Information and Privacy Commissioner,
Ontario, Canada

Commissaire à l'information et à la protection de la vie privée,
Ontario, Canada

PHIPA DECISION 202

HI21-00010

A Health Centre

February 14, 2023

Summary: During the course of working with this office on a privacy breach file, a Health Centre notified the Information and Privacy Commissioner of Ontario that additional possible unauthorized accesses by a number of employees had been discovered. This file was opened to address the additional unauthorized accesses and the systemic issues related to the breaches.

The Health Centre ultimately determined 28 of those accesses to be breaches of the *Act*. This decision concludes that at the time of the breaches the Health Centre had inconsistencies regarding staff requirements to sign confidentiality and EMR authorized user agreements, there was an inadequate privacy notice on the Health Centre's EMR system, and a formal privacy breach policy was not in place. As such, this Decision finds that at the time of the breaches, the Health Centre had not taken reasonable steps to protect the personal health information within the meaning of section 12(1) of the *Act*. However, this decision also finds that the Health Centre has since remedied these issues.

This decision also finds that the Health Centre did not provide the patients affected by this breach the notification required by section 12(2) of the *Act*. Specifically, the Health Centre did not provide notice of the breach "at the first reasonable opportunity."

Lastly, I decide that no review of this matter is warranted.

Statutes Considered: *Personal Health Information Protection Act, 2004*, S.O. 2004, c. 3 (the *Act* or *PHIPA*);

Decisions Considered: Orders HO-010 and HO-013 and *PHIPA* Decisions 44, 64, 70. 74 and 124.

BACKGROUND:

[1] In September 2020, the Information and Privacy Commissioner of Ontario (IPC or this office) received a breach report from the Health Centre regarding an inappropriate access by a Health Centre manager. Subsequent to receiving the initial breach report, the Health Centre also reported that an audit also revealed a number of questionable chart accesses by other employees.

[2] The additional accesses identified were made by five staff members of a particular unit at the Health Centre (the unit) and appeared to be unauthorized. While the accesses made by the manager were addressed in a separate file, this file was opened to address the systemic issues associated with the unauthorized accesses of the five employees as well as the Health Centre's response to the breaches.

[3] The Health Centre initially advised that the additional accesses occurred on October 24, 2019, when the unit was participating in Electronic Medical Records (EMR) system training. The Health Centre explained that fake charts had been set up for training purposes, however, based on the audit, the five employees were found to have also accessed real patient charts. A further audit of the five employees also identified a number of questionable accesses that continued after the date of training.

[4] Initially, the Health Centre did not make any final determination on whether the accesses of the employees were breaches under the *Act*. The Health Centre explained that although a reason for many of the accesses could not be identified, they were unable to determine whether the accesses were unauthorized because the five staff members involved had failed to follow procedures for documenting chart accesses. The audits revealed that encounters with patients and schedules were frequently left blank or filled out incorrectly.

[5] As a result, this matter moved to the Investigation Stage of the IPC's *PHIPA* complaint process. As part of the investigation, this office requested and received written representations from the Health Centre.

[6] During the investigation of this file, the Health Centre completed an in-depth analysis of the accesses and determined that, between the five employees, there were 28 unauthorized accesses.

DETAILS OF THE ACCESSES OF THE FIVE EMPLOYEES:

[7] Under this heading I will summarize details of the accesses identified by the Health Centre for each employee. Later in this decision, I describe the Health Centre's responses to the accesses and the steps that have been taken to address the systemic issues identified in this decision.

[8] According to the Health Centre, the inappropriate accesses that occurred on

training day were initially believed to be from a misunderstanding about what the employees were supposed to do, and what charts they were supposed to be accessing. However, given the number of accesses on training day that were of concern, the Health Centre believed that this demonstrated wide-spread insufficient training for the staff of this unit. The Health Centre advised that it believed the breaches were a result of misdirection and poor leadership.

Employee One:

[9] An audit conducted by the Health Centre revealed that on the training day, employee one accessed the records of 12 patients the employee previously encountered. After the training day, the employee accessed the records of a number of additional patients.

[10] The Health Centre interviewed the employee about the accesses and the employee advised that she had accessed the records to obtain contact information for the patients. During the interview, the employee was advised on how to properly access patient contact information and to complete proper documentation of accesses. The employee was also provided a verbal warning advising that any additional breach would result in an immediate dismissal.

[11] Upon the completion of an in-depth review of this employee's accesses, it was determined by the Health Centre that there was no appropriate explanation for the employee's access to nine of the patient records noted above. The Health Centre found no evidence that the employee used the personal health information accessed for non-health care purposes, however the accesses were determined to be unauthorized.

[12] A follow-up audit was completed on this employee and no additional inappropriate accesses were identified. This employee resigned during the investigation and no longer works at the Health Centre.

Employee Two:

[13] The audit conducted by the Health Centre determined that on the training day, employee two accessed the records of 24 patients the employee had previously encountered, and one record of an employee at a different location. After the training, employee two accessed the records of a former colleague, a possible family member and one patient that is no longer active at the Health Centre.

[14] The Health Centre's privacy officer met with employee two (along with employee three) to discuss the accesses. Both employees advised the privacy officer that their accesses to patient records were for work purposes. The interview did not garner any information from either employee about specific accesses. During the interview, the employees were warned by the privacy officer that staff should not be accessing the records of family or friends.

[15] Employee two's accesses were reviewed in-depth and the Health Centre determined that four accesses to patient records were deemed to have been unauthorized and breaches of the *Act*.

[16] This employee retired during the Health Centre's investigation and no longer works at the Health Centre.

Employee Three:

[17] The Health Centre advised that on the day of training, employee three accessed five records. After the training, employee three accessed two additional patient records that appeared to be unauthorized.

[18] After an in-depth review of the accesses, the Health Centre determined that all seven of the above noted accesses were unauthorized and breaches of the *Act*. The Health Centre identified that the accesses were records of possible family members, known members of the community, a former colleague and a patient where the relationship was unknown. As previously mentioned, during an interview regarding this matter, this employee was warned by the privacy officer that staff should not be accessing the records of family and friends.

[19] This employee no longer works at the Health Centre.

Employee Four:

[20] The Health Centre advised that on the training day, employee four accessed 24 records of patients they had previously encountered, and three records of patients where the relationship was unknown. After the training day, the Health Centre determined that employee four had accessed the records of three patients to whom employee four had relationships with.

[21] The privacy officer was unable to meet with this employee as they went on a leave of absence, and no longer works for the Health Center.

[22] After the Health Centre's in-depth review of the accesses, it determined that three of accesses were unauthorized and breaches of the *Act*.

Employee five:

[23] The Health Centre advised that employee five did not access any patient records on the training day however, after the training day, six patient records were accessed.

[24] The privacy officer did not meet with employee five after the accesses were identified as the employee went on a leave of absence.

[25] After an in-depth review of the accesses by the Health Centre, it determined four

accesses were unauthorized and breaches of the *Act*. The Health Centre was able to identify that the employee accessed the file of a colleague, and five records where the relationship was unknown.

[26] This employee no longer works at the Health Centre.

PRELIMINARY ISSUES:

[27] There is no dispute that the Health Centre is a health information custodian and that the employees are agents of the Health Centre under the *Act*. There is also no dispute that the records accessed by the employees are records of "personal health information".

[28] Based on the information set out above, as a preliminary matter, I find that:

- the Health Centre is a "health information custodian" under paragraph 4 of section 3(1) of the *Act*;
- the employees are an "agent" of the Health Centre, within the meaning of section 2 of the *Act*;
- the records at issue contained "personal health information" under section 4(1)(a) and (b) of the *Act*; and
- the employees' access was a "use" within the meaning of section 2 and 6 of the *Act*,

ISSUES:

[29] In this decision, the following issues will be discussed:

1. Did the Health Centre take reasonable steps to protect personal health information?
2. Did the Health Centre notify the individuals affected by the unauthorized use of the personal health information in accordance with section 12(2) of the *Act*?
3. Is a review warranted under Part VI of the *Act*?

RESULTS OF THE INVESTIGATION:

Issue 1: Did the Health Centre take reasonable steps to protect personal health information?

[30] Section 12 of the *Act* requires health information custodians take "reasonable" steps to protect personal health information in their custody and control against unauthorized use or disclosure, among other things. The *Act* also requires health information custodians to take appropriate steps when confronted with a breach, or in this case, a possible breach of the *Act*. These steps include completing an investigation to determine whether there has been a breach, determine the scope of the breach, containment of the personal health information involved, notification of those affected and remediation of the breach.

[31] Section 12(1) of the *Act* states:

> A health information custodian shall take steps that are reasonable in the circumstances to ensure that personal health information in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal.

[32] Administrative and technical safeguards are critical to protecting personal health information. The IPC has previously stated that, in order to comply with the requirement in section 12(1) of the *Act,* custodians must take steps that are reasonable in the circumstances to protect personal health information and must implement administrative and technical measures or safeguards.[1] Such measures and safeguards can include privacy policies, privacy training and awareness programs and initiatives.

[33] In *PHIPA* Orders HO-010 and HO-013, and more recently in *PHIPA* Decisions 64 and 70, the IPC held that section 12(1) of the *Act* required health information custodians to review their measures or safeguards from time to time to ensure that they continue to be reasonable in the circumstances to protect personal health information in the custodians' custody or control. Health information custodians are expected to identify risks to privacy and take reasonable measures to reduce or eliminate such risks and mitigate the potential harms that may arise.

[34] As part of this investigation, I reviewed the steps the Health Centre took to contain the breach, its privacy practices and policies, training, processes for confidentiality agreements, audits and privacy notices. I will explore the issues, concerns and response of the Health Centre in detail below.

---

[1] See HO-013

Containment:

[35] In October 2020, when the Health Centre initially determined through an audit that there were potential breaches by five employees from a particular team, patient charts were reviewed to determine whether the accesses were authorized. The Health Centre initially advised that based on this review it was unable to confirm whether accesses were unauthorized because the staff involved had failed to follow proper procedures regarding the documentation of patient charts.

[36] In November 2020, the Health Centre's privacy officer interviewed three of the five employees as two had gone on a leave of absence. The Health Centre concluded that these interviews did not garner additional information that allowed the Health Centre to decide whether the accesses by these employees were authorized.

[37] Subsequent to the above, in response to concerns raised by this office during this investigation, the Health Centre completed an in-depth review of 138 chart entries identified through an audit as possible breaches. The review determined that 110 entries were for the provision of care and authorized accesses. The remaining 28 accesses were determined to be unauthorized.

[38] The Health Centre reported that the 28 accesses were determined to be a breach of the *Act* due to one or more of the following reasons:

- no evidence of a working relationship between the patient and the employee;
- a lack of evidence that the employee was part of the patient's circle of care;
- no identified collaboration with other employees working with the patient;
- no appointments booked between the patient and the employee;
- no record of a program relevant referral on file;
- no reason for entering the chart, documented or not; or
- access to charts of family members, former colleagues or inactive patients.

[39] The Health Centre ultimately determined that the unauthorized accesses were due to a lack of knowledge, insufficient training, and a lack of support from the Health Centre.

[40] As noted previously, the duty of health information custodians to take reasonable steps to protect personal health information in its custody and control, including protecting the personal health information from unauthorized use, includes a duty to respond adequately to the identification of a potential privacy breach. A proper response will, among other things, help to ensure that the breach, if any, is contained,

and will not re-occur.[2]

[41] When a health information custodian is investigating whether a breach occurred and the scope of the breach, it is important that a thorough review be completed.

[42] Health information custodians must contain a breach in a timely manner and complete a thorough review and investigation of the accesses including, but not limited to, the following issues:

a. whether the staff member was a part of the patient's circle of care;

b. proper documentation of the date of access;

c. whether the employee has the same last name, address or phone number as the patient;

d. whether the patient is a colleague, family or friend;

e. review the relevant policies related to accessing patient files;

f. determine the role and duties of the employee at the time of access to establish whether access is authorized based on the role of the employee (i.e., what was the reason for access to the record, and was the access related to the provision of care).

[43] According the Health Centre, after interviewing three of the five employees, the Health Centre was unable to obtain pertinent information to confirm whether the accesses were authorized. Despite this, further inquiries required to make this determination were not completed. It was not until this office requested a further detailed review that the Health Centre took steps and was able to determine which accesses were authorized and which were not.

[44] Based on the lengthy delay between the Health Centre becoming aware of a possible breach and taking the appropriate steps to make a determination, it appears that the Health Centre did not prioritize the safeguarding of their patients' personal health information.

[45] In response to this concern, the Health Centre created a new privacy breach policy that now outlines the responsibilities of Health Centre employees when responding to a suspected privacy breach. Going forward the Health Centre has committed to following its policy and prioritizing the containment of any future breach.

[46] Importantly, one of the challenges the privacy officer faced during their investigation into the breaches was the lack of response by employees to the privacy

[2] PHIPA Decision 44, para. 140

officer's requests for meetings with them. The Health Centre has addressed this issue and advised that moving forward, meetings with the privacy officer will be mandatory for employees to attend, and failure to attend will result in disciplinary actions. The privacy officer will also be required to inform the individual's direct supervisor and the Director of Operations of the individual's failure to meet with the privacy officer.

Discipline

[47] With the exception of the verbal warning provided to employee one, no disciplinary measures for the other staff were considered. Instead, the Health Centre determined the employees needed more training. The Health Centre's position was that the breaches that occurred on training day were initially believed to be from a misunderstanding about what the employees were supposed to do and what charts they were supposed to be accessing. However, given the number of questionable accesses on training day, the Health Centre ultimately determined that this demonstrated wide-spread insufficient training for the staff of this unit. The Health Centre advised that in their view, they had a responsibility to provide more training and support to staff, which it did.

[48] In addition, the lack of discipline was based on the information available at the time. By the time the in-depth analysis was completed and determinations were made about the accesses, three of the five employees were no longer working at the Health Centre, and the remaining two employees were on a leave.

[49] With respect to the Health Centre's decision to only issue a verbal warning to one employee and re-train the remainder of the employees involved, I am satisfied that it was reasonable in the circumstances and does not take away from the adequacy of the Health Centre's response to the breaches. In this case, the Health Centre ultimately determined that the inappropriate accesses were a result of a lack of knowledge of the employees, insufficient training and a lack of support from the Health Centre.

[50] In previous investigations, this office has stated that its role is not to judge the severity or appropriateness of sanctions taken by a custodian against its agents[3]. However, the IPC can take into account a custodian's disciplinary response as part of its assessment of whether the custodian has taken reasonable steps to protect personal health information against unauthorized access.[4]

Privacy Training:

[51] According to the Health Centre, at the time of the breaches, new employees were receiving privacy and security training as part of their orientation and annually. They were also required to read and sign off on the Health Centre's privacy policies. In addition, the privacy officer circulates a monthly privacy newsletter and privacy is a

[3] *PHIPA* Decision 74
[4] *PHIPA* Decision 124

standing agenda item at all monthly all-staff meetings. Finally, program area managers are instructed to reiterate privacy obligations at team meetings.

[52] In response to these breaches, the Health Centre provided additional training for the employees involved in the breaches (those that were still working there), as well as separate training for all staff. The Health Centre advised that it had three all-staff meetings to train employees on audits, how to complete proper documentation in charts, when to access a patient's chart, how to find demographic information of patients and what steps to take if staff enter a chart without authorization. The Health Centre also had a training session for all staff on the Privacy Breach Protocol and the Human Resources procedure for privacy breaches. The policy requires that all staff review this policy annually and sign off on it. Specifically, staff are confirming that they have read and understood the policies, and will apply them to their work duties.

[53] The Health Centre has committed to continuing to provide annual privacy training and track all privacy training of its employees.

Confidentiality Agreements:

[54] The Health Centre advised that its policies require all-staff to sign a confidentiality agreement upon hire and at the time of the breaches, it was each manager's responsibility to ensure that new staff complete the required onboarding and all the requirements of orientation, including signing the confidentiality agreement.

[55] However, when the Health Centre reviewed its records for the employees involved in the breach, it determined that only two of the five employees had signed a confidentiality agreement upon hire.

[56] After the breaches were identified, the employees involved were asked to re-sign (or sign, if they had not done so already) the confidentiality agreement, however, only two employees involved re-signed the confidentiality agreement and not until many months after requested. The remaining employees did not sign as they were no longer working at the Health Centre.

[57] During this investigation, the Health Centre was asked to review to confirm that all employees had signed a confidentiality agreement. Contrary to its policy, not all of the Health Centre's employees had signed a confidentiality agreement upon hire. In addition, employees were not required to re-sign on an annual basis.

[58] Moving forward, in order to ensure that its policies are followed and all staff sign a confidentiality agreement upon hire, the Health Centre has implemented an orientation checklist with deadlines and designated a human resources employee with the responsibility to track all staff orientation, training and signed agreements rather than have the responsibility rest solely on the various managers of the Health Centre. The Health Centre also advised that if a new employee does not sign the confidentiality agreement within the first week of hire, the employee and their manager will be

contacted by human resources. The new employee will also not be able to book vacation or professional development until the confidentiality agreement is signed.

[59] In addition, all employees are now required to re-sign a confidentiality agreement on a yearly basis. In order to ensure that employees re-sign the confidentiality agreements annually, managers are required to review this requirement at weekly meetings starting in October 2022. All confidentiality agreements will be signed by the end of October on a yearly basis. If not signed, vacation, other leave requests and professional development requests will not be approved until they are completed.

[60] The Health Centre has also reviewed the files of all of its employees and confirmed that all their active employees have now signed a confidentiality agreement.

[61] The Health Centre advised that employees are also required to sign an EMR Authorized User Agreement upon hire. When the Health Centre reviewed its records, it was determined that three of the employees involved in the breaches did not sign an EMR Authorized User Agreement upon hire. Several months after the breach, the employees involved were asked to re-sign the EMR Authorized Agreement. However, two of the staff no longer worked at the Health Centre by the time this occurred.

[62] The Health Centre also reviewed its records for all employees and determined that not all of its employees had signed the EMR Authorized User Agreement.

[63] Moving forward, the Health Centre advised that in order to ensure that the EMR Authorized User Agreement is signed upon hire, it has put all the documents to be signed in one package for new employees. The employees will be required to review and submit the signed documents to human resources staff rather than their manager. If it is not signed within the first week, human resources will follow-up the following week to ensure it is completed. This has been changed as a result of the breach. Previously, the Health Centre was allowing this document to be signed up to one month after hire.

[64] In addition, new employees will not be given access or training on the EMR until a signed copy of the EMR Authorized User Agreement is received and shared with the privacy officer.

[65] During this investigation, the Health Centre confirmed to this office that all their employees have now signed the EMR Authorized User Agreement.

Audit Functionality:

[66] During the Health Centre's investigation into the breaches, it performed audits of the five employees' accesses. These breaches came to the attention of the Health Centre as a result of the audits completed.

[67] Moving forward, the Health Centre has committed to completing monthly privacy audits of all of its program areas. Both random and targeted audits are completed, including targeted audits of family members that are known patients.

[68] In addition, the Health Centre advised that it has asked employees to voluntarily provide information about known family and friends that receive services at the Health Centre. The Health Centre explained that this information will be used to compare accesses during the auditing process.

[69] The Health Centre also completed a review of the levels of access employees have to patient charts based on their various roles to ensure that all employees have an appropriate level of access based on their role at the Health Centre.

Privacy Notices:

[70] The Health Centre initially advised that it had a privacy warning implemented on its EMR system, however, it was later determined that the warning was only triggered if an employee attempted to access a patient's chart at a different location than the location the employee is based at.

[71] Privacy notices remind custodians and their agents of their obligations and of the consequences of unauthorized access and may also serve to prevent or reduce the risk of unauthorized access to personal health information.[5]

[72] On September 27, 2021, a privacy notice was implemented on the Health Centre's EMR system and is now displayed upon every login for all employees.

[73] In addition, if an employee attempts to access a health record of a patient that they do not have privileges to access, a notice is viewed by the employee prior to access. If the employee proceeds with access to the record, the employee is required to provide a reason for overriding the security measure to gain access to the chart. In addition, a notice is also sent to the privacy officer for review and determine that access was authorized.

Policies:

[74] At the time of the breaches, the Health Centre did not have a formal privacy breach policy. There was a document in place for the privacy officer to follow should there be a breach, which was shared with administration staff and leadership but the Health Centre could not confirm if the document had been shared with all of its employees prior to the breaches.

---

[5] Information and Privacy Commissioner of Ontario. (January 2015) *Detecting and Deterring Unauthorized Access to Personal Health Information*. Retrieved from https://www.ipc.on.ca/wp-content/uploads/resources/detect_deter.pdf

[75] The Health Centre developed a formal policy for privacy breaches in March 2021, after the breaches at issue in this investigation were identified. This policy has been approved and implemented. Employees were provided a copy of this policy and it is accessible to all employees on the Health Centre's internal database.

[76] Employees of the Health Centre are required to review all Health Centre policies on an individual basis every other year, and review the Privacy Breach Policy annually. Staff are required to review and confirm/sign off that they have read, understood and agree to follow these policies as a condition of employment.

[77] With respect to documentation of employee work products, the Health Centre has three policies related to proper documentation. After the privacy breaches were identified, the three employees involved who were not on a leave were retrained on proper documentation. Proper documentation was also reviewed at an all staff meeting after the breaches.

[78] At the time of the breaches, the Health Centre had a policy that addresses what is deemed as an inappropriate access by an employee which includes the patient having the same last name or address as the user, and the person being a high-profile community member if this individual did not receive service from the employee. However, the Health Centre advised that given that it is located in a small community it may be the case that an employee provides health care service to a family, friend or colleague. The policy has been updated to address this by stating that an employee is to notify the privacy officer if they need to enter the chart of a family member or colleague.

[79] Moving forward, the Health Centre has advised that if employees are found not to be following policies, a formal investigation will be launched and any necessary discipline would be implemented based on the findings.

[80] This investigation was opened in response to concerns about possible breaches of the *Act* and systemic issues at the Health Centre. I also had a number of concerns about the adequacy of the Health Centre's response to the breaches. During this investigation a number of gaps in the Health Centre's privacy breach protocols and related practices were identified. In response, the Health Centre took a number of steps which included:

- conducting an in-depth review of the chart entries;
- implementing a new privacy breach policy;
- providing additional communications and training to all their employees on privacy breach protocols, audits, proper documentation in charts, when to access patient charts and what steps to take to enter a chart without authorization;

- ensuring all employees signed a confidentiality agreement and modified their policy to require they be re-signed annually;
- conducting monthly audits; and
- implementing a privacy notice on their EMR system.

[81] At the time of the breaches, the Health Centre's privacy policies and training fell short and were lacking in areas. There were inconsistencies related to the signing of confidentiality and EMR Authorized User Agreements, and there was an inadequate privacy notice on the Health Centre's EMR system. The Health Centre also did not have a formal privacy breach policy in place at the time of the breaches. In light of these shortcomings, it is my view that at the time of the breaches, the Health Centre had not taken reasonable steps to protect the personal health information within the meaning of section 12(1) of the *Act*. However, I also find that the Health Centre has since remedied these issues to bring them in compliance with the *Act*.

Issue 2: Did the Health Centre notify the individuals affected by the unauthorized use of the personal health information in accordance with section 12(2) of the Act?

[82] Section 12(2) of the *Act* requires that health information custodians notify individuals whose personal health information is disclosed without authorization. This section states:

> (2) Subject to subsection (4) and to the exceptions and additional requirements, if any, that are prescribed if personal health information about an individual that is in the custody or control of a health information custodian is stolen or lost or if it is used or disclosed without authority, the health information custodian shall,
>
> > (a) notify the individual at the first reasonable opportunity of the theft or loss or of the unauthorized use or disclosure; and
> >
> > (b) include in the notice a statement that the individual is entitled to make a complaint to the Commissioner under Part VI.

[83] At the beginning of this investigation, the Health Centre had not notified any patients because it had yet to determine which accesses were unauthorized. As a result of the delays in determining whether accesses were unauthorized, there was also a delay in the notification of the patients that were affected. However, once the Health Centre confirmed that unauthorized accesses had occurred, they did notify the patients in a timely manner.

[84] Notification letters were mailed out to the 26 affected patients on August 30 and 31, 2021. The notification letters included details about the circumstances of the

breach, the date of the breach of the patient's chart, steps taken to ensure that further breaches do not occur in the future, contact information for the privacy officer should the patients have any questions and contact information for this office.

[85] Of the 26 letters that were mailed out, two letters were returned to the Health Centre. These two letters were placed on the patients' charts with a note requesting that staff contact the privacy office should the Health Centre receive updated contact information. If contact information is received, the privacy office will resend the letters.

[86] Two patients could not be contacted because the Health Centre did not have contact information on file.

[87] The Health Centre's "Human Resources Procedure for Privacy Breaches" requires that any individual affected by a privacy be notified. The Health Centre's policy has been updated to reflect that any letter to patients notifying them of a privacy breach that are returned will have the letter attached to the file and a note made on the file that an updated address is required upon the patient's next interaction with the Health Centre, and that the privacy officer is to be notified when updated contact information is obtained.

[88] In the circumstances of these breaches, there was a significant delay in the Health Centre determining which accesses were a breach of the *Act,* and therefore notification did not occur in the early stages of the Health Centre's investigation. Rather, notification occurred almost one year after the Health Centre reported this matter to the IPC. It is expected that when a privacy breach, such as the one at issue in this matter is suspected, a health information custodian will make a determination regarding the scope of the breach within a reasonable timeframe, and that after such a determination is made, any affected patients will be notified at the "first reasonable opportunity".

[89] Despite the delay, once the unauthorized accesses were determined, notification did occur in a timely manner. In my view, the significant delays in notifying the affected parties were directly related to gaps in the Health Centre's Privacy Breach Protocol, which resulted in an inadequate investigation into the breaches. As such, I find that the Health Centre did not provide the patients affected by this breach the notification required by section 12(2) of the *Act*. Specifically, the Health Centre did not provide notice of the breach "at the first reasonable opportunity."

[90] Despite my finding above, and as noted previously, I am satisfied that the Health Centre has addressed the gaps in their privacy breach policies which would have also impacted the timely notification of the affected patients.

Issue 3: Is a review warranted under Part VI of the Act?

[91] Section 58(1) of the *Act* sets out the Commissioner's discretionary authority to

conduct a review as follows:

> The Commissioner may, on his or her own initiative, conduct a review of any matter if the Commissioner has reasonable grounds to believe hat a person has contravened or is about to contravene a provision of this Act or its regulations and that the subject-matter of the review relates to the contravention.

[92] In accordance with my delegated authority to determine whether a review is conducted under section 58(1) of the *Act* and for the reasons set out above, I find that a review is not warranted.

NO REVIEW:

For the foregoing reasons, no review of this matter will be conducted under Part VI of the *Act.*

Original signed by: February 14, 2023

Lucy Costa
Manager of Investigations