include the responsibility to determine whether discipline is reasonable in any specific case. Health PEI relies upon an Ontario decision, Order HO-010 (December 31, 2010), wherein the Ontario Commissioner stated:

Under the Act, I cannot address the severity or appropriateness of the sanctions imposed against the technologist, as it is not part of the Commissioner's identified role. Rather, the issue I must address is whether the actions taken provided adequate safeguards, in accordance with section 12(1) of the Act.

[63] I agree with former Commissioner Cavoukian's statements in Order HO-010, *supra*. In this particular breach, I must determine whether Health PEI has taken reasonable steps to ensure that personal health information is secured against further unauthorized access. As Commissioner Cavoukian went on to state in Order HO-010, *supra*:

The complainant has a right to receive assurances that the incident has been appropriately addressed and that steps have been taken to prevent its re-occurrence. Critical to this assurance are details of the steps taken by the hospital, including the results of its investigation and the fact that disciplinary action was taken against the employee in question.

[64] Health PEI states that they accept that the Commissioner's role is to provide oversight of custodians' management of privacy breaches, and welcomes the Commissioner's input in this regard. Health PEI further states:

HPEI is committed to ensuring the protection of all personal information in its systems, both that of employees and members of the general public. We do not disagree that in order to carry out this mandate, the Commissioner may need to know that discipline was imposed, which was done in this case, taking into account both the Freedom of Information and Protection of Privacy Act duties and responsibilities and the necessary considerations imposed upon the Employer pursuant to the Collective Agreement in force. However, we do not agree that the specific details of the disciplinary action taken should be provided.

[65] I find Health PEI's decision to discipline the Employee, based on the considerations outlined at paragraph [60] above, to be a reasonable step of remediation.

Auditing access of the Employee

[66] The Employee accessed the personal health information of the Affected Individual without authorization. The Affected Individual is now aware that the Employee has been disciplined, but not terminated. The Affected Individual is also aware that the

Employee will continue to have access to the CIS, as this a requirement of the Employee's job duties. In these circumstances, the Affected Individual requires reasonable assurances that their personal health information will not be put at risk of unauthorized access in future. Other patients of the QEH are also entitled to such assurances, in the case of the Employee, who has proven themselves to be someone who has accessed personal health information without authorization.

[67] Health PEI advised the Affected Individual that, in the Employee's area, they would introduce random auditing of staff access to patient electronic charts. While this is a positive step, in my view, regular random auditing of program staff does not adequately address the risk of unauthorized access to personal health information by the Employee, with regard to all patients, and particularly with regard to the Affected Individual. The Employee and the Affected Individual are known to each other. Health PEI has an enhanced duty to ensure that the Employee, who has already had unauthorized access to the Affected Individual's personal health information, will not have such access again. A reasonable measure to address this risk would include regular auditing of this particular Employee's access to the CIS, with specific attention to the personal health information of the Affected Individual.

III. SUMMARY OF FINDINGS

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

[68] I find that the Employee accessed the personal health information of the Affected Individual, without authorization. Because the Employee did not need to access the personal health information of the Affected Individual 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?

[69] I find that Health PEI has established reasonable information practices for the protection of personal health information from access by unauthorized individuals.

Issue Three: Did Health PEI respond reasonably?

[70] I find that Health PEI notified the affected individual, and the Commissioner, at the first reasonable opportunity following discovery of the breach.

[71] I find that Health PEI took reasonable steps to contain the breach.

[72] I find that Health PEI adequately investigated the access to personal health information by an unauthorized person.

[73] I find that implementing staff training, and disciplining the Employee, are reasonable steps Health PEI took to remediate the unauthorized access of personal health information by the Employee. However, I find that Health PEI should also provide the Affected Individual with reasonable assurances relating to the continued security of their personal health information. Therefore, I have made a recommendation for further remediation below.

IV. RECOMMENDATION

[74] Victims of unauthorized access to personal health information require reasonable assurances that their personal health information will not be put at continued or further risk of unauthorized access. As a result of the foregoing, I recommend that Health PEI introduce regular auditing of the Employee's access to the CIS, with particular attention to the personal health information of the Affected Individual.

[75] I thank Health PEI for their cooperation, and I appreciate the input of the Affected Individual during this investigation.

Karen A. Rose
Information and Privacy Commissioner