Information and Privacy Commissioner,
Ontario, Canada

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

PHIPA DECISION 287

Complaint HR21-00463

Algonquin Family Health Team

June 27, 2025

Summary: Algonquin Family Health Team (AFHT) reported a breach of its patients' privacy under the *Personal Health Information Protection Act* relating to messages sent within its electronic medical records (EMR) system. The AFHT found that in cases where a health care provider sent a prescription via the EMR's prescription messaging system and the message could not be delivered, the EMR messaged all users of the shared EMR who had elevated privileges. These messages included the patient's name and other personal health information.

The AFHT was not able to resolve the issue on its own. The AFHT had purchased the prescription messaging feature through its EMR provider and for some time, was neither able to contact the messaging system vendor directly nor obtain assistance from the EMR provider on this matter. Eventually, the AFHT, the EMR provider, and the messaging system vendor were able to discuss the issue and obtain a software fix, which the family health team successfully implemented.

In this decision, the adjudicator finds that the email broadcasts of the non-delivery alert messages were disclosures of personal health information that were not authorized under the *Act*. The adjudicator also finds that the family health team has taken reasonable steps to address the breaches, largely through measures preventing similar broadcasts occurring in future. The adjudicator finds that the AFHT did not provide notice to the affected patients as required under section 12(2) of the *Act* and orders the AFHT to provide this notice within six months of the date of this decision.

Statutes Considered: *Personal Health Information Protection Act, 2004, c*. 3; Sched. A., sections 1, 2, 3(1), 4(1), 12(1), 12(2), 29, 37(1)(a), 38(1)(a) and 58(1).

OVERVIEW:

[1] This decision sets out my findings following my review under section 58(1) of the *Personal Health Information Protection Act, 2004* (*PHIPA* or the *Act*) of privacy breach incidents reported to this office by Algonquin Family Health Team (AFHT). These incidents arose from the AFHT's electronic medical records (EMR) system broadcasting messages that include personal health information to users of the shared EMR system, some of whom were not authorized to access that personal health information. The AFHT reported its concerns that, because of these broadcasts, users had viewed patients' personal health information in contravention of *PHIPA*.

[2] Under section 58(1) of *PHIPA*, the Information and Privacy Commissioner of Ontario (the IPC) may, on its own initiative, conduct a review of any matter if it has reasonable grounds to believe that a *PHIPA* provision has been contravened or is about to be contravened.

[3] The AFHT and a related clinic, Lakeview Physicians, identified three separate issues resulting in breaches of *PHIPA* and reported all three to the IPC. While all three of these breaches involved the shared EMR system in some way, the circumstances and causes of each of the breaches are distinct, so the IPC opened three separate files to address these matters. This decision addresses only the first of these files; the other files will be addressed in subsequent decisions.

[4] In this decision, I find that the email broadcasts of the non-delivery alert messages were disclosures of personal health information that were not authorized under the *Act*. I find that the family health team has since taken reasonable steps to address the breaches. Finally, I find that the family health team did not provide notice to the affected patients as required under section 12(2) of the *Act* and order the family health team to provide this notice within six months of the date of this decision.

BACKGROUND:

EMR System

[5] The AFHT uses a shared EMR system obtained from a third-party provider (the EMR provider). This EMR is shared with all family doctors in Huntsville, Ontario, where the AFHT is located. The shared EMR has over 140 users over 13 locations. Of these, 31 users have "administrator" privileges. This means that these users have access to more functions within the EMR than a typical user would have, for information technology or other administrative purposes.

[6] The AFHT also uses PrescribeIT, an electronic prescribing system provided by Canada Health Infoway (Infoway). The AFHT uses this system to send prescriptions from participating healthcare providers to participating pharmacies via the EMR. The EMR

provider offers PrescribeIT as an "add on" to the EMR, which is how the AFHT obtained the use of this prescribing service. The EMR provider set up the PrescribeIT software for the AFHT and functioned as the point of contact for all software issues relating to the EMR, including those relating to PrescribeIT. The contract that the AFHT provided covering its use of the PrescribeIT services was a copy of a standard Canada Health Infoway "Personal Information Sharing Agreement," (the contract) which was neither filled in nor signed by either party.

Circumstances of the Breach

[7] The AFHT contacted the IPC to advise it of a privacy breach related to the use of the PrescribeIT feature. Sometimes when providers send prescriptions within the EMR via PrescribeIT, these prescriptions cannot be delivered to the intended recipient. In such cases, a single message should be sent to the prescriber to alert them that their message could not be delivered. However, the AFHT found that what was instead happening was that these non-delivery alert messages were being sent to all users of the shared EMR who had administrative privileges within that system. Because the EMR was shared with other clinics, this included users outside the AFHT with administrative privileges to the shared EMR.

[8] The AFHT states that these non-delivery alert messages include the patient's name and the medication prescribed. They may also include other information, such as communicating that the prescription has been faxed or that the healthcare provider instead must contact the pharmacy directly. The AFHT reported this as a breach to the IPC because the EMR was sending personal health information to those who did not have authority under the *Act* to access the individuals' personal health information.

[9] In addition, the non-delivery alert messages do not state who the prescribing healthcare provider is, so the recipient cannot just forward the message to that provider. Instead, the recipient forwards the message to a privacy officer. This privacy officer then reviews the patient's demographics screen to determine the who the healthcare provider is and forwards the message accordingly.

[10] This redirection process requires that, to direct the message appropriately, recipients must view the personal health information within the messages. However, the messages are sent to all users with administrative privileges, and not all recipients have authority under the *Act* to access this personal health information.

[11] The AFHT states that they identified over 400 messages that were broadcast to those with administrative privileges because they could not be delivered to the intended recipient. These broadcasts were ongoing when the AFHT first contacted the IPC, and through most of the life of this file.

Attempts to Stop Further Broadcasts

[12] The AFHT advised the IPC that the broadcasts were due to a software feature that

it had no control over. The AFHT states that analyzing the software required a level of access to the software that it did not have.

[13] As it could not resolve this issue on its own, the AFHT contacted its EMR provider in an attempt to resolve the message broadcast issue. The AFHT states that it did not have a direct relationship with Infoway, as the EMR provider was its contact point for the PrescribeIT feature. The AFHT therefore asked the EMR provider to determine if there was a way to prevent these alert messages from being broadcast to all those who had administrative privileges to the shared EMR.

[14] The AFHT reported that the EMR provider's view of the issue was that administrators have special privileges and are therefore permitted to view messages. As such, the EMR provider did not view these message broadcasts as a problem and did not assist the AFHT in resolving the matter. The AFHT states that it did not have a contact at Infoway, so was not able to reach out to Infoway directly to try to resolve the matter.

[15] The AFHT states that it explored some options on its own to resolve the broadcasting issue. In particular, it looked at ways that it could reduce the number of message recipients, given that it could not address the broadcasts themselves.

[16] The AFHT determined that the administrator accounts that the alert messages were being sent to were largely held by individuals in positions such as IT/Privacy Officer, Office Manager, and Quality Improvement Decision Support Specialist, as well as some general support accounts and backup accounts. These are positions that require elevated privileges beyond those available to typical users in order to perform IT or other administrative tasks, such as assigning patients to a patient or making changes for other users. Removing administrator privileges from these accounts would hinder those employees' abilities to perform certain job functions. As such, removing administrative privileges was not a feasible way of reducing the scope of the privacy breaches.

[17] The AFHT also explored creating a rule that would limit who the non-delivery alert messages were broadcast to. They found that the EMR messaging system that sends the messages does not have the ability to create this type of rule for the distribution of the messages.

[18] During the investigation of this privacy breach, the AFHT stated that it was planning on implementing new software that it expected would resolve the broadcast issue. However, it did not have a firm timeline for when this software would be put in place.

[19] At the conclusion of the IPC's investigation, there remained a number of unresolved issues in this file, including whether the AFHT had reasonable measures in place to ensure that the personal health information in its custody was protected from unauthorized use, and whether notice of the privacy breaches had been provided in accordance with *PHIPA*. Given this, the file was transferred from the investigation stage

to the adjudication stage of the IPC's process.

[20] The adjudicator assigned to the file decided that there were reasonable grounds to conduct a review of this matter under section 58(1) of *PHIPA*. As part of his review, the adjudicator sought and received representations on the issues at hand from the AFHT. The AFHT also provided a later update addressing a software fix. The file was then transferred to me. I asked the AFHT for a further update, regarding the extent of the software fix and the timeline for the implementation of the new software.

[21] In the discussion that follows:

- I review the family health team's efforts to stop or limit the broadcast of the non-delivery alert messages;
- I review the the family health team's contractual provisions with the vendor of the prescription messaging feature;
- I recommend that for any future service providers that it contracts with, the family health team ensures that it not only have adequate contractual terms, but also the means to enforce these terms, including identifying the appropriate point of contact to reach out to for contractual matters or ensuring that it has a way to escalate its concerns if it obtains such services via a go-between;
- I find that the email broadcasts of the non-delivery alert messages were disclosures of personal health information that were not authorized under the *Act*;
- I find that the family health team has since taken reasonable steps to address the breaches, largely through measures preventing similar broadcasts occurring in future;
- I find that the family health team did not provide notice of the unauthorized disclosure of personal health information to the affected patients as required under section 12(2) of the *Act*;
- I order the family health team to provide notice of the unauthorized disclosure of personal health information to the affected individuals within six months; and
- I order the family health team to provide this office with proof of compliance with the order provision requiring notice, in the form of an affidavit, within six months.

DISCUSSION:

[22] *PHIPA* sets out rules for the collection, use, and disclosure of personal health information to protect the confidentiality of that information and the privacy of the individuals to whom that information relates, while at the same time facilitating the

effective provision of health care (section 1). *PHIPA* achieves these purposes by, among other things, imposing duties on health information custodians to protect personal health information in their custody or control, and by establishing independent oversight powers of the IPC to address contraventions or potential contraventions of *PHIPA*.

[23] The AFHT does not dispute, and I find, that:

- the information at issue contains "personal health information" as that term is defined within section 4(1) of *PHIPA*; and
- the AFHT is a "health information custodian" pursuant to section 3(1) of *PHIPA*.

Duty to Protect Personal Health Information

AFHT has a duty to take reasonable steps to protect personal health information it holds from unauthorized disclosure

[24] *PHIPA* requires health information custodians to protect personal health information in their custody or control. This includes protecting this personal health information from unauthorized use or disclosure. Section 12(1) of *PHIPA* 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.

[25] The duty to take reasonable steps to protect personal health information includes a duty to respond adequately to a complaint of a privacy breach. Among other things, a proper response will help ensure that any breach is contained and will not re-occur.[1]

[26] Part IV of *PHIPA* sets out the regime for collection, use and disclosure of personal health information. Under section 29 of *PHIPA*[2], a health information shall not use or disclose personal health information without an individual's consent, unless that use or disclosure is permitted or required by *PHIPA*. Permitted uses are set out in section 37, while permitted disclosures are enumerated later in Part IV of *PHIPA*.

---

[1] PHIPA Decision 44, at para 140. See also PHIPA Decisions 69, 70, 74, and 80.

[2] Section 29 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.

[27] Under section 37(1)(a)[3], health information custodians may use personal health information "for the purpose for which the information was collected or created and for all the functions reasonably necessary for carrying out that purpose." This will often be for the purpose of providing health care to that individual. Similarly, section 38(1)(a)[4] authorizes a health information custodian to disclose personal health information to another health care provider "if the disclosure is reasonably necessary for the provision of health care and it is not reasonably possible to obtain the individual's consent in a timely manner." The group of providers who may rely on the implied consent of the patient to collect, use, or disclose their personal health information for health care purposes is commonly referred to as the patient's "circle of care."

[28] The term "disclose" is defined under section 2 of the *Act* as:

> "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

[29] Generally, when messages are sent within the EMR using PrescribeIT, they are sent from the prescribing health care provider to the patient's pharmacist, both of whom are within the patient's circle of care. However, when a message cannot be delivered to the intended recipient, the non-delivery alert messages are broadcast to all users of the shared EMR who have administrative privileges. Most of the message recipients will not be within the patient's circle of care. The result is that personal health information is sent outside of the patient's circle of care, to those who do not have authority under *PHIPA* to collect, use, or disclose that personal information.

[30] There is nothing before me to indicate that the AFHT or its agents intended to send personal health information outside of the affected patients' circles of care. Rather, this occurred because of a feature of the software that AFHT uses to communicate

---

[3] Section 37(1)(a) states:

> 37 (1) A health information custodian may use personal health information about an individual,
>
> (a) for the purpose for which the information was collected or created and for all the functions reasonably necessary for carrying out that purpose, but not if the information was collected with the consent of the individual or under clause 36 (1) (b) and the individual expressly instructs otherwise;

[4] Section 38(1)(a) states:

> 38 (1) A health information custodian may disclose personal health information about an individual,
>
> (a) to a health information custodian described in paragraph 1, 3 or 4 of the definition of "health information custodian" in subsection 3 (1), if the disclosure is reasonably necessary for the provision of health care and it is not reasonably possible to obtain the individual's consent in a timely manner, but not if the individual has expressly instructed the custodian not to make the disclosure;

prescriptions within its shared EMR. However, disclosure of personal health information does not require the intention to do so;[5] it can occur inadvertently.

[31] In this case, personal health information was sent from prescribers, who were agents of AFHT, to shared EMR users. This meets the definition of disclosure, which includes a health information custodian either making the information available or releasing it. Accordingly, I find that the sending of the non-delivery alert messages were disclosures of personal health information.

[32] Section 29 of the *Act* states that a health information custodian shall not collect, use, or disclose an individual's personal health information without their consent, unless that collection, use, or disclosure is permitted or required by the *Act*. The AFHT has not claimed that it had authority under the *Act* to send the patients' personal health information to recipients not within the circle of care and does not dispute that the disclosures were unauthorized under the *Act*. I find that the broadcasts of the non-delivery alert messages containing patient personal health information were disclosures of personal health information contrary to section 29 of the *Act*.

[33] Having found that there were disclosures of personal health information in contravention of *PHIPA*, I must consider the circumstances that may have contributed to these breaches and the steps taken by the AFHT to address them. This is required in order to determine if the AFHT has met its duty to take reasonable steps to protect personal health information it holds from unauthorized disclosure. This includes reviewing the contractual measures that the AFHT had in place with Infoway, the provider of PrescribeIT, to protect patients' personal health information.

Contractual safeguards

[34] As noted above, the AFHT uses the PrescribeIT service provided by Infoway to send prescriptions from prescribers to patients' pharmacists. The AFHT indicated that its EMR provider functioned as the go-between in the relationship between AFHT and Infoway. However, the AFHT was able to supply the IPC with a copy of an Infoway contract, when asked to provide this office with a copy of the agreement they had with Infoway.

[35] As noted, the contract is called "Personal Information Sharing Agreement" and is not completed or signed. The contract appears to be a standard version provided by Infoway. However, the terms of the contract are still relevant in outlining the rights and obligations of the parties.

[36] The contract begins with a preamble, which forms part of the agreement between the parties.[6] This preamble acknowledges that both parties wish to uphold individuals'

---

[5] For a discussion of disclosure not requiring intentionality, see PHIPA Decision 255, paragraphs 28-32.
[6] Section 15.12 of the contract states that "[the] preamble shall govern and form an integral part of this Agreement."

privacy and access rights. It recognizes that the custodian is a health information custodian under *PHIPA*, with the associated obligations to protect "patient personal information"[7] and further states that "Infoway has obligations to protect [personal health information] on the Custodian's behalf." The preamble explicitly sets out that, under *PHIPA*, custodians need to ensure that service providers they contract with have appropriate safeguards in place, stating as follows:

> In providing the Services, PHIPA requires Infoway to enter into a written agreement with the Custodian concerning the services provided to the Custodian that: (i) describes the Services; (ii) describes the administrative, technical, and physical safeguards relating to the confidentiality and security of personal health information involved in the Services; and (iii) requires Infoway to comply PHIPA (the "Service Agreement").

[37] The contract then goes on to set out the terms agreed to, which explicitly include compliance with *PHIPA*. Under those terms, Infoway shall only use and share personal health information to provide the services, unless otherwise authorized or required or permitted by law.

[38] The contract further addresses the safeguards by requiring both parties to notify the other of "any suspected or actual compromise in the protection of [personal health information]." It also states that both parties are required to "reasonably cooperate in any subsequent investigation or resolution."

[39] The "Compliance Challenges" term of the contract includes an obligation that "Infoway shall assist the Custodian in timely response to challenges regarding the privacy-respectful use of PrescribeIT by the Custodian…" It also requires both parties to "reasonable cooperate" in any investigations stemming from "challenges regarding the privacy-respectful use of PrescribeIT by the Custodian or the privacy-respectfulness of PrescribeIT."

[40] Furthermore, the contract also includes an "Answering Questions" term stating that "[each] party shall reasonably cooperate in any investigations arising from challenges regarding the privacy-respectful use of PrescribeIT by the Custodian or the privacy-respectfulness of PrescribeIT."

---

[7] The contract uses the terms "Patient Information" and "Patient Personal Information", both of which include personal health information. In the preamble, "Patient Personal Information" is defined to include personal health information, and "Patient Information" is in turn defined as including "Patient Information" and therefore, personal health information, per the following provision:

> Provision of the Services requires (a) the Custodian to provide the personal information of clinical end users to Infoway ("End User Personal Information") and (b) the provision of personal information, including personal health information, of the Custodian's patients to PrescribeIT in order to share the personal health information of patients within the circle of care ("Patient Personal Information"). Together, End User Personal Information and Patient Personal Information constitute the "Personal Information".

[41] Finally, Schedule B to the contract sets out administrative and technical safeguards that Infoway will use to protect the personal information.

[42] The contract has provisions that appear to address situations such as the one that occurred in this case. The contract recognizes that the custodian (in this case, AFHT) has obligations to protect personal health information, and that Infoway, as the provider of services to the AFHT, is required to comply with *PHIPA*. Infoway has a contractual obligation to assist AFHT if it experiences challenges with the "privacy-respectful use of PrescribeIT by [AFHT]." Moreover, Infoway is also obligated to reasonably cooperate in any investigations relating to such challenges. Based on my review of the contract, it appears that AFHT and Infoway had arrangements in place to address privacy breaches arising from the use of PrescribeIT, such as the broadcasting of personal health information to those not authorized to receive it.

[43] Despite the terms of the contract, the AFHT was not able to address the issue of the broadcast messages until September 2024, nearly three years after it first identified the issue. During this time, the AFHT tried to stop the broadcasts from happening or limit the number of people who received these broadcast messages, but were not able to do so. I will next address what the AFHT tried, why their attempts were not successful, and what led to the AFHT eventually fixing the issue of the ongoing privacy breaches.

Measures to stop broadcasts of non-delivery alerts

[44] As discussed, a health information custodian is obliged under section 12 of the *Act* to take steps that are reasonable in the circumstances to ensure that personal health information in its custody or control is protected against unauthorized use or disclosure. In this case, unauthorized disclosures of personal health information were occurring due to a malfunction of software that AFHT was using to send out prescriptions.

[45] From the evidence before me, it is clear that the AFHT did not anticipate disclosures of this nature happening, and that the AFHT tried to prevent future occurrences when they found out about the broadcasts. The AFHT explored options to limit the number of recipients of these emails, such as putting in place message rules or limiting the number of users with administrative privileges, but found that neither of those options could be put in place. The AFHT also contacted its EMR provider, who had set up both the shared EMR and the PrescribeIT add-on service for them.

[46] According to the AFHT, they found that, at least initially, the EMR provider did not view the messages being broadcast to administrative users of the shared EMR as a privacy issue, because the messages were being sent to users with increased privileges. It appears that the EMR provider's view was that these users were permitted to view or receive the personal health information, based on their additional privileges within the EMR system.

[47] The AFHT stated that they did not have a contact at Infoway that they could raise

their concerns with directly. Without getting assistance from Infoway or the EMR provider, and with their own attempted solutions proving ineffective, the AFHT was unable to stop the broadcasts, unless it stopped using PrescribeIT entirely. The AFHT provided instructions to its administrators to ignore and delete the non-delivery alert messages or forward them to the privacy officer, but these measures contained the disclosures, rather than preventing them. During the time that AFHT was looking for a solution to the broadcast issue, the AFHT continued to disclose personal health information contrary to the *Act*, despite their wish not to do so.

[48] This was addressed by the AFHT during the investigation stage of this complaint. At that time, the AFHT informed the IPC that it had identified a contact person at Infoway and scheduled a meeting between representatives of the AFHT, Infoway, and the EMR provider to attempt to address this issue. Following this meeting, the AFHT reported that they had identified a potential fix. This fix was implemented in September 2024. The AFHT later confirmed that non-delivery alert messages were no longer being broadcast to users of the shared EMR with administrative privileges.

[49] In addition, the AFHT also stated that the EMR provider acquired new software and would be migrating existing users to that new software at some point. The AFHT later reported that early in 2025, the EMR provider advised them that this software was ready. Given that the AFHT's last software migration took 7-8 months, they expect that the software would be in place late in 2025.

[50] Having reviewed the AFHT's efforts throughout, as well as the results of the software fix, I am satisfied that the AFHT took adequate steps to address the unauthorized disclosures of personal health information. After the AFHT was able to work with Infoway and the EMR provider to identify a fix to the software issue, they implemented this fix and confirmed that it worked to prevent similar disclosures from occurring. In addition, the AFHT is taking the additional step of migrating to new software that would not have the same broadcast issue.

[51] However, I note that significant time elapsed between the AFHT identifying the issue of the broadcast disclosures and being able to identify and implement a solution. During this period of nearly three years, over three hundred non-delivery alerts were broadcast, resulting in disclosures of patient personal health information contrary to *PHIPA*. These occurred despite a contract between the AFHT and Infoway that mandated Infoway to assist the AFHT in investigating privacy issues related to the operation of its software.

[52] At least some portion of this time appears to be related to the EMR provider's misunderstanding of the *PHIPA* obligations that the AFHT is subject to. Based on the information provided by the AFHT, the EMR provider appeared to conflate additional administrative privileges within the EMR system with additional authority to collect, use, or disclose personal health information under *PHIPA*. However, granting additional privileges is an administrative matter determined within a clinic; it does not confer any

additional authority to collect, use, or disclose personal health information under the *Act*.

[53] In addition, when the AFHT considered approaching Infoway directly, they were unable to do so for some time, as they could not identify a contact person to reach out to. The AFHT subscribed to the PrescribeIT services but did so through the EMR provider. Thus, despite contractual provisions with Infoway that obliged Infoway to participate in investigations of privacy concerns, the AFHT was not able to exercise its rights because it was not able to contact Infoway about those concerns.

[54] Under section 12(1), the AFHT has an obligation to take steps that are reasonable in the circumstances to ensure that personal health information in its custody or control is protected against unauthorized use or disclosure. This includes taking steps to ensure that service providers it engages with have adequate protections in place to protect against unauthorized uses or disclosures. In this case, the contractual terms adequately addressed security obligations. However, to enforce these terms, the AFHT needed to have a way to communicate with Infoway, either directly or through an EMR provider who was willing to facilitate enforcement of the contract. Neither avenue was available to the AFHT until long after the AFHT had identified the non-delivery alert broadcasts as a problem and tried to obtain assistance from its EMR provider regarding this matter.

[55] This has since been rectified, and I understand that the AFHT, Infoway, and the EMR provider have now worked together to arrive at a solution. I am satisfied that the steps taken to fix the broadcast error are reasonable to ensure that the personal health information in the AFHT's custody or control is protected against unauthorized use or disclosure. However, I recommend that for any future service providers that it contracts with, the AFHT ensures that it not only have adequate contractual terms, but also the means to enforce these terms. That may include ensuring that service providers identify the appropriate point of contact to reach out to for contractual matters or ensuring that it has a way to escalate its concerns if it obtains such services via a go-between.

Notification

[56] Section 12(2) of *PHIPA* mandates that individuals be notified if their personal information is used or disclosed without authority, stating:

> Subject to [a subsection of *PHIPA* that does not apply in the circumstances of this review] 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.

[57] During the investigation stage of the complaint, the AFHT stated that it had not provided notice to patients of the unauthorized disclosures. This was due to the AFHT's misconception of when notification is required under the *Act*. The AFHT stated that its understanding was that notification was required in cases where an individual accessed personal health information when they should have known they were not authorized to do so. Because the broadcasting of non-delivery alerts did not involve such instances, the AFHT did not realize that they needed to provide notification to patients regarding the unauthorized disclosures of personal health information.

[58] After corresponding with the investigator regarding notification, the AFHT committed to notifying the affected individuals, but stated that it had to determine both the appropriate means of providing notice and the patients affected.

[59] The AFHT was able to see which messages had been sent out via the broadcasts, as all such messages had the same subject line. From these, the AFHT was able to identify the patients whose personal health information had been disclosed via these broadcasts. This was done for the broadcasts that occurred before and after the AFHT reported the first breaches to the IPC.

[60] During the adjudication of this complaint, the AFHT reported that it had drafted notices to the patients affected by the earlier breaches. The AFHT provided the managers of the offices involved with a mail merge so that the individual office could then send these out to their patients via email.[8]

[61] When asked if all patients had been notified, the AFHT was not able to confirm all notifications had occurred. The AFHT reported that one office put a note into patients' charts and is notifying the affected patients when they come in for appointments. One office reported that it was not sure whether it had notified the affected patients. One office no longer exists, though the AFHT was reaching out the to the doctor in that clinic (who is no longer practicing in Ontario) about notification. Finally, the fourth office did not respond to the privacy officer's question about notification at all.

[62] For broadcasts that occurred after the AFHT committed to notifying the patients affected, the AFHT put in place the following process. The AFHT forwarded the broadcast email to the appropriate administrator, with a covering email. The AFHT's covering email notified the administrator that the forwarded message had been broadcast to all administrators, rather than just to the prescriber, and stated that the patient should be notified of the email broadcast. The AFHT also stipulated the information that should be included in the notification email to the patient, and provided instructions about what the

[8] The AFHT also noted that these individual offices could choose to notify affected patients in another way. For example, one office planned to telephone the patients to notify them of the breaches, rather than emailing them.

local office should tell the patient about the nature and scope of the breach.[9]

[63] The requirement set out in section 12(2) of *PHIPA* is to "notify the individual at the first reasonable opportunity of the theft or loss or of the unauthorized use or disclosure." For more recent broadcasts – those occurring since the AFHT committed to notifying the patients affected – the AFHT put a process in place under which it instructed the local offices to send out the notifications shortly after the broadcasts occurred. However, the AFHT provided these instructions over two years after the first broadcasts occurred. This delay in notification does not adhere to the requirement to provide notice of unauthorized use at the first reasonable opportunity.

[64] Moreover, it appears that, despite the AFHT's instructions, only one of its four offices notified affected patients of the earlier unauthorized disclosures. As such, I find that the AFHT did not comply with the section 12(2) requirement to notify affected individuals at the first reasonable opportunity of the unauthorized disclosure of their personal health information.

[65] I therefore order the AFHT to provide notice of the unauthorized disclosure of personal health information to all affected individuals as soon as possible, but no later than six months after the date of this order. I also order the AFHT to provide this office with proof of their compliance with this order, in the form of an affidavit that is to be provided to this office within six months of the date of this order.

[66] With this order, I conclude the review.

ORDER:

For the foregoing reasons, pursuant to section 61(1) of the *Act*:

1. I order that the AFHT provide notice of the unauthorized disclosure of personal health information to all affected individuals in accordance with section 12(2) of the *Act* as soon as possible, but no later than six months after the date of this order.

[9] Among other things, AFHT stated that the notification to patients should include an estimate of how many people saw the patient's name, what medication was listed in the message, and how long between the time that the message was delivered and when it was first forwarded to the appropriate administrator. Patients were to be told that this is a software issue that the AFHT was working to address. The AFHT also stated that the message should provide a name and number of someone in the patient's local AFHT office that patients may contact about their concerns, as well as informing the patient of their right to make a complaint to the IPC. Finally, the AFHT's email to its local offices advised that if the patient wants additional details, they can direct these concerns to the AFHT's privacy officer.

2. I order that the AFHT provide this office with proof of compliance with order provision 1, in the form of an affidavit, no later than six months after the date of this order.

Original Signed by: June 27, 2025

Jennifer Olijnyk
Adjudicator