OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
for
Prince Edward Island

Breach Report HI-19-001

Re: Dental services custodian

Prince Edward Island Information and Privacy Commissioner
Karen A. Rose

March 29, 2019

Summary: A custodian discovered that an employee had been emailing clients' personal health information to a family member contrary to the *Health Information Act*.

Information Practices
With regard to the Custodian's information practices required to ensure compliance with the *Health Information Act*, the Commissioner found that the Custodian did not maintain reasonable safeguards to prevent disclosures to an unauthorized individual.

Breach response
The Commissioner found that the Custodian acted reasonably to contain the breaches, and conducted an adequate investigation. The Commissioner further found that the Custodian's process and content of their original notification to affected individuals was not adequate. However, the Commissioner found that the Custodian's decision not to identify the employee or the family member was reasonable in the circumstances.

The Commissioner found that the Custodian has adequately remedied the shortcomings in their information practices, and in their notifications, and has taken reasonable steps to prevent similar breaches from occurring in future.

Statutes Considered: *Health Information Act*, SPEI 2014, cap 31, ss. 1(a), 1(r), 1(t), 36, and 39.

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

I. BACKGROUND

[1] This report relates to a privacy breach under the *Health Information Act* ("the *HIA*"). Before issuing this report, the Office of the Information and Privacy Commissioner (the "Commissioner") prepared an investigation summary, based on submissions of the Custodian and on their responses to questions from the Commissioner. The investigation summary consists of the following 15 paragraphs, which the Commissioner mailed to the individuals affected by the breach (the "affected individuals") in November, 2018.

INVESTIGATION SUMMARY

1. In or about December, 2017, a dental services provider under the *Health Information Act* ("the Custodian") was investigating an employee's personal use of business email. During the Custodian's investigation, they discovered that the employee of the Custodian ("the Employee") had disclosed to a family member, by email, personal health information of the Custodian's clients.

CUSTODIAN'S INITIAL RESPONSE

2. The Custodian's immediate response was to ensure the Employee had no further access to any personal health information. The Custodian terminated the Employee from their job, pursuant to the Custodian's policy, that a breach of the

responsibility to protect the confidentiality of patient information would be grounds for immediate termination.

3. The Custodian, via its agent, then notified the Office of the Information and Privacy Commissioner, by telephone and in writing, of this unauthorized disclosure of personal health information.

4. The Custodian also notified the appropriate police agency.

INVESTIGATION

5. The Custodian commenced an investigation into the nature and scope of the privacy breach. The Custodian reviewed the emails and interviewed the Employee.

6. The Custodian states that, over a period of time leading up to December 2017, the Employee forwarded email messages containing the personal health information of the Custodian's clients. The Employee forwarded the emails while at the Custodian's workplace. All emails were forwarded to the same family member ("the Recipient").

7. The amount of personal health information varied for each client. The types of personal health information disclosed in most cases included the following:

    - payment information, including patient contract information;
    - payment amounts, discounts, late payments, and information about returned payments (NSF payments); and
    - banking information related to payments. For further clarification, banking information includes financial institution, bank account numbers, account holder, credit card institution and/or credit account numbers.

8. In a smaller number of instances, the personal health information disclosed, included:

    - Case information, appointment dates and other information about appointments, including clients' address, phone number, information about family members, and/or place of employment;
    - Email correspondence with patients;
    - Internal emails which may include personal health information;
    - Clients' test results, medical or other professional opinions or treatment, medical conditions, patient signs and symptoms, and/or questions and concerns.

9. The Employee was cooperative during their interview with the Custodian. The Custodian was persuaded that the unauthorized disclosures were not for any illegal or nefarious purposes, e.g. to facilitate the commission of crimes such as theft, fraud, or harm to property, or to embarrass or harass the clients. The Employee advised the Custodian that the Employee forwarded the emails to the Recipient, throughout the work day, to confirm to the Recipient that the Employee was at work.

10. The Custodian states that it is their understanding that the Recipient had no interest in the personal health information contained in the emails. The Recipient provided their written certification that they had not further disclosed, and had securely destroyed the emails containing the personal health information. As the Employee forwarded some of the emails to the Recipient's work email, the Custodian also obtained the Recipient's employer's written certification that every email and enclosure has been securely destroyed and that no emails from the Custodian's domain name had been transmitted to anyone else from their servers.

11. Police services interviewed the Recipient, as part of their investigation. Police services confirmed that they were satisfied that the Recipient had no interest in the content of the emails from the Employee, apart from confirming the Employee's presence at the workplace. Police services assessed that there was no intent by the Recipient to further disclose the personal health information.

NOTIFICATION OF AFFECTED PARTIES

12. The Custodian considered the criteria of clause 36(1)(c) of the *Health Information Act*, relating to notification to clients. The Custodian determined that the exception to notification of the clients, set out at subsection 36(2) of the *Health Information Act*, applies to the circumstances of these unauthorized disclosures, and the Custodian determined that they are not required to notify the clients whose personal health information was subject to unauthorized disclosure. The Custodian, however, notified the Commissioner, in the interests of transparency.

13. The Custodian stated that they would provide notification to individuals if the Commissioner requires it. On May 1, 2018, the Commissioner issued a Notification Order, in consideration of the potential adverse impact on the mental, physical, economic or social well-being of the individuals to whom the personal health information relates. The Commissioner required the Custodian to notify, as soon as practicable, those clients whose personal health information was disclosed on or after July 1, 2017, by the Employee, without authorization, and to provide confirmation when notification is complete.

14. During the week of June 11, 2018, the Custodian sent written notices of this privacy breach to all individuals who were patients of the Custodian at the time the breach was discovered, a total of 1041 patients. If the patient was a minor, the notice was sent to their parent or guardian. Although some of the disclosures pre-dated July 1, 2017, the coming into force of the *Health Information Act*, the Custodian notified all patients out of an abundance of caution.

    ADDITIONAL STEPS TAKEN

15. As a result of this breach, the Custodian has undertaken further privacy compliance in-person training for its staff, and plans to repeat the training annually.

    <end of investigation summary>

[2] The Custodian provided the names and addresses of the affected individuals to the Commissioner, who mailed the investigation summary to the affected individuals. The affected individuals were invited to provide input, including any questions, concerns, or comments they may have. Fifty-one affected individuals, or their parent or guardian, responded. The Commissioner summarized the concerns of the affected individuals, and presented them to the Custodian for their response. The Custodian was also asked to address questions relating to how they responded to the privacy breach.

II. ISSUES UNDER REVIEW

[3] I agreed with the Custodian at the outset, that a breach of the *HIA* had occurred in the circumstances described above. The *HIA* defines "personal health information" as follows:

> "personal health information" means identifying information about an individual in oral or recorded form that
> ….
> (iii) relates to the provision of health care to the individual,
> ….
> (v) is collected in the course of, and is incidental to, the provision of a health care program or service or payment for a health care program or service, …

[4] I agree that the information disclosed by the Employee, satisfies the definition of personal health information at subsection 1(t) of the *HIA*. It is notable that most of the information does not relate directly to health care, but rather to payment for a health care service. However, based on the clauses cited above, such payment information also satisfies the definition.

[5] Section 23 of the *HIA* sets out limits on the disclosure of personal health information. It states in part:

> 23. Disclosure of personal health information
>
> (1) A custodian shall not disclose personal health information except as authorized under this Act or the regulations

[6] Sections 23 and 24 of the *HIA* list circumstances that are authorized disclosures of personal health information. None of these circumstances apply to the Employee's disclosure of the personal health information of the affected individuals.

[7] Because the Employee did not need to disclose the personal health information of the affected individuals for any health-related purpose, or any enumerated authorized purpose, I find that these are disclosures of personal health information to an unauthorized person, pursuant to clause 36(1)(c)(iv) of the *HIA*.

[8] The issues I will address in this review are:

> Issue one: Did the Custodian establish and implement reasonable information practices to protect personal health information from disclosure to an unauthorized person?
>
> Issue two: Did the Custodian respond reasonably to the disclosures of personal health information to an unauthorized person?

[9] When the Custodian first notified the Commissioner of the breaches, their position was that they were not required by the *HIA* to notify the affected individuals. The Commissioner considered the matter and issued a notification order, which is attached to this Breach Report as Appendix A.

Issue One: Did the Custodian establish and implement reasonable information practices to protect personal health information from disclosure to an unauthorized person?

[10] Clause 36(1)(a) of the *HIA* sets out 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;

[11] The expression "information practices" is defined at subsection 1(r) of 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;

[12] Information practices must be reasonable, and what is reasonable depends on the circumstances, including the sensitivity of the information. The specifics of information practices are not set out in the *HIA*, but section 39 includes several required

components. 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;
> . . .
> (f) ensure agents of the custodian adhere to the safeguards and controls implemented to protect personal health information.

[13] Some of the affected individuals expressed concerns about whether employees of the Custodian receive adequate training, or whether the Employee had been adequately supervised, particularly considering the large number of affected individuals and the long period of time over which the disclosures occurred. Others questioned whether the Employee's access to information was restricted. As one affected individual stated:

> My concern is that some health related businesses hire employee on short term basis for the reception desk and they are not retained or they leave after a short period. They have access to personal contacts of the clients and in some cases they have

> access to banking information. Every new employee should be trained and access to information should have several levels.

[14] The concerns of affected individuals raise issues surrounding three types of safeguards to ensure the confidentiality and security of personal health information. I will address each concern under the following headings: training, supervision, and limiting access.

Training

[15] I consider training, or some other demonstrated awareness and commitment to privacy protection, to be a reasonable administrative safeguard for the protection of personal health information. With respect to the training the Employee received, the Custodian advises that:

> At the commencement of [their] employment with [the Custodian], the Employee was provided with an office manual that included information regarding the responsibility of all employees to protect the confidentially of patient information, including a warning that breach of this obligation would be grounds for immediate termination of [their] employment.

Supervision

[16] I consider supervision of employees to be another reasonable administrative safeguard for the protection of personal health information. The Custodian discovered the personal health information disclosures to an unauthorized person during an investigation of the Employee, relating to their use of emails. This indicates that the Custodian supervises their employees, and investigates suspected non-compliance with Custodian policies. However, many months of unauthorized disclosures had passed before the Custodian discovered the breach.

Limiting access to personal health information

[17] The affected individual who states that "access should have several levels", may be referring to the practice of restricting the information that employees can access, based

on their job duties. For example, an accounting clerk should not normally have access to all treatment information, and a medical technician should not normally have access to accounting and banking information. Such information controls are a required component of information practices under clause 39(4)(a) of the *HIA*.

[18] It appears that the Employee had access to much of the personal health information of clients, as the Custodian advises that in a few incidents the Employee disclosed case information, test results, medical or other professional opinions or treatment, medical conditions, patient signs and symptoms, and/or questions and concerns.

Summary

[19] The fact that disclosure to an unauthorized person occurred, does not automatically mean that the Custodian did not have reasonable information practices in place. Even reasonable information practices will have some risk of disclosure to an unauthorized person. However, discovery of a breach will often reveal a gap in a custodian's information practices. Most employers would not foresee that an employee would disclose such a large volume of personal health information to prove they were at work. However, custodians must prepare for disclosures to unauthorized persons for other reasons such as errors, financial or social gain, malicious intentions, and poor judgment. It is unreasonable to fail to foresee these possibilities, and custodians must prepare for them.

[20] Clause 39(4)(f) of the *HIA* requires custodians to ensure agents of a custodian adhere to the safeguards and controls implemented to protect personal health information. The expression "agent" is defined in the *HIA* at section 1(a), and includes employees of a custodian.

[21] I am not persuaded that, at the time that these breaches were discovered, the Custodian had implemented reasonable controls to limit the persons who may use

personal health information, or to restrict access to only that personal health information that the employee required. On the contrary, it appears that the Employee had access to all of the clients' personal health information, which put the personal health information at additional risk.

[22] If the Custodian had adequate practices in place relating to training, supervision, and limits on access to personal health information, there would have existed a culture of privacy protection in the workplace. Such a culture, when accepted as the normal course of things by employees and management, is the best method of ensuring that all types of privacy breaches are minimized. The Custodian had a manual which included obligations of confidentiality, but did not have privacy training for employees. The Custodian supervised employees, but such supervision did not detect a large number of privacy breaches which continued over many months. The Custodian also did not appear to turn their mind to limiting access to personal health information, based on what is necessary for employees to carry out their job duties. Based on these facts, I find that, prior to this breach, the Custodian failed to establish and implement reasonable information practices, in contravention of subsection 36(1) and section 39 of the *Health Information Act*.

[23] It is important to note that, at the time of the discovery of this breach, the *HIA* had only recently been proclaimed in force. The newness of the privacy protection obligations do not relieve the Custodian of responsibility, but they do provide some context, in that the Custodian may have been operating under policies which existed prior to the proclamation of the *HIA*. As will be described below in the discussion of remediation, the Custodian has recently advised that they have retained an IT security specialist and that they will be implementing several technical safeguards to prevent privacy breaches. I will examine whether these planned safeguards meet the requirement of reasonable information practices.

Issue Two: Did the Custodian respond reasonably to the disclosures of personal health information to an unauthorized person?

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

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

Breach notification

[25] Subject to some exceptions, on discovering disclosure of personal health information to an unauthorized person, custodians are required to notify the individual to whom the personal health information relates and the Commissioner at the first reasonable opportunity. This requirement is set out at clause 36(1)(c) of the *HIA*.

> 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.

[26] I will review the Custodian's process of notification, the content of their notice to affected individuals, and the Custodian's decision not to notify the affected individuals of the identity of the Employee or the Recipient.

Process of notification

[27] On May 1, 2018, the Commissioner ordered the Custodian to notify the affected individuals to this privacy breach. As the Order at Appendix A indicates, the Commissioner's order only applied to those breaches which occurred after July 1, 2017, the date the *HIA* came into effect. The Custodian did not have a legal obligation to notify those affected individuals whose personal health information was breached prior to July 1, 2017, which would have been hundreds of individuals. Although there was no legal obligation to do so, the Custodian decided to notify all affected individuals.

[28] The Custodian provided evidence detailing the process of mailing out the notifications to affected individuals. In June, 2018, a four person team addressed the envelopes by hand, referring to a list of responsible parties to match with the list of patients, who are mostly minors. Of the four employees, only one of them remains employed by the Custodian. That employee advised that they worked with two other employees, in a shared space, during regular work hours, to address, stamp, and seal the envelopes for mailing. With regard to the number of notification letters addressed by the employee, the employee states, "I estimate that it would have been hundreds".

[29] Some of the affected individuals state they did not receive the notice the Custodian mailed the week of June 11, 2018. This was discovered when the Commissioner mailed the investigation summary in November, 2018, to 1,035 individuals. The majority of people who contacted the Commissioner, 49/51 individuals, advised that, despite the paragraph in the investigation summary stating that the Custodian notified affected individuals in June of 2018, the investigation summary from the Commissioner was the first they had heard of the breach. Some individuals advise that they had attended at the Custodian for treatment several times, and there was no mention or indication that there had been a privacy breach. None of the 51 individuals were able to confirm that they had received the notice from the Custodian.

[30] The Custodian advises that Canada Post returned approximately 30 of the 1041 notices that they had mailed. In some cases, the Custodian was able to contact the client and obtain an updated mailing address. Canada Post returned 108 of the 1035 letters the Commissioner sent, as address unknown.

[31] Following the mailout of the investigation summary by the Commissioner, the Custodian was also advised by a number of affected individuals who received the Commissioner's letter and enclosures, that they had not received the Custodian's notice in June of 2018. The Custodian advises that they have no explanation for why these individuals did not receive their notices. The Custodian confirmed they had used the same addresses for their notices as the Commissioner had used.

[32] Due to the reports of affected individuals not receiving the original notification letter, the Custodian recently advised the Commissioner that they decided to re-issue notification letters to all affected individuals. The contents of the new notification letters will be discussed further below.

[33] Based on the evidence provided by the Custodian, I find that the Custodian made efforts to notify the affected individuals. However, based on the statements of those affected individuals who contacted the Commissioner, and based on the discrepancy in the number of returned notices of the Custodian compared with those of the Commissioner, when using the same mailing list, I find that it is likely that notices for some affected parties were not mailed by the Custodian. The Custodian advises they take the feedback of failed deliveries very seriously, and they have decided to mail new notification letters, albeit nine months later.

Content of Notification letter

[34] Section 36 of the *HIA* requires that custodians notify affected individuals when their personal health information is stolen, lost, disposed of improperly, or disclosed to or

accessed by an unauthorized person, but the *HIA* and the regulations are silent on the content of the notification.

[35] The Custodian's original notice included a brief description of the privacy breach, and advised that the Employee had been terminated, and the Recipient had confirmed that they had deleted all of the emails containing the personal health information. The Custodian also advised that they had reported the matter to the Commissioner, and to the Police. This information is well written and is in plain language. Although the notice did not specify the precise personal health information of the individual to whom the notice was being sent, it did provide contact information of a Custodian manager, should the affected party have any questions.

[36] In the notification order attached as Appendix A, I offered to provide the Custodian guidance with regard to the content of the notification. The Custodian did not seek guidance from the Commissioner. What is missing from the original notification are steps the Custodian is taking to prevent similar privacy breaches in the future. Custodians may not always be in a position to provide such information, as notifications are often sent before the custodian has completed their investigation of the breach. In this case, however, the notices were sent six months after discovery of the breach, and the Custodian's investigation had been completed for some time. It would have provided significant comfort to the affected individuals to know the Custodian's plans to prevent future breaches of their personal health information. Failure to add this information to the notification letter is a shortcoming.

[37] The above-noted shortcoming has been remedied by the Custodian, with the new notification letters recently sent by the Custodian to all affected individuals. In the new notification, the Custodian advises as follows:

> We want to assure you that were are taking measures to prevent this type of incident from taking place in the future. [The Custodian] has retained a third-party security firm to accelerate

> the ongoing security enhancements to our network. As well, we have been and will continue to provide mandatory data privacy training to all full-time and part-time staff.

Should the Employee and/or the Recipient be identified to the affected parties?

[38] Some affected individuals asked for the name of the Employee and the Recipient. This information was not contained in the notification letter or the Commissioner's investigation summary.

[39] I have considered whether the Custodian ought to provide the name of the Employee and the name of the Recipient. The position of the Custodian is that disclosure of the identity of the Employee and the Recipient would constitute an unreasonable invasion of their personal privacy.

[40] There is no requirement in the *HIA* that a custodian identify to the affected individuals the person who stole, lost, disposed, disclosed or accessed their personal health information, nor is there a prohibition against it.

[41] A recent report of the Commissioner, Breach Report HI-18-005, *Re: Health PEI*, 2018 CanLII 130517 (PE IPC), discusses the heightened need for an affected individual to know the identity of a snooper, someone who has accessed personal health information without authority:

> [72] . . . 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. . . .

[42] In cases of snooping, the *HIA* specifically requires that custodians maintain an electronic record, detailing each person who has accessed personal health information from an

information system. Similar to victims of snooping, individuals affected by a disclosure of their personal health information to an unauthorized person may, in some circumstances, have a need to know the identity of the person who disclosed, and/or the person who received, their personal health information without authority.

[43] Several affected individuals who contacted the Commissioner expressed concern that the Employee will obtain another position in which they will have access to personal health information. I consider this factor, the objective of protecting the public, to weigh in favour of disclosing the name of the Employee and of the Recipient. However, there are other factors to consider.

[44] Both the Custodian and police services were satisfied, based on their investigations, that the purpose of the Employee's disclosure, and the purpose of the Recipient's collection, was unrelated to the content of the personal health information. The Employee was disclosing the information to confirm to the Recipient that the Employee was at work. In my view, the need to know the identity of the Employee and the Recipient is reduced somewhat by these conclusions. In addition, the declaration by the Recipient and the Recipient's employer confirming the destruction of personal health information, and that the personal health information was not used or disclosed, and will not be used or disclosed, weighs in favour of not disclosing the identities of the Employee and the Recipient.

[45] The Custodian has been placed in the position of following their legal obligations to protect the privacy of their clients and patients, while also attempting to determine whether it is necessary to provide the personal information of the Employee and the Recipient. Based on the particular circumstances of this breach, and weighing all factors as set out above, I find the decision of the Custodian not to disclose the identities of the Employee or the Recipient to the affected individuals, is reasonable.

Breach Containment

[46] Containing a privacy breach includes taking reasonable steps to ensure that no further personal health information is at risk of disclosure to an unauthorized person, and if possible, that personal health information is returned, and not subject to further risk of unauthorized access, use or disclosure.

[47] In this matter, the Custodian dismissed the employee. They reported the matter to the police, and contacted the Recipient, and the Recipient's employer to assess the scope of the disclosures. They obtained statutory declarations from the Recipient and the Recipient's employer. The Recipient certifies that:

> . . .I have not accessed and will refrain from accessing or using any information of the Company, including personal information of patients. I hereby certify that I have securely destroyed every document susceptible to contain Company Information and I have not disclosed any Company Information.

[48] The Recipient's employer confirms that:

> We reviewed your request and our digital records. In response to your request, we have deleted all email material on our servers sent from @[Custodian's domain name] domain name. Moreover, to the best of our knowledge, no material that we received from the @[Custodian's domain name] domain name has, at any time, been transmitted from our servers.

[49] Police services also interviewed the Recipient, and are satisfied that the purpose of the disclosures was as the Employee had stated, to confirm to the Recipient that they were at work.

[50] Some of the affected individuals asked how they could be sure their personal health information was not further disclosed. This is a valid concern. However, based on the foregoing, I find that the Custodian took reasonable steps to prevent further unauthorized access, use or disclosure of personal health information.

Breach Investigation

[51] Custodians should conduct internal investigations, to determine all of the causes of a breach. There is rarely only a single shortcoming that permits a breach of privacy to occur. The requirement for different types of safeguards is an acknowledgement that there are multiple layers of preventative measures. Without investigations into all of the potential causes, it is not possible to prevent future similar breaches.

[52] Once the breach was discovered, the Custodian met with the Employee, notified the Commissioner, and contacted police services. The Custodian's prompt investigation led them to confirm the Employee did not further disclose, intend to further disclose in the future, or use the personal health information for malicious purposes. The Custodian also sought and received confirmation from the Recipient that the emails containing personal health information were deleted.

[53] 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 disclosing personal health information may indicate a malicious intent. As part of their investigation, the Custodian inquired about the Employee's reasons. The Custodian interviewed the Employee, who stated they disclosed the information to the Recipient for the purposes of confirming the Employee's location to the Recipient. No other purpose was identified.

[54] Several affected individuals were skeptical of the reason provided by the Employee for the breach. The Custodian recognizes that the reason the Employee provided is not an acceptable purpose of disclosure of personal health information. However, following their investigation, the Custodian accepted that the Employee was being truthful about their stated purpose. Given that the Recipient and the Employee were consistent in their description of the purpose, and that police services also confirmed the Recipient had no interest in the personal health information, except to confirm the Employee's

presence at the workplace, I find that it is reasonable that the Custodian did not investigate further.

[55] Based on all of the foregoing, I find that the Custodian conducted an adequate investigation.

Remediation

[56] Good information practices are key to the 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.

[57] The Custodian advised that between the time the breach was discovered and the time the Commissioner distributed the investigation summary, the Custodian had provided privacy training for its staff, and planned to repeat the training annually.

[58] Some affected individuals who contacted the Commissioner asked whether credit card tracking/fraud protection would be provided by the Custodian. The Custodian responded and advised that, although there is no reason to believe that they are at any risk of fraud or identity theft, as a goodwill gesture they will offer to provide credit monitoring services to the seven individuals whose credit card and/or banking information was disclosed, for a two year period.

[59] Since then, the Custodian further advises that they have provided employees with guidance documents, and plans to train new employees. They also advise as follows:

> The privacy breach in this case arose in unique circumstances and would not necessarily have been detected by additional safeguards. Nonetheless, [the Custodian] is taking steps to implement enhancements to its IT security regime. In addition to the training described above, these measures will include:

1. The introduction of a strong password policy and two-step verification
2. Encryption of data at rest and in transit
3. Implementation of a mobile device management policy
4. Implementation of Google Data Loss Prevention
5. Improved data segregation, to limit access to sensitive information to those employees who have a need to know
6. Implementation of GSuite email monitoring tool to detect unusual or suspicious activity in employee email accounts
7. Use of firewalls to block access to inappropriate or harmful sites.

[60] If the Custodian carries out their annual training, and the seven measures described above, they will address the shortcomings in their information practices described at paragraphs [21] and [22] above. In particular, the improved data segregation will address limiting access to personal health information, and the email monitoring tool will address shortcomings in supervision of employees. I am confident that these seven measures, combined with annual training, and training of new employees, will foster the culture of privacy protection the *HIA* is meant to create.

I. SUMMARY OF FINDINGS

Issue One: Did the Custodian establish and implement reasonable information?

[61] I find that, at the time of discovery of this privacy breach, the Custodian had not established reasonable information practices to prevent the disclosure of personal health information to unauthorized individuals. However, I find that the Custodian has since implemented reasonable information practices to prevent such disclosures in future.

Issue Two: Did the Custodian respond reasonably?

[62] I find that there were shortcomings in the process of the Custodian's notification, and in the content of the notifications. However, these shortcomings were addressed adequately by the Custodian, by sending out new notification letters.

[63] I find that the Custodian's decision not to identify the Employee or the Recipient was reasonable in these circumstances.

[64] I find that the Custodian took reasonable steps to contain this breach.

[65] I find that the Custodian adequately investigated the disclosures of personal health information to an unauthorized person, and has adopted reasonable measures to remediate the disclosures.

[66] Based on all of the above, I have no further recommendations to make.

[67] I thank the Custodian for their cooperation with this investigation, and I am particularly appreciative of each affected individual who contacted the Commissioner with questions, concerns, or comments.

_____

Karen A. Rose
Information and Privacy Commissioner

APPENDIX A

IN THE MATTER OF AN INVESTIGATION BY THE INFORMATION AND PRIVACY COMMISSIONER OF PRINCE EDWARD ISLAND UNDER PART III OF THE *HEALTH INFORMATION ACT*, 1988, R.S.P.E.I .Cap H-1.41

NOTIFICATION ORDER
Case File Number BRH-17-007
May 1, 2018

FACTUAL BACKGROUND

[1] In or about December, 2017, a custodian under the *Health Information Act* ("the Custodian") was investigating an employee's personal use of business email. During the Custodian's investigation, they discovered that the employee of the Custodian ("the Employee") had disclosed to a family member, by email, personal health information of the Custodian's clients.

CUSTODIAN'S INITIAL RESPONSE

[2] The Custodian's immediate response was to ensure the Employee had no further access to any personal health information. The Custodian terminated the Employee from their job, pursuant to the Custodian's policy, that a breach of the responsibility to protect the confidentiality of patient information would be grounds for immediate termination.

[3] The Custodian, via its agent, then notified the Office of the Information and Privacy Commissioner, by telephone and in writing, of this unauthorized disclosure of personal health information.

[4] The Custodian also notified the appropriate police agency.

INVESTIGATION

[5] The Custodian commenced an investigation into the nature and scope of the privacy breach. The Custodian reviewed the emails and interviewed the Employee.

[6] The Custodian states that, over a period of time leading up to December 2017, the Employee sent email messages containing the personal health information of the Custodian's clients. The Employee sent the emails while at the Custodian's workplace. All emails were sent to the same family member ("the Recipient").

[7] The amount of personal health information varied for each client. The types of personal health information disclosed in most cases included the following:

- payment information, including patient contract information;
- payment amounts, discounts, late payments, and information about returned payments (NSF payments); and
- banking information related to payments. For further clarification, banking information includes financial institution, bank account numbers, account holder, credit card institution and/or credit account numbers.

[8] In a smaller number of instances, the personal health information disclosed, included:

- Case information, appointment dates and other information about appointments, including clients' address, phone number, information about family members, and/or place of employment;
- Email correspondence with patients;
- Internal emails which may include personal health information;
- Clients' test results, medical or other professional opinions or treatment, medical conditions, patient signs and symptoms, and/or questions and concerns.

[9] The Employee was cooperative during their interview with the Custodian. The Custodian was persuaded that the unauthorized disclosures were not for any illegal or nefarious purposes, e.g. to facilitate the commission of crimes such as theft, fraud, or harm to property, or to embarrass or harass the clients. The Employee advised the Custodian that the Employee sent the emails to the Recipient, throughout the work day, to confirm to the Recipient that the Employee was at work.

[10] The Custodian states that it is their understanding that the Recipient had no interest in the personal health information contained in the emails. The Recipient provided their written certification that they had not further disclosed, and had securely destroyed the emails containing the personal health information. As the Employee sent some of the emails to the Recipient's work email, the Custodian also obtained the Recipient's employer's written certification that every email and enclosure has been securely destroyed and that no emails from the Custodian's domain name had been transmitted to anyone else from their servers.

[11] Police services interviewed the Recipient, as part of their investigation. Police services confirmed that they were satisfied that the Recipient had no interest in the content of the emails from the Employee, apart from confirming the Employee's presence at the workplace. Police services assessed that there was no intent by the Recipient to further disclose the personal health information.

NOTIFICATION

[12] The Custodian considered the criteria of clause 36(1)(c) of the *Health Information Act,* relating to notification to the clients. The Custodian determined that the exception to notification of the clients, set out at subsection 36(2) of the *Health Information Act,* applies to the circumstances of these unauthorized disclosures, and the Custodian determined that they are not required to notify the clients whose personal health information was subject to unauthorized disclosure. The Custodian, however, notified

the Commissioner, in the interests of transparency. The Custodian states that they will provide notification to individuals if the Commissioner requires it.

[13] Clauses 36(1)(c) and 36(2) of the *Health Information Act* state:

> 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.
>
> Exception
> (2) Clause (1)(c) does not apply if the custodian reasonably believes that the theft, loss, disposition, disclosure or access of personal health information will not
>
> (a) have an adverse impact on the provision of health care or other benefits to the individual to whom the personal health information relates;
> (b) have an adverse impact on the mental, physical, economic or social well-being of the individual to whom the personal health information relates; or
> (c) lead to the identification of the individual to whom the personal health information relates.

[14] Section 36 of the *Health Information Act* has not yet been considered by the Office of the Information and Privacy Commissioner. Based on my analysis of section 36, and based on the evidence provided, I find that the Custodian is required to notify the clients whose personal health information was disclosed on or after July 1, 2017.

[15] Clients of the Custodian belong to a relatively small group of individuals seeking private medical services. Prince Edward Island is a small province, with a population of about 150,000. The community in which the Custodian conducts business is still smaller. Even if I accept that the Recipient has no interest in the content of the information sent to

them, the fact remains that the Recipient viewed personal health information, and that the personal health information cannot be unseen by the Recipient. Taking into consideration all relevant factors, including the scope of the disclosures and the size of the community, I find that there is a reasonable expectation that the Recipient may have recognized a client's name, or still recalls the content of at least some of the emailed records.

[16] The types of personal health information disclosed by the Employee to the Recipient, without authorization, outlined at paragraphs [7] and [8] above, is sensitive in nature. This information could be used for a range of purposes, from identity theft to embarrassment of the clients to whom the information relates. In my view, therefore, the Custodian's belief that the Employee's disclosure of personal health information will not have an adverse impact on the mental, physical, economic or social well-being of the individuals to whom the personal health information relates, is not a reasonable belief. I find that the Custodian cannot properly rely upon clause 36(2)(b) of the *Health Information Act*, in support of a decision not to notify the affected clients.

[17] The *Health Information Act* was proclaimed into force in Prince Edward Island on July 1, 2018. Section 3 states:

> 3. Application
>
> This Act applies
>
> > (a) to personal health information that is collected, used or disclosed by a custodian or that is in the custody or control of a custodian; and
> >
> > (b) to personal health information that was collected before the coming into force of this Act and that is prescribed by regulation whether or not it was collected by a person or organization that meets the criteria of a custodian under this Act.

[18] Although the *Health Information Act* applies to personal health information that was collected before the coming into force of the *Act*, it does not apply to those disclosures of personal health information which occurred prior to July 1, 2017. Therefore, my Order under section 36 cannot apply to those disclosures which predate July 1, 2017.

ORDER

[19] Based on the foregoing, I order the Custodian to notify, as soon as practicable, those clients whose personal health information was disclosed on or after July 1, 2017, by the Employee, without authorization, and to provide confirmation to this office when notification is complete. If the Custodian requires guidance relating to the content of the notifications, this office will provide such guidance.

[20] I thank the Custodian for their submissions relating to this breach.

_____

Karen A. Rose
Information and Privacy Commissioner