Information and Privacy Commissioner,
Ontario, Canada

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

PHIPA DECISION 260

Complaint HR23-00157

[a public hospital]

October 16, 2024

Summary: A public hospital contacted the Information and Privacy Commissioner of Ontario to report a breach under the *Personal Health Information Protection Act* (the *Act*). The breach involved an unauthorized use of personal health information of patients by a physician. In response to the breach, the hospital updated its privacy training, confidentiality agreements and privacy policies. In this Decision, I find that the hospital was in breach of sections 10 (Information practices) and 12 (Security) of the *Act*. However, given the steps taken by the hospital to address the breach, I have also found that no formal review of this matter will be conducted under Part VI of the *Act*.

Statutes Considered: *Personal Health Information Protection Act, 2004, S.O. 2004, c. 3;*

INTRODUCTION:

[1] On April 14, 2023, a public hospital (the hospital) notified the Information and Privacy Commissioner of Ontario (the IPC) of a breach under the *Personal Health Information Protection Act* (the *Act* or *PHIPA*) of unauthorized accesses by a physician.

[2] The IPC opened complaint HR23-00157 to address this matter.

[3] During the early resolution stage of this complaint, the hospital provided details of its response to the breach. After a review of the hospital's responses by the IPC, the file was moved to the investigation stage of the IPC's *PHIPA* complaint process, and I was assigned as the investigator. As part of my investigation, I requested and received written

representations from the hospital.

[4] In this decision, I find that at the time of the breach, the hospital was in violation of the *Act*. However, in light of the steps taken by the hospital to address the privacy concerns identified, I am satisfied that the hospital now has adequate measures in place to comply with sections 10 (Information practices) and 12 (Security) of the *Act*, and no review is warranted under the *Act.*

BACKGROUND:

[5] On June 2, 2022, the hospital was alerted to suspicious activity in one of its patient charts by a doctor working in the emergency department. The doctor had identified a blank note in a patient chart by another doctor (the physician) who was not working on that date.

[6] The hospital initiated an investigation into the matter which included a targeted audit. This audit revealed that the physician had made approximately 60,000 entries per month into the hospital's electronic medical record. The hospital required further review to determine if there were unauthorized accesses. Due to the voluminous amount of data, a six-week audit was completed to determine the scope of the potential breach. The hospital reviewed the results of the narrowed audit and compared that information to the physician's shifts and visit volumes. After this review, the hospital estimated that there could be unauthorized accesses of approximately 1400 patients and that the unauthorized accesses were from a remote device using the organization's Virtual Private Network.

[7] The hospital initiated its privacy breach process and notified the chief of staff and department chief who spoke with the physician directly about the accesses.

[8] While the hospital proceeded to conduct a full audit on the physician's accesses, weekly audits of the physician's access were completed to ensure the breach had been contained.

[9] The hospital conducted a full audit for the period of December 3, 2021-August 14, 2022 (prior to December 3, 2021, the physician did not have remote access to the electronic health record). The hospital's investigation determined that accesses were mainly limited to the emergency department where the physician worked. The physician had accessed various sections of the emergency department chart such as triage notes, diagnostic reports, and laboratory results.

[10] At the conclusion of their investigation, the hospital determined that 3928 patient charts had been accessed by the physician without authorization and that all the unauthorized accesses were completed from a remote workstation outside of work hours in respect of patients who were not under the physician's care.

[11] The physician admitted to accessing the electronic health record for "educational

purposes." The physician explained that he thought accessing the electronic health records of patients remotely for this purpose was authorized. He was informed that was not the case and educated as to why. According to the hospital, the physician understood, acknowledged his error, and recognized he was wrong. In addition, the physician apologized, took responsibility for his actions, showed remorse, and committed immediately to stopping that type of access. The hospital explained that this physician had recently moved to Ontario in the middle of the COVID-19 pandemic to start working at the hospital, devoting himself to his department. The hospital advised that the chief of the emergency department found that the physician's explanation and apology were sincere.

[12] Based on the results of the audits, the physician's interview responses, a written statement by the physician and discussions with affected parties who contacted the hospital in response to receiving the notification letter, the hospital determined that the physician did not have a personal affiliation with any of the affected parties and there was no evidence of malicious intent. Although the hospital identified that some records accessed were of hospital staff or their family, the hospital determined through its investigation that the physician "did not or may not have known" that. The physician did not access records of hospital staff with whom he worked directly or had a close affiliation.

[13] The hospital advised that the physician did not access any records belonging to patients with the same last name or any other relevant information that would indicate a personal connection.

[14] The hospital's position is that the audit determined that accesses were not targeted and occurred on the date the patient was seen in the emergency department. The physician did not search specifically for a patient's information and had selected patients from a list of patients who visited the emergency department.

[15] Following its investigation and discussion with the physician, the hospital continued to audit the physicians' accesses on an ongoing basis. This ongoing auditing showed that the physician was no longer accessing records for patients for whom he did not provide care.

[16] In addition, the hospital reported that there was no evidence of inappropriate disclosure or unauthorized access after this issue was raised with the physician. The hospital also considered the fact that the physician had no prior conduct issues. Given the above, the hospital did not suspend the physician's privileges. The hospital was also of the view that a suspension would have seriously reduced the hospital's ability to provide care to its community.

[17] The physician's unauthorized uses were brought for consideration before the hospital's medical advisory committee, which is the body made up of the hospital's physician leaders that makes recommendations to the hospital's board of directors on matters of physician privileges. After discussion and deliberation, the medical advisory

committee recommended that the physician attend privacy training and that a revocation or suspension of the physician's privileges was not warranted. The hospital's board of directors accepted the recommendation.

PRELIMINARY ISSUES:

[18] The hospital does not dispute, and I find that the hospital is a "health information custodian" within the meaning of section 3(1) of the *Act* and the physician is an agent within the meaning of section 2 of the *Act*.

[19] Further, there is no dispute, and I find that the information at issue is personal health information pursuant to section 4 of the *Act* and that the accesses in question are "uses" of personal health information within the meaning of the *Act*.

ISSUES:

[20] This decision addresses the following issues:

1. Did the hospital have and comply with information practices and take steps that were reasonable in the circumstances to protect personal health information in accordance with the *Act*?

2. Is a review warranted under Part VI of the *Act*?

RESULTS OF THE INVESTIGATION:

Issue 1: Did the hospital have and comply with information practices and take steps that were reasonable in the circumstances to protect personal health information in accordance with the *Act*?

[21] In response to this breach, the hospital identified the scope of the breaches through its auditing capabilities and processes. This breach raised concerns about the hospital's policies that address training, confidentiality agreements and notification, as well as compliance with these policies.

[22] My analysis below focuses on these concerns, the steps the hospital took to remediate the breach, and the policies and practices in place to protect the personal health information of patients as required under sections 10 and 12 of the *Act*.

[23] The *Act* requires that health information custodians have in place, and comply with, information practices that protect personal health information in their custody and control, including administrative, technical, and physical safeguards.

[24] 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.

[25] Section 10(2) of the *Act* states:

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

[26] Section 2 of the *Act* defines information practices as follows:

> "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;

[27] The *Act* also requires health information custodians take "reasonable" steps to protect personal health information in their custody and control against unauthorized use or disclosure, among other things. Specifically, sections 12(1) and 12(2) of the *Act* states:

1. 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.

2. Subject to subsection (4) and to the exceptions and additional requirements, if any, that are prescribed, if personal health information about an individual that is in the custody or control of a health information custodian is stolen or lost or if it is used or disclosed without authority, the health information custodian shall,

   a. notify the individual at the first reasonable opportunity of the theft or loss or of the unauthorized use or disclosure; and

   b. include in the notice a statement that the individual is entitled to make a complaint to the Commissioner under Part VI.

[28] As part of my investigation, I examined the hospital's privacy policies, training, confidentiality agreements, and notification requirements against the obligations in

sections 10, 12(1) and 12(2) of the *Act.* Although I conclude that the hospital had inadequate administrative safeguards in place to protect patients' personal health information at the time of the breach, the hospital has since addressed the issues raised.

Privacy training:

Privacy training for physicians:

[29] This complaint raised concerns about the privacy training provided to the hospital's physicians. The physician involved in this breach had not received privacy training upon hire or annually thereafter. In fact, at the time of the breach, the hospital did not provide privacy training to any of its physicians.

[30] The hospital did have a written policy that addressed privacy training. This policy required its agents, which the hospital confirmed included physicians, to complete privacy training. The privacy training policy stated, in part:

> Staff and agents of the hospital must complete privacy training upon the commencement of their employment, contractual or other relationship with the Hospital and before they are given access to personal health information in the custody or control of the Hospital.
>
> Privacy education/training will be completed annually.

[31] The hospital confirmed that it did not provide mandatory privacy training to its physicians, as required by its policy. However, the hospital advised that it did provide privacy training during onboarding and annually for its non-physician agents.

[32] In response to this breach, the physician involved was required to complete privacy training. The hospital has confirmed that the physician completed privacy training in 2023 and 2024.

[33] The hospital also acknowledged the gap in privacy training of its other physicians and advised that it intended to expand its privacy training program to include physicians by implementing an electronic credentialing system that would include a requirement for physicians to complete privacy training. Unfortunately, there was a delay in the implementation of its electronic credentialing system, and the hospital was unable to provide physicians privacy training through this means in 2023, nor did it take alternative steps to ensure that its physicians received privacy training. As a result, the hospital's physicians did not receive privacy training in 2023.

[34] In March 2024, the hospital confirmed that its electronic credentialing system had been implemented and included privacy training. The hospital confirmed that all physicians have now completed privacy training for 2024 through this process.

[35] Now that the electronic credentialing system is implemented, the hospital

confirmed that the privacy officer is responsible for tracking the completion of privacy training through the electronic credentialing system and working with managers, supervisors, and the chief of staff to ensure compliance.

[36] In addition to the above, the hospital advised that it has dedicated a month each year to focus on the importance of privacy. Moving forward, the hospital confirmed that it will continue to encourage its physicians to complete credentialing and privacy education/training during this time. The hospital explained that during privacy month, the completion rates for privacy training are sent weekly to managers and senior leadership and continue to be sent until all agents have completed privacy training and signed their confidentiality agreements.

[37] The hospital also offers privacy education throughout the year through eLearning sessions, in person lunch and learns, focused huddles on the units and newsletters.

[38] As part of its efforts to remediate this matter and ensure a similar breach does not occur again, the hospital reviewed its privacy training policy and updated the policy to provide further details about the hospital's expectations. The policy now clarifies that all agents are required to complete privacy training at the beginning of their employment and annually thereafter and that the privacy officer will track the completion of training by all agents.

[39] The hospital has also advised that physicians who are not in compliance with the requirement to complete privacy training will not be eligible for re-application of hospital privileges.

Privacy training for agents other than physicians:

[40] At the time of the breach, the hospital privacy training policy required that agents were to complete privacy training, upon hire and annually thereafter. The hospital had an online Learning Management System set up to provide its non-physician agents with privacy training. The hospital also provided a privacy presentation to its non-physician agents.

[41] When responding to this breach the hospital reviewed the completion rate of training by its non-physician agents and discovered that only 50.4% had completed the required privacy training in 2023.

[42] After becoming aware of this, the hospital took steps to ensure that a privacy program was implemented to include privacy-focused huddles on the units throughout the year, communications related to privacy through the hospital's weekly newsletters, and a month focused on privacy. Throughout its privacy month, the hospital sends privacy completion rates to managers and senior leadership weekly. The hospital's senior leadership team also encourage teams to complete the training and attend department huddles to ensure that the privacy training is completed as required by policy.

[43] The hospital advised that, as a result of these efforts, to date, 87% percent of its non-physician agents have completed privacy training for 2024. The hospital explained that all full-time and part-time non-physician agents have completed the requirements. The remaining staff who have not completed the training are casual/contract staff who did not work during the re-training period. These staff will be required to complete the training during when they resume work.

[44] Moving forward, the hospital will continue to implement a privacy focused month. Privacy education will be offered by eLearning sessions, in person lunch and learns and focused huddles on the units. The hospital will continue to send privacy completion rates to department managers and senior leadership during the privacy month for follow up.

[45] Agents who are not in compliance with the requirement to complete privacy training will be subject to the hospital's process of progressive discipline which is set out in the hospital's discipline policy.

Confidentiality agreements:

[46] This breach also raised concerns about the signing of confidentiality agreements.

[47] The hospital advised that it requires all agents; employees, physicians, and volunteers to sign a confidentiality agreement upon hire and on an annual basis thereafter.

[48] At the time of the breach the hospital's privacy training policy provided the following direction about confidentiality agreements:

> The *Confidentiality Agreement* will be attached to annual privacy education requiring acknowledgement the agreement has been read and understood.

[49] The physician involved in this breach signed a confidentiality agreement upon hire but did not sign a confidentiality agreement thereafter.

[50] The hospital explained that at the time of the breach, there was no formal process for the physicians to sign or for the hospital to track the signing of confidentiality agreements by its physicians.

[51] In response to this breach, the hospital required the physician re-sign a confidentiality agreement. The hospital also confirmed that the physician re-signed a confidentiality agreement in 2023 and 2024.

[52] In addition, to remediate the matter and mitigate the risk of a similar breach reoccurring, the hospital advised that it would have all physicians re-sign confidentiality agreements through the online credentialing system that it was implementing. As noted above, this system was delayed, and physicians did not sign confidentiality agreements through this system in 2023.

[53] However, in the spring of 2024, the hospital launched its online electronic credentialing system, and all physicians signed a confidentiality agreement through this system in 2024.

[54] The hospital is now able to track the signing of confidentiality agreements by its physicians through this system. Like the tracking of privacy training, the signing of confidentiality agreements is included with privacy education, which the privacy officer is responsible for tracking, and works with managers, supervisors, and the chief of staff to ensure compliance.

[55] Additionally, in response to the breach the hospital has reviewed and updated its privacy training policy to provide greater clarity that the confidentiality agreement is required to be signed upon hire and annually thereafter.

Confidentiality agreement for non-physician agents:

[56] As noted above, the hospital's policy required all agents to sign confidentiality agreements upon hire and on an annual basis.

[57] The hospital can track the signing of confidentiality agreements by its agents through its Learning Management System.

[58] In response to this breach, the hospital discovered that only 50.4% of its non-physician agents had signed a confidentiality agreement in 2023.

[59] The hospital took steps to address this by reimplementing initiatives it had prior to the COVID-19 pandemic, such as having confidentiality agreements signed at the time that privacy education was undertaken.

[60] Additionally, during the focused privacy month in 2024, completion rates were sent as weekly reminders to department managers and the hospital's senior leadership team during the privacy focused month for follow up.

[61] The hospital's privacy training and confidentiality agreements are now provided together. Identical to the privacy training completion rates noted above, the hospital advised that to date, 87% of its non-physician agents have completed the signing of confidentiality agreements for 2024. The hospital explained that its full-time and part-time non-physician agents have completed the requirements. The remaining staff who have not signed a confidentiality agreement are casual/contract staff who have not worked during the re-training period. These staff will be required to re-sign the confidentiality agreement when they resume work.

[62] Non-physician agents who are not in compliance with the requirement to sign confidentiality agreements will be subject to the hospital's process of progressive discipline which is set out in the hospital's discipline policy.

Policies and procedures related to education:

[63] At the time of the breach, the hospital did not have a specific policy on the use of personal health information for education purposes and the hospital's physicians were not provided training about such use.

[64] The IPC's guidance document titled "Detecting and Deterring Unauthorized Access to Personal Health Information" outlines the importance of policies and procedures. It states, in part:

> Custodians should develop and implement comprehensive privacy policies and procedures that set out the expectations and requirements for all agents. Written policies and procedures are necessary to formalize and clarify required practices.
>
> …..
>
> Privacy policies and procedures should be in place to detect, prevent and reduce the risk of unauthorized access to personal health information by custodians and their agents.

[65] The physician in this case was not provided training on the use of personal health information for educational purposes, nor was there any specific guidance available through hospital policy. It is important that agents are provided with training and policies that address the uses of personal health information for education purposes.

[66] The hospital acknowledged this policy gap and took steps to update and strengthen its privacy policies and confidentiality agreement to include direction for all agents on the use of personal health information for education purposes.

[67] The hospital updated its privacy policy to include the following, in part:

> Agents of [the hospital] are not allowed to engage in self-study (such as but not limited to learning how to document or learning about our patients and the services we offer them or learning how others provide services) with personal health information in the custody or control of [the hospital] without written permission from my supervisor/manager or the Privacy Officer.

[68] The hospital's privacy training was also updated to include the above, and agents who completed training in 2024 received training on these updates to the privacy policy. The hospital's training in 2023 included an example showing that the use of personal health information for self-study is considered a privacy breach. The hospital also advised that the updates to the policy and guidance on this issue was included in eLearning sessions and lunch and learns.

[69] In addition to the updated privacy policy and training, the hospital also updated its confidentiality pledge to include the following statement:

> I am not allowed to engage in self-study (such as but not limited to learning how to document or learning about our patients and the services we offer them or learning how others provide services) with personal health information in the custody or control of [the hospital] without written permission from my supervisor/manager or the Privacy Officer.

[70] The privacy breach process policy also includes the following as an example of what constitutes a privacy breach.

> A Team Member looks at health records of patients on a self-initiated education project without being assigned to those patients and without specific authorization for an approved educational exercise.

Analysis:

[71] This breach came to the attention of the hospital after one of its physicians alerted the hospital to suspicious activity in the chart of a patient. When a hospital receives an allegation of unauthorized use, it is the hospital's responsibility to determine the scope of the breach, contain the breach and demonstrate that it has taken steps to prevent a similar breach from occurring.

[72] The issues identified in this file relate to concerns about a lack of privacy training for physicians, lack of annual signing of confidentiality agreements by physicians, failure to ensure agents completed the required training and signed the annual confidentiality agreements, and the lack of a policy or guidance about the use of personal health information for education purposes.

[73] At the time of the breach, the hospital had information practices in place that required its agents, which included physicians, to complete privacy training and sign confidentiality agreements at the time of hire and on an annual basis. The hospital had implemented a system to provide annual training and sign confidentiality agreements for its non-physician agents; however, the hospital failed to implement the same for its physicians. It is inadequate for a health information custodian to have different expectations for privacy training and confidentiality agreements between its physicians and non-physician agents.

[74] In addition, because of this breach, it became clear that the hospital had not completed the necessary reviews and follow-ups to confirm that its agents had actually completed the privacy training and signed the confidentiality agreements as required by its policy.

[75] In my view, it is not enough to simply have polices in place. Health information custodians must implement their policies in practice and take steps to ensure that they

have safeguards in place to protect personal health information in their custody and control. Health information custodians are required to ensure that all of its physicians and non-physician agents are compliant with the *Act*.

[76] The circumstances of this breach demonstrate the importance of having policies, communicating these policies to agents, and actually enforcing them.

[77] When the hospital identified the gap between physicians and non-physician agents, steps were taken to address the matter by including privacy training and the signing of confidentiality agreements as part of an online electronic credentialing system that was being developed. However, this system was delayed, and the hospital did not implement an alternate method during this delay period to ensure its physicians were compliant with its policies and the *Act*.

[78] When a situation like this arises, it is not acceptable for a health information custodian to simply not provide its agents privacy training or not require signing confidentiality agreements. In my view, health information custodians must provide alternative methods of training and signing of confidentiality agreements should an electronic system be delayed or fail.

[79] In this case, the hospital failed to ensure that its physicians had read and were trained on its policies and privacy obligations, and failed to provide guidance to the physician on the use of personal health information for education purposes which resulted in the physician breaching patient privacy without understanding that he was doing so.

[80] During the investigation of this incident, the hospital addressed the identified gaps by: implementing a system to provide privacy training and have its physicians sign confidentiality agreements on an annual basis; implementing a tracking system to ensure that all physicians and non-physician agents have completed privacy training and signed confidentiality agreements as required by its policies; updating its policies and training to provide its physicians and non-physician agents clear guidance on its expectations for privacy training and confidentiality agreements; and providing guidance on the use of personal health information for education purposes.

[81] Although I find that at the time of the breach the hospital was in violation of the *Act*, I have considered the steps taken by the hospital to address the privacy concerns identified, and I am satisfied that the hospital now has adequate measures in place to comply with sections 10 and 12(1) of the *Act*.

Notification to affected individuals:

[82] When the hospital completed its investigation, it mailed 3731 notices of the breach to affected patients or their parents/guardians if the patient was under the age of 18.

[83] For notices that were returned as undeliverable, and where the hospital was not able to identify a new address, the notice was placed in the patient's file. A notice was

also placed in the patient's chart advising registration staff to collect updated contact information and to advise the privacy officer of the update.

[84] The hospital determined that 197 of the affected patients were deceased. For deceased patients with no known estate trustee, the notification was scanned to the patient's chart.

[85] As part of the hospital's response to the breach, it reviewed and updated its privacy breach policy to include further details about the steps that should be taken when notices are returned, or patients are deceased.

[86] As part of this investigation, I reviewed the notice provided to patients. The notice describes the incident and the measures taken in response, including notifying the IPC. It also provided the name and contact information should the patient have any questions and informed the patients they could complain to the IPC.

[87] Although the notice advised patients of an unauthorized access to their health record it did not identify the type of personal health information the physician accessed.

[88] The hospital's privacy breach policy states that the hospital is to:

> Provide details of the extent of the breach and the specifics of the personal health information at issue.

[89] The hospital advised that given that the number of patients affected and that the specific type of personal health information accessed varied significantly between those affected, it decided to include in the notice that the patient's health records were accessed without authorization. Any affected patient who contacted the hospital after receiving the letter was provided with more specific information about the type of personal health information accessed, if requested.

[90] I acknowledge that there were a substantial number of patients affected by this breach with a variety of personal information involved in each case, however, in my view it would have been reasonable for the hospital to have included in the notice examples of general types of personal health information that had been accessed.

[91] Considering all the above, however, I am satisfied that the clinic has provided the notification required by section 12(2) of the *Act*. Moving forward, if a similar breach of personal health information occurs in the future, the hospital should include the specific personal health information or at minimum a general description of the type of personal health information accessed.

Issue 2: Is a review warranted under Part VI of the *Act*?

[92] 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.

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

NO REVIEW:

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

Original Signed by: October 16, 2024

Alanna Maloney
PHIPA Investigator