Information and Privacy Commissioner,
Ontario, Canada

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

PHIPA DECISION 266

Complaint HI22-00028

A Clinic

November 22, 2024

Summary: A source contacted the Information and Privacy Commissioner of Ontario to report that a multi-disciplinary health clinic was disposing of records of personal health information in an unsecured manner in contravention of the *Personal Health Information Protection Act, 2004* (the *Act* or *PHIPA*). The investigator finds that the clinic, as the health information custodian in this matter, was not in compliance with sections 10(1) (Information practices) and (2) (Duty to follow practices), 12(1) (Security) and 13(1) (Handling of records) of the *Act.* However, considering the measures applied in response to the breach, including the creation and implementation of privacy and security policies, practices, procedures and training, the investigator finds that an order is not warranted.

Statutes Considered: *Personal Health Information Protection Act, 2004, S.O. 2004, c. 3;* sections 1(a), 3(1), 4(1), (2) and (3), 10(1) and (2), 12(1), and 13(1).

Decisions Considered: Order HO-001; Order HO-003, Order HO-006; PHIPA Decision 50, PHIPA Decision 102.

BACKGROUND:

[1] In August 2022, the Information and Privacy Commissioner of Ontario (IPC or this office) received a complaint from a person (the source[1]) regarding a multi-disciplinary health clinic (the clinic). The source alleged that the secretary/office manager at the clinic

[1] The source advised the IPC that they did not want their identity disclosed to the clinic.

was destroying and disposing of records of personal health information (PHI) in an unsecured manner.

[2] The source provided the IPC with photographs to substantiate the allegations. The pictures showed what appeared to be patient records (papers with handwritten and typed clinical information) in a blue recycling bin. Some of the records were ripped, and others were intact. There were also pieces of paper that appeared to be hand torn, mixed with shredded pieces of paper.

[3] According to the source, to obtain proof that the clinic was disposing of PHI in an unsecured manner, they removed some of the records from the clinic's recycle bin and placed them in a locked box in a secure location.

[4] The circumstances described above raised questions about the clinic's obligations under the *Act*. Specifically, the IPC was concerned about the clinic's information and security practices in relation to the disposal of records of PHI.

[5] After receiving the complaint and pictures, the IPC wrote the clinic to inquire into the allegations. In response, the clinic submitted a report regarding the concerns raised.

[6] The clinic's response raised additional concerns for the IPC and as such, the matter was moved to the Investigation Stage of the IPC's complaint process, and I was assigned as the investigator.

[7] During my investigation, this office issued a *Notice of Review* under section 58 of the *Act* and a determination under section 60(13) of the *Act*, so the records of PHI could be retrieved from the source.

[8] After obtaining custody of the records, I pieced together many of the torn and shredded portions, and was able to read the following information:

a. The name, contact information and address of the clinic;

b. The name and contact information of a registered health professional working for the clinic;

c. Dates showing patient visits and consent for treatment between 2013 and 2019;

d. A patient's date of birth;

e. A patient's complete name and self-reported health history, and

f. Six other complete patient names, a partial first and partial last name, and other first names or last names of patients.

[9] During my investigation, I wrote to the clinic and requested information about its information and security practices and its response to the concerns raised in this matter.

I also provided the photographs to the clinic. The responses I received are discussed below.

The Clinic's Response

[10] According to the clinic, during the summer of 2022 (June to end-of-August) its office manager was trying to make more space in the clinic by clearing out records for inactive clients of a former business partner. The clinic owner initially supervised the disposal of these records by the clinic manager and ensured the records were shredded.

[11] The clinic submitted that at some point the office manager also decided to dispose of records belonging to several registered massage therapists (RMTs) who no longer worked at the clinic. The clinic manager disposed of some of these patient records by hand-tearing them and placing them in a recycling bin under a desk, to be disposed of by cleaners.

[12] The clinic advised that it was not aware of its office manager's decision to dispose of these records. According to the clinic, the office manager began hand tearing the RMT records because of a concern that the noise of the shredder was disturbing patients in appointments.

[13] The recycling material containing the torn patient records was picked up by cleaners biweekly and placed in a dumpster in the locked garage area of the plaza where the clinic is located. The garbage was picked up weekly by the local garbage collector.

[14] The clinic acknowledged that the cleaners would have had access to and ultimately disposed of the records, noting that "insecurely destroyed material ended up at the garbage dump."

[15] The clinic stated that when the clinic owner received a notice from the IPC in April of 2023 advising that the IPC was investigating allegations of inappropriate disposal of patient records, staff were instructed to cease all destruction of records to ensure that no further records were disposed of in an inappropriate manner.

[16] The clinic acknowledged that its containment efforts were not successful as the clinic owner only learned of the breach almost a year after the garbage would have been collected.

[17] The clinic advised that it had no written policies or procedures about record retention or secure record destruction or disposal. Rather, expectations had been communicated to staff verbally.

[18] In view of the above, the clinic acknowledged that at the time of the breach, the clinic was not in compliance with sections 10(1) (Information Practices), 10(2) (Duty to follow Practices), 12(1) (Security) and 13(1) (Handling of records) of *PHIPA*.

[19] Despite the above, the clinic did not initially notify the affected patients whose records were disposed of in this unsecured manner. However, during my investigation, after reviewing the photographs of the records, and its physical client records, the clinic determined that a total of 482 patients could have been affected and decided to notify them.

[20] In addition to the above, the clinic took steps to address the IPC's concerns and as a result, the following measures were implemented:

- A *Client Records* policy was created;
- The clinic's *Privacy Policy* was updated;
- Training sessions were provided to staff about the new/updated polices;
- Staff were required to submit a written acknowledgement in relation to the new/updated polices;
- A *Privacy Statement* was created for posting on the clinic's website to inform clients about practices regarding their PHI;
- Practices and polices were set to be reviewed and revised yearly as necessary; and
- Staff was required to review and reaffirm their commitment to the clinic's *Privacy Policy* annually.

PRELIMINARY ISSUES:

[21] The clinic does not dispute, and I find, that the clinic is a "health information custodian" within the meaning of section 3(1) of the *Act*.

[22] Further, the clinic does not dispute, and I find, that the patient health records at issue contained PHI within the meaning of section 4 of the *Act*.

[23] Lastly, the clinic admitted, and I find, that at the time of the disposal of personal health information, it was not in compliance with sections 10(1),10(2), 12(1) and 13(1) of the *Act*.

ISSUE:

[24] This decision addresses whether the clinic responded adequately to the breach.

RESULTS OF THE INVESTIGATION:

[25] *PHIPA* requires health information custodians to protect PHI in their custody or control, including against unauthorized disposal. This breach raised concerns about the clinic's information practices regarding written policies, training and notification, as well as compliance with these practices.

[26] My three-part analysis below focuses on these concerns, the steps the clinic took to remediate the breach, and the policies and practices enacted to protect the PHI of patients as required by sections 10, 12, and 13 of the *Act*. Consequently, my analysis will look at:

- Information practices and duty to follow these [s. 10(1) and (2) of *PHIPA*],
- Security of PHI [s. 12(1) and 13(1) of *PHIPA*], and
- Notification to affected parties [s. 12(2) of *PHIPA*].

Information practices and duty to follow practices:

[27] Section 10 (1) of the *Act* states:

> A health information custodian that has custody or control of personal health information shall have in place information practices that comply with the requirements of this Act and its regulations.

[28] Section 10 (2) states:

> A health information custodian shall comply with its information practices.

[29] Section 2 of the *Act* defines "information practices" as:

> "information practices", in relation to a health information custodian, means the policy of the custodian for actions in relation to personal health information, including,
>
> > (a) when, how and the purposes for which the custodian routinely collects, uses, modifies, discloses, retains or disposes of personal health information, and
> >
> > (b) the administrative, technical and physical safeguards and practices that the custodian maintains with respect to the information

[30] The clinic acknowledged that it did not have written policies with respect to information practices at the time of the breach. According to the clinic, it had in place "verbally expressed expectations" that patient records "be disposed of in a secure manner (which for physical records includes shredding) and that physical records should never

be left unattended, when they are not in a secure locked cabinet."

[31] As a result of this investigation, the clinic created and implemented policies and training which are discussed below in greater detail. Polices include a new *Privacy Policy* that addresses how the clinic routinely collects, uses, modifies, discloses, retains or disposes of personal health information, and a *Client Records* policy which specifically addresses measures to be taken to protect the security of client records and the secure disposal of client records.

[32] The new policies were brought to the attention of all staff, and staff were required to submit a written acknowledgement indicating their understanding and willingness to comply with them. Staff also reviewed the *Privacy Policy* at two training sessions. Further, the clinic confirmed that privacy policies and practices would be reviewed with staff "at least once annually."

[33] The clinic's policies were given to each staff member at staff training sessions in October and December 2023. Hardcopies of these policies were made available to staff in the break room and the front desk filing cabinet and an electronic copy is available on the clinic's computer system.

Analysis:

[34] The clinic admitted to failures that constituted a contravention of its obligations under sections 10(1) and 10(2) of the *Act*. Based on my review of the clinic's newly implemented information practices in relation to this matter, discussed in detail below, I am satisfied that reasonable steps have been taken to address the concerns raised in this breach. Overall, I find that the clinic's policies are now adequate.

[35] It is also my opinion that the clinic has implemented an adequate training program for its staff to explain the clinic's privacy and security policies, practices and procedures.

[36] Although at the time of the breach the clinic did not have any written policies, I am satisfied that the clinic is now in compliance with sections 10(1) and 10(2) of the *Act*.

Security:

[37] 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.

[38] Section 13(1) of the *Act* states:

> A health information custodian shall ensure that the records of personal health information that it has in its custody or under its control are retained, transferred and disposed of in a secure manner and in accordance with the prescribed requirements, if any.

[39] As described in PHIPA Decision 50, sections 12(1) and 13(1) of the *Act* impose significant obligations on health information custodians to protect PHI in their custody or control.

[40] PHIPA Decision HO-001 long ago set out the importance of disposing of PHI in a secure manner. That decision noted that: "To guarantee the protection of personal health information, the information must be physically destroyed in an irreversible manner prior to being disposed of, sold or recycled."

[41] During my investigation, the clinic acknowledged deficiencies leading to the disposal of PHI in an unsecured manner. The clinic also recognized that further steps to ensure secure disposal of this information should have been in place.

[42] The clinic noted that prior to this matter coming to the IPC's attention, it had verbally expressed privacy information practices and expectations to staff. These included instructions that patient records should be disposed of in a secure manner (which for physical records included shredding), and that physical records should never be left unattended when not in a secure, locked cabinet.

[43] The clinic acknowledged that at the time of this breach, it had not taken steps that were reasonable under the circumstances to protect against theft, loss, and unauthorized use or disclosure of PHI, and accordingly, that it was not in compliance with section 12(1).

[44] The clinic also recognized that it did not have clearly established written information practices and did not provide staff with adequate training to ensure that staff understood and complied with the clinic's verbally expressed information practices.

[45] Importantly, in response to this breach, the clinic created and implemented several policies including the following:

Privacy Policy

[46] This policy specifically addresses measures to be taken to protect the privacy of patient records. The measures include keeping physical patient records in locked cabinets, ensuring that records removed from cabinets are not left unattended, and ensuring that staff return records to the locked cabinet immediately after using them.

[47] The policy also addresses record retention, responsibility for managing the disposal of client records, the maintenance of a record of destroyed PHI, and contractual obligations vis-à-vis secure disposal when third parties are retained.

[48] With respect to destruction, the policy specifies that:

- The clinic owner/Privacy Officer, is solely responsible for managing the disposal of client records;
- Where a third party is retained to dispose of personal health information, the clinic will enter into a written agreement with the third party that sets out the requirements for secure disposal and requires the third party to confirm in writing that secure disposal has occurred; and
- The clinic will maintain a record of all personal health information that has been destroyed, including:
    - the date,
    - the way the personal health information was disposed of, and
    - the names of the individuals involved in the disposal process.

Client Records Policy

[49] This policy specifically addresses measures to be taken to protect the security of patient records and the secure disposal of such records. This information is contained under two headings: *Storage and Security of Client Records* and *Retention and Destruction of Records of Personal Health Information*.

[50] The *Storage and Security of Client Records* section of this policy contains information on where PHI is to be kept, who will have access to it and reminders about restricting access to passwords and PHI/sensitive information.

[51] The *Retention and Destruction of Records of Personal Health Information* section of this policy contemplates the transfer of PHI, timelines and practices for the destruction of PHI, the training of staff, updates to the policy and consequences for the violation of this policy.

Privacy Training

[52] The clinic stated that the clinic owner conducted one-on-one training with two staff members on April 14 and 17, 2023. The training included the following topics:

- Importance of privacy obligations
- Safeguards and security of records
- Disposal of records

[53] The clinic also advised that the *Client Records* policy was reviewed with all staff in

October 2023, and that all staff were required to submit a written acknowledgment indicating their understanding and willingness to comply with this policy.

[54] The clinic conducted further training on information practices at its year-end business meeting in December 2023. This training session was approximately 45 minutes in length and focused on reviewing the changes to the clinic's revised Office Policies and Procedures, with particular focus on the disposal of PHI.

[55] The clinic confirmed that going forward, privacy policies and practices will be reviewed with staff in June and December yearly. Most recently the clinic completed a review on June 11, 2024. The next review is scheduled for December 2024.

[56] In addition to the policies it created and updated, the clinic has also created a new section in its employee handbook designed to provide staff with additional resources related to its obligations under the *Act*. The resources include a training video regarding the *Act* and a link to the entire statute, links to the IPC's website (including regarding frequently asked questions about the *Act*) and resources from the College of Chiropractors of Ontario, including its *Guidelines for Office Staff* and *Code of Ethics*.

Analysis:

[57] Based on information gathered during my investigation, and by the clinic's own admission, it is my view that at the time of the breach, the clinic had failed to take reasonable steps to ensure the protection of PHI as is required in the *Act*. Specifically, the clinic disposed of the PHI in an unsecured manner when the PHI was torn rather than shredded, and then placed in a bin for disposal, leading to the source retrieving some of this PHI and contacting the IPC.

[58] As noted in PHIPA Decision 102, administrative and technical measures and safeguards are critical to protecting PHI. The IPC has previously stated that, to comply with the requirements in section 12(1) of the *Act* and to take steps that are reasonable in the circumstances to protect PHI, custodians must implement administrative and technical measures or safeguards, including privacy policies, procedures and practices, audit functionality, as well as privacy training and awareness programs and initiatives.

[59] By its own admission, and I agree, the clinic's disposal of PHI in an unsecured manner and the absence of administrative and technical measures to protect PHI, were failures that constituted a contravention of the clinic's obligations under section 12(1) of the *Act*.

[60] In my view, the clinic's lack of measures and safeguards resulted in its failure to ensure that the records of PHI in its custody or under its control were retained and disposed of in a secure manner. Records containing PHI were found in a recycle bin and ended up in a dumpster because they were not disposed of securely. As a result, I find that the clinic did not comply with section 13(1) of the *Act*.

[61] Despite the above, based on my review of the clinic's newly created policies, training material and staff acknowledgment requirements, I am satisfied that reasonable steps have now been taken to bring the clinic into compliance with the requirements of sections 12(1) and 13(1).

Notification to affected individuals:

[62] Section 12(2) of the *Act* states:

> 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.

[63] The duty to notify in section 12(2) of the *Act* applies only where PHI in the custody or control of a custodian is "stolen or lost," or "used or disclosed without authority."

[64] In this matter, the IPC has evidence of records of PHI being disposed of in an unsecured manner. Specifically, as previously noted in this decision, the PHI of several patients was retrieved from the clinic's recycling bin by the source and provided to the IPC. In addition, during my investigation, the clinic confirmed that it was possible that an additional 482 patients' PHI could have been affected. More importantly, the clinic has acknowledged that the unsecured manner of disposal of these records resulted in the loss of PHI, which ultimately ended up outside of its custody and control. Specifically, the clinic stated that it "did not take all steps that were reasonable under the circumstances to protect against theft, loss, and unauthorized use or disclosure of personal health information."

[65] Despite the circumstances that led the IPC to be in possession of the records, at the outset of this investigation the clinic took the position that "The insecure disposal of personal information was a failure to take reasonable steps to protect against the risk of a privacy breach," but that it was not a privacy breach. This position was the result of the clinic's belief that the source had provided all the insecurely disposed of records they observed in the recycling bin to the IPC. Later, the clinic acknowledged that its office manager could not be certain whether the records provided to the IPC were the only records that were disposed of in an unsecured manner, and stated the following:

> It is therefore assumed that insecurely disposed of health records were in a recycling bin and ultimately disposed of by the cleaners in the garbage,

> which is a privacy breach because it is a loss or an unauthorized use or disclosure.

[66] The clinic reviewed its physical patient records and identified 482 additional records as having possibly been disposed of in an unsecured fashion. As a result, the clinic decided to notify these patients of this possibility. The clinic confirmed that it sent notification letters to the last known address of all 482 patients on February 15, 2024.

Analysis:

[67] The language of section 12(2) of *PHIPA* makes clear that the duty to notify arises in the event personal health information in the custody or control of a custodian is stolen or lost, or is used or disclosed without authority.

[68] The clinic acknowledged the fact that patients' PHI ended up in a recycle bin and then a dumpster, and ultimately out of the clinic's custody and control. In addition, as noted earlier, the clinic acknowledged that it: "did not take all steps that were reasonable under the circumstances to protect against theft, loss, and unauthorized use or disclosure of personal health information." In my view, the unsecured disposal of PHI over the period of June – August 2022, constitutes a loss of PHI, triggering the obligation to notify affected individuals, and it therefore is a privacy breach.

[69] The IPC's resource document titled Responding to a Health Privacy Breach: Guidelines for the Health Sector sets out guidance for notifying affected individuals. This document recommends that individuals affected by a breach be provided with the following information:

- the date of the breach;
- the description of the nature and scope of the breach;
- a description of the PHI that was subject to the breach;
- the measures implemented to contain the breach; and
- the name and contact information of the person in [the] organization who can address inquiries.

[70] Based on my review of the initial notification letter that was sent to the affected individuals in December 2023, I am generally satisfied that it contained the recommended information from the guideline, with one exception. I find the third paragraph in the notification letter to have been misleading. This paragraph stated:

> Thankfully, your client records were not in fact recycled by the facility cleaners because an anonymous source noticed the insecure disposal of the

> records and reported their concerns to the Information and Privacy Commissioner.

[71] In my view, this statement omitted important details and misrepresented what happened. It also minimized the transgression that occurred. I did not find this language satisfactory or in keeping with the seriousness of the requirement to notify those affected by the breach; I do not have the same concern about the notification letter that was sent to the 482 patients in February 2024 as the statement above was omitted.

[72] However, given that later in this investigation the clinic acknowledged the privacy breach resulting from health records being disposed of in an unsecured manner in a recycling bin, and ultimately disposed of by cleaners in the garbage, the clinic proposed to send a corrected notice to the affected patients (clarifying that it is possible that their insecurely disposed of client health records were picked up by facility cleaners). Consequently, I am satisfied that the duty to notify was ultimately fulfilled.

[73] Finally, I want to comment on the legislated requirement to notify affected parties "at the first reasonable opportunity." This breach occurred in August 2022. The clinic was made aware of the loss of its patients' PHI in March 2023. The affected individuals were not notified until December 2023 and February 2024. Therefore, the clinic took over 9 months to notify affected parties.

[74] The IPC notified the clinic via letter on March 3, 2023, of allegations of improper retention, destruction, and disposal of personal health information. In my view, had the clinic acted more expeditiously, the affected individuals could have been notified much sooner.

[75] Despite the considerations noted above, I am satisfied that the clinic did provide the notification required by section 12(2) of the *Act*, although it should have done so much sooner.

[76] I take note of the regret expressed by the clinic about not acting expeditiously when informed of the possible breach. I am also mindful of the acknowledgment that the unsecured disposal was a loss or an unauthorized use or disclosure, and that at the time that this event occurred, the clinic did not have appropriate information practices and policies in place, nor staff training, to adequately safeguard PHI. Finally, I recognize that the clinic cooperated fully with this investigation.

[77] In conclusion, I am of the view that the clinic has responded adequately to the breach.

NO ORDER:

In accordance with my delegated authority under the *Act*, and for the reasons set out above, this review will be concluded without proceeding to the adjudication stage and without an order being issued by the IPC.

Original Signed by: November 22, 2024

Alexandra Madolciu
Investigator