Information and Privacy Commissioner,
Ontario, Canada

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

PHIPA DECISION 124

HR17-222

A Rehabilitation Clinic

July 9, 2020

Summary: A rehabilitation clinic (the Clinic) contacted the Office of the Information and Privacy Commissioner of Ontario (IPC) to report a privacy breach under the *Personal Health Information Protection Act, 2004* (*PHIPA*). A Clinic employee downloaded, and failed to delete, personal health information to her family computer. Her then-spouse later found this personal health information and reported the matter to the IPC. During the investigation of this breach, the employee's spouse alerted the IPC to a further breach. The second breach involved personal health information which had been stored in the spouse's email account.

In light of the Clinic's response to the breach and improvements it has since made, no review of this matter will be conducted under Part VI of *PHIPA*.

Statutes Considered: *Personal Health Information Protection Act*, 2004, sections 2, 4(2), 4(3), 12(1), 29, and 58(1).

Decisions Considered: PHIPA Decisions 74 and 82

INTRODUCTION:

[1] This investigation was opened under the *Personal Health Information Protection Act, 2004* (*PHIPA* or the *Act*) as a result of information submitted by a rehabilitation clinic (the Clinic). The Clinic reported that the estranged spouse (the Spouse) of a Clinic employee (the Employee) had access to personal health information of Clinic clients. This personal health information was stored on personal computing devices that were in the possession of the Spouse. During the investigation of this reported breach, the Clinic reported a second breach to the IPC, in which the Spouse reported having

discovered emails in his account that contained additional personal health information belonging to Clinic clients.

BACKGROUND:

Breach #1 – Files on Personal Computer

[2] The Spouse contacted the Clinic, stating that he had two personal computing devices, which had previously belonged to the Employee, and that these contained patient files relating to clients of the Clinic. At the time the Clinic reported this breach to the IPC, it was not able to provide details of the types of records or the clients affected. The Clinic reported that it had been in communication with the Spouse, but had not been successful in having the Spouse either delete the files or provide the computers to the Clinic. The Spouse later sent the Employee's family lawyer a link to a Google drive folder, and advised her that the documents in that drive contained personal health information of Clinic clients.

[3] The Clinic accessed this folder and determined that the Spouse had access to the personal health information of three Clinic clients. According to the Clinic, the Employee identified the documents as reports she had opened from her Clinic email. She accessed her email via a secure server, but when she "double-clicked" the files, a copy downloaded automatically to her personal computer, without her knowledge. The Employee stated that she had a practice of deleting any files she downloaded but failed to delete these automatic downloads, as she did not know they had been stored on the device.

[4] After accessing the files, the Clinic did not get in contact with the Spouse to request that he delete the files; the Clinic's lawyer instead contacted the IPC.

[5] The IPC sent the Spouse a letter in which we informed the Spouse that it was this office's preliminary view that he was prohibited under section 49(1)(a) of the *Act* from using or disclosing the personal health information in his possession. The IPC stated that it was seeking his cooperation in destroying all copies of the personal health information on the computers, and in providing a written attestation to that effect.

[6] The Spouse confirmed that he had deleted the three files shared via Google drive, but stated that he had additional records of Clinic clients' personal health information on the computers. While the Spouse initially confirmed that he would cooperate by either deleting those files or allowing Clinic representatives to delete them, this was followed by several months of correspondence involving the Clinic's lawyer, the Spouse, and the IPC regarding how to best transfer or delete the files. The Spouse eventually arranged to provide the personal computer and tablet to the Employee's family lawyer. Once the family lawyer received these devices, she provided them to the Clinic, without looking at their contents.

[7] According to information provided by the Clinic, IT professionals hired by the Clinic located a folder on the computer desktop, which included hundreds of files containing personal health information, though many were identified as duplicate files. In total, 164 unique files contained the personal health information of 46 Clinic clients. These included documents which would contain a significant amount of personal health information, such as applications for benefits, test results, treatment plans, and letters from hospitals.

[8] IT did not find any other files containing personal health information on the computer. All personal health information was deleted from the computer and the computer was returned to the Employee. The Clinic was not able to access the tablet, but the Employee confirmed she had not used that tablet for work purposes.

Breach #2 – Files in Spouse's Email Account

[9] During the correspondence regarding the return of the computer, the Spouse reported that he had five emails in his personal email account that contained information belonging to clients of the Clinic. He provided these to the Clinic.

[10] One email, sent from the Spouse to the Employee (the Business Email), contained information belonging to an individual who was not a Clinic client. This individual had contacted the Employee at her home number regarding the Employee's private business. The Spouse had taken down the details provided by the individual, and sent these to the Employee at her Clinic email address.

[11] The remaining emails (the Clinic Emails) were sent from the Employee's Clinic email account to the Spouse and contained information relating to three Clinic clients. Two of the emails had attached assessment reports relating to the same client, and included information such as the client's injury history, details of his physical, emotional, and cognitive circumstances, and recommendations for occupational therapy and other services. The other two emails included details of two other clients' situations, medical and otherwise, as well as contact information for those close to the clients.

[12] Only one of the Clinic Emails included a client's name, though others included a client's initials, age, and address. Collectively, the Client Emails also contained the names and/or contact information of those close to Clinic clients, such as a parent or other family member, care provider, and/or lawyer.

[13] The Clinic stated that the Employee had sent these emails to the Spouse for printing at home, and that she thought she had taken the steps necessary to de-identify the client information in the Clinic Emails. Initially, the Clinic took the position that, of the Clinic Emails, only the one containing a client's name contained personal health information, stating that the others did not contain identifying information. The Clinic later acknowledged that all the Clinic Emails contained personal health information belonging to Clinic clients.

[14] The Spouse confirmed to the IPC that while he had forwarded the emails to the Clinic's lawyer, he did not delete them. The Clinic did not initially communicate with the Spouse to request he do so, believing that the Spouse's word had not previously been reliable and that the Spouse had a history of behaviour that included making threats of litigation and filing complaints with regulatory bodies. The Clinic asked instead that the IPC contact the Spouse to seek confirmation that he had deleted the emails. Following further correspondence with this office, the Clinic contacted the Spouse about deleting the emails. The Spouse then confirmed to the Clinic that he had deleted the personal health information, providing the following response:

> I confirm that I have deleted each of the Emails you refer to in your letter of today's date. Regarding those Emails, I further confirm that I have not made any copies of, retained or shared the Emails or any other personal health information relating to clients of [the Employee] or [the Clinic].

DISCUSSION:

[15] It is not in dispute and I find that the person who operates the clinic is a health information custodian. Under sections 17 and 37(2) of the *Act*, a health information custodian which is permitted to use personal health information may permit its agents to use that information in order to carry out their duties. Section 2 contains a definition of an "agent". It is not in dispute and I find that the Employee is an "agent" of the Clinic, within the meaning of the *Act*.

Preliminary Issue #1 – Business Email

[16] The security obligations of health information custodians are set out in section 12(1) of the *Act* as follows:

> 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.

[17] From the information before me, it does not appear that the section 12 security obligations are engaged by the Spouse's access to the Business Email. There was no indication that the individual described in the Business email was a client of the Clinic. The Clinic stated that this email was in the Clinic's possession due to the Spouse having sent it to the Employee's Clinic email, rather than her personal email. As such, it does not appear that the Clinic was a "health information custodian" for the purposes of its dealings with the Business Email, in that it did not have custody or control of that email for the purpose of providing health care to the individual.

[18] Nevertheless, the Clinic ensured that the Employee made efforts to notify the individual, and obtained confirmation from the Spouse that this email was deleted. Given this, I will not be addressing the Business Email further.

Preliminary Issue #2 – Was the information in the Clinic Emails "personal health information?"

[19] After initially taking the position that only one of the Clinic Emails – the email that contained a client's name – contained personal health information, the Clinic later acknowledged that all such emails contained personal health information.

[20] I note that it is clear that all the Clinic Emails included personal health information, even if they did not contain the names of Clinic clients. Section 4(2) of the *Act* defines identifying information as "information that identifies an individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual." That a record does not include a client's name does not preclude it from containing identifiable information.[1]

[21] The test, as articulated in PHIPA Decision 82, is whether it is reasonably foreseeable, in the circumstances, that those without special knowledge could identify the patient by combining the information provided by the custodian with other available information. In this case, the extent of the information in the emails (such as a client's initials, names of clients' family members, details of clients' circumstances, as well as contact information of family members and/or care providers) indicates that the clients could reasonably be identified. As such, the Clinic's latter position that the Clinic Emails contain personal health information is affirmed and this decision is proceeding on that basis.

ISSUES:

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

1. Was personal health information "disclosed" in accordance with the *Act*?
2. Did the Clinic take steps that were reasonable in the circumstances to protect personal health information in accordance with section 12(1) of the *Act*?
3. Is a review warranted under Part VI of the *Act*?

[1] PHIPA Decision 82

RESULTS OF THE INVESTIGATION:

Issue 1: Was personal health information "disclosed" in accordance with the *Act*?

[23] Section 2 of the *Act* defines "disclose" as follows:

> "disclose", in relation to personal health information in the custody or under the control of a health information custodian or a person, means to make the information available or to release it to another health information custodian or to another person, but does not include to use the information, and "disclosure" has a corresponding meaning;

[24] I will address each breach separately.

Breach #1

[25] When the Spouse alerted the Clinic to Breach #1, he stated that he was in possession of two personal computing devices with multiple files containing the personal health information of Clinic clients. The Clinic, after discussions with the Employee, determined that the Employee had inadvertently stored these files on her personal computer. The Clinic stated that this had likely happened via files being saved on a temporary basis prior to being printed or uploaded to the Clinic's secure server. The Employee stated that she did not intentionally retain copies of records containing personal health information on the computer, and had thought she had deleted all files containing client information from her computer. There is no indication in the information before me that the Employee intended for these records to remain on the computer.

Breach #2

[26] The personal health information involved in Breach #2 was contained in email exchanges between the Employee and the Spouse. The Employee stated that she sometimes encountered issues printing documents at her home, and when that happened, she would send the information to the Spouse, so that he could print the documents via his wireless printer. The Employee stated that she believed that the emails sent to the Spouse either contained no personal health information, or contained personal health information that had been adequately de-identified. The Clinic later acknowledged that all of the Clinic Emails contained personal health information.

Disclosure of Personal Health Information

[27] The evidence before me indicates that the Employee did not intend for the Spouse to have access to personal health information, or in the case of the Clinic Emails, to have access for any longer than it would take to print the relevant documents. However, the Employee did make the personal health information available

to the Spouse, even if she did so inadvertently and in error. The *Act* does not require that a disclosure be deliberate.

[28] Under the *Act*, personal health information is permitted to be disclosed if the disclosure complies with section 29, which states:

> A health information custodian shall not collect, use or disclose personal health information about an individual unless,
>
> > (a) it has the individual's consent under this Act and the collection, use or disclosure, as the case may be, to the best of the custodian's knowledge, is necessary for a lawful purpose; or
> >
> > (b) the collection, use or disclosure, as the case may be, is permitted or required by this Act.

[29] In this case, there is no claim that the disclosures were authorized under the *Act*, and for the purposes of this decision I will assume that they were not.

Issue 2: Did the Clinic take steps that were reasonable in the circumstances to protect personal health information in accordance with section 12(1) of the *Act*?

[30] As set out above, section 12(1) of the *Act* requires that health information custodians take reasonable steps to ensure that records of personal health information in their custody or control are protected against unauthorized disclosure, among other things.

[31] In this case, the breaches arose from the Employee accessing and/or printing personal health information at her home. This resulted in the Spouse being able to access this information, with the Employee's knowledge at the time and without her knowledge afterwards. These circumstances raised questions about whether the Clinic had taken reasonable steps to guard against unauthorized disclosures, including sufficient steps to train its employees about their privacy obligations and technical safeguards.

Privacy Policies & Procedures

[32] At the time of the breaches, the Clinic had a secure server in place for remote access. Safeguards for personal health information were included in the Clinician Agreement, which prohibited staff from printing, copying, or downloading electronic records except "where necessary for the provision of care or in circumstances where access to records is required for the provision of care and remote access to [the Clinic's] server is not available."

[33] The Clinic's Clinician Agreement also required the Employee to maintain the

confidentiality and security of records that were located at her home office or otherwise with her. This included an agreement that the Employee "will not store any identifiable PHI Records on [her] personal computer's hard drive, applications or cloud technology." At the time, the Employee had incorrectly thought that the records at issue were de-identified, in the case of the emails, and had been unaware that the other records had not been deleted from her personal computer.

[34] The Clinic revised both its Clinician Agreement and Privacy Policy during the course of this investigation, making explicit the steps to be taken should a similar situation arise in future. This includes a recognition in the Clinician Agreement that printing a document may create a copy in a computer's temporary downloads file, and imposes an obligation on the staff member to either delete this folder daily or set up automatic deletion. The Clinic has advised that they have provided training to staff on how to delete the folder contents and how to set up automatic deletion. The Clinic has further advised that their IT staff have upgraded their current system to allow for printing of documents directly from the secure server, such that they are not downloaded to the local computer at all.

[35] The Privacy Policy includes a directive to only send, download, or store personal health information in very limited circumstances; namely, where remote access is not available and the records cannot be viewed from an encrypted device. If doing so in those limited circumstances, the Clinician Agreement requires that such information be encrypted and permanently deleted when no longer required. The Clinician Agreement also prohibits sending personal health information to a clinician's personal email address and requires that any records with identifying information be treated in the same manner as other records of personal health information. The Clinic's Privacy Policy was similarly updated.

Confidentiality Agreements

[36] In addition to the Clinician Agreements, the Clinic had a practice of having all staff sign Confidentiality Agreements. During the investigation, the Clinic amended its Confidentiality Agreements to include statements that staff members "will not under any circumstances send or transmit Confidential Information to my personal email account" and "will not leave Confidential Information exposed for others to view." The Clinic states that all Clinic staff have signed the amended version of the Confidentiality Agreement, and that all Clinic staff have signed both the amended Confidentiality Agreement and the Clinician Agreement.

Privacy Training and Education

[37] The Clinic informed the IPC that it provides privacy training to all staff upon hire. In addition, existing staff have the option of refreshing their training by attending the webinars given to new hires.

[38] Since the breach, the Clinic has instituted annual privacy training for all employees. The Clinic has stated that this annual training includes training on the Clinic's Privacy Policy and Breach of Privacy Policy, review of privacy safeguards, and highlights of changes to legislation. The Clinic held its first annual all-staff privacy session in January 2019, which addressed both breaches, and has scheduled training sessions each January going forward.

[39] The Clinic provided additional privacy instructions and training to all staff in response to the breaches. The Clinic's Privacy Officer emailed all staff regarding: the use of personal computing devices; the safe storage and use of encrypted USBs to store identifiable personal health information outside of the server; and how to ensure that temporary files that may be stored in downloads are deleted on a daily basis. The Privacy Officer also made a presentation to all staff regarding Clinician Agreements and safeguards, including technological safeguards.

[40] The Clinic provided training to the Employee in response to these breaches. In addition to group session privacy training as described above, the Employee received one on one training regarding both breaches. In particular, this training addressed the procedures the Employee used in printing and downloading personal health information, and the procedures she should have used to safeguard these records of personal health information. Following the first annual privacy training, the Privacy Officer reviewed the training with the Employee individually. At that time, the Employee reported implementing the changes in her practice and following the Clinic's requirements as set out in the revised Clinician Agreement.

[41] The duty to take reasonable steps to ensure that personal health information in the Clinic's custody or control is protected against theft, loss and unauthorized use or disclosure includes a duty to respond adequately to a complaint of a privacy breach. A proper response will, among other things, help to ensure that a breach, if any, is contained, and will not re-occur. The standard in section 12 is "reasonableness". It does not require perfection, and the section does not provide a detailed prescription for what is reasonable.

[42] In assessing the adequacy of the custodian's response to this breach, the following steps are most relevant in the circumstances of this case:

1. Containment of the breach.

2. Notification of appropriate parties.

3. Investigation and remediation.

The Clinic's efforts to contain the breach

[43] As part of the Clinic's efforts to contain the Breach #1, it made numerous attempts to reach out to the Spouse to determine what information was stored on the

personal computer and tablet in his possession. The Clinic also made efforts to arrange to have these devices brought into its possession, so that the files containing personal health information could be identified, transferred to the Clinic, and deleted from the personal devices.

[44] The Clinic faced considerable difficulty in its efforts, as the Spouse's position on what steps he was willing to take varied significantly through their dialogue. The Spouse ultimately returned the personal computer and the tablet to the Employee during their family law proceedings. The return of the devices contained Breach #1, as it related to the information stored on those devices. At that point, the Clinic was also able to identify the scope of Breach #1 for the first time.

[45] During the efforts to contain the first breach, the Spouse alerted the Clinic to the second breach, involving the personal information contained in his email accounts. In contrast to Breach #1, the Spouse provided the Clinic Emails to the Clinic promptly, and the Clinic was able to identify both the extent of the personal health information at issue and the identities of the affected clients. The remaining step for containment of Breach #2 was for the Clinic to ensure that the Spouse did not retain copies of those emails.

[46] The Clinic initially did not get in contact with the Spouse to ensure this containment took place. The Clinic asked that the IPC do so instead, stating as follows:

> Given [the Spouse's] inconsistent responses to our requests, his threats of retaliation in response to our communications, and his decision to initiate a [regulatory college] complaint even as he was agreeing to return [the Employee's] computer to her, we did not think it prudent or worthwhile to seek confirmation from [the Spouse] that he had deleted all copies of the email messages at issue in Breach #2. Rather, we were hopeful that your office would seek this confirmation from him…

[47] It is clear that interactions between the Clinic and the Spouse had been very challenging, chiefly due to the Spouse's changing positions throughout this investigation. However, the obligations on a health information custodian to contain the breach remain, even in the face of challenging circumstances. The Privacy Breach Guidelines are clear that there is an obligation on the health information custodian to retrieve any copies of personal health information that have been disclosed and ensure that no copies of personal health information have been made or retained by anyone who was not authorized to receive the information. Nothing in the legislation or these guidelines transfers this obligation to the IPC.

[48] In discussions with the Clinic, the IPC reminded the Clinic of this obligation. The Clinic later confirmed to the IPC that it had since emailed the Spouse. The Clinic relayed that the Spouse had confirmed that he no longer had personal health information of Clinic's clients in his possession, stating as follows:

> I confirm that I have deleted each of the Emails you refer to in your letter of today's date. Regarding those Emails, I further confirm that I have not made any copies of, retained or shared the Emails or any other personal health information relating to clients of [the Employee] or [the Clinic].

[49] Having confirmed with the Spouse that he no longer possessed any personal health information of Clinic clients, and having earlier obtained the personal computing devices from him, I am satisfied with the Clinic's efforts to contain the breaches.

Notification of appropriate parties

[50] Among those individuals affected by Breach #1, the Employee met with the active clients to notify them of the breach, and the Clinic sent the active clients follow up notification letters. The Clinic sent notification letters to the remaining individuals affected, whose files were inactive. The Clinic was unable to notify five individuals, and instead added notification letters to their files, in the event they contact the Clinic in future.

[51] For those affected by Breach #2, the Clinic notified two of the affected individuals both in person and by letter. The remaining affected individual was a minor child, and the Clinic made several efforts to reach out to that minor's mother. As it was not able to reach her, the Clinic placed a copy of the notification letter on that individual's file.

[52] In both cases, the Clinic provided detailed letters, outlining the circumstances of the breach, the containment efforts, the steps the Clinic has taken to enhance its privacy policies, and the additional training that was conducted in response to the breach. The letters also contained the contact information for the IPC, in the event any affected individuals wished to make a complaint to this office.

[53] The Clinic did not notify the Employee's regulatory college of the breaches, though it did note that the Spouse himself had reported Breach #1 to this college. The Clinic stated that it was their understanding that reporting to the college was only required in instances where it had taken disciplinary action, which had not occurred in this case. The Clinic provided its reasoning in opting to educate, rather than discipline, the Employee:

> [The Clinic] opted not to take disciplinary action in the circumstances of this case. They recognized that [the Employee] attempted to delete all PHI records downloaded (for legitimate purposes) to her computer, and that [the Employee] took steps to de-identify information, and only later learned that the de-identification was not as complete as she intended. Recognizing that [the Employee] was concerned about safeguarding her clients' privacy, that she believed that she had acted responsibly throughout, and that her actions were not repeated or deliberate or

> blatantly careless or sloppy, [the Clinic] determined that education, rather than discipline, was an appropriate response.

[54] Section 17.1(2) of the *Act* requires a custodian to notify a health profession regulatory college if it disciplines an employee who is a member of such a college, because of unauthorized access to personal health information. In this case, the Clinic made the decision not to discipline the Employee, and this obligation therefore does not apply.

[55] With respect to the Clinic's decision, I am satisfied that it was reasonable in the circumstances. This office has stated that its role is not to judge the severity or appropriateness of sanctions taken by a custodian against its agents (see PHIPA Decision 74). However, the IPC can taken 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.

[56] In the circumstances of this case, I am satisfied that the Clinic's decision to educate rather than impose discipline does not detract from the adequacy of its response to the breaches.

Investigation and remediation

[57] The Clinic's Privacy Policy, at the time of the breaches, did prohibit the Employee from storing identifiable personal health information on her personal computer. However, the training provided by the Clinic did not result in the Employee understanding how to avoid downloading personal health information to her computer, or how to adequately de-identify personal health information. After reviewing all of the information provided by the Clinic, including the improvements made to both its policies and training subsequent to the breach, I am satisfied that the issues in this matter have been adequately addressed. As a result, it is not necessary for me to make a finding on whether, at the time of the breach, the Clinic was in compliance with section 12(1) of the *Act*.

[58] I would also like to note the Clinic's responsiveness to our Office during this investigation. The Clinic's responses throughout displayed a high level of both detail and cooperation.

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

[59] 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 that 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.

[60] 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.

DECISION:

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

Original Signed by: July 9, 2020

Jennifer Olijnyk
Investigator