Information and Privacy Commissioner,
Ontario, Canada

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

PHIPA DECISION 174

HR19-00196 and HR19-00289

A Public Hospital

March 18, 2022

Summary: A public hospital (the hospital) contacted the Information and Privacy Commissioner/Ontario (the IPC) to report two privacy breaches under the *Personal Health Information Protection Act, 2004* (*PHIPA* or the *Act*). Specifically, and unrelated to each other, a clerk and a nurse had each accessed the personal health information of many patients without authorization. In light of the steps taken by the hospital to address both breaches, 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*

Decisions Considered: IPC Order HO-010; PHIPA Decision 163

BACKGROUND:

[1] A public hospital (the hospital) separately reported two privacy breaches to the Information and Privacy Commissioner/Ontario (the IPC) in the spring of 2019, both of which involved inappropriate accesses to patients' personal health information. The IPC opened Complaints HR19-00196 and HR19-00289 to address these matters.

The Events of HR19-00196

[2] On April 9, 2019, the hospital reported to the IPC that a clerk (the Clerk) had accessed a patient's personal health information without authorization. This followed a complaint to the hospital that the Clerk had posted a patient's personal health information to Facebook. The patient provided the hospital with screenshots of posts made by the Clerk, but was unable to provide any posts containing her personal health

information, stating that the Clerk had deleted these. The hospital found that the Clerk had booked an appointment for this patient, but the Clerk denied having posted or otherwise disclosed any of the patient's personal health information.

[3] Based on the information available, the hospital was not able to determine if the Clerk had posted the patient's personal health information. The hospital did conduct a preliminary audit of the Clerk's accesses to the hospital's electronic medical registry (EMR) system and found evidence that she had made unauthorized accesses to several patients' files. It placed the Clerk on administrative paid leave while it investigated further. As the Clerk would not be present at the hospital while on leave, and did not have remote access to the EMR, the hospital did not find it necessary to remove her EMR access rights at that time.

[4] The hospital reviewed all of the Clerk's accesses to personal health information between March 2016 and September 2018 for all patients. The hospital identified 19 individuals whose records the Clerk had accessed not in the course of her duties, with a total of 83 apparently unauthorized accesses. The affected individuals were largely either hospital employees, or friends and family of the Clerk. The Clerk also accessed her own medical file four times. The hospital noted that the Clerk had signed a confidentiality agreement upon hire in 1998 and again in 2017, and had also completed some limited privacy training relating to lockboxes in 2017. The hospital did not indicate that she had attended any other training.

[5] During a meeting with hospital staff following the hospital's investigation, the Clerk took the position that her searches were acceptable because the affected individuals she had searched for were family members. The Clerk was not able to provide any reasons related to her duties for the accesses. She stated that she had not copied or otherwise disclosed any patient personal health information that she had accessed.

[6] The hospital terminated the Clerk's employment, citing the seriousness of the breach and its loss of trust in the Clerk.

The Events of HR19-00289

[7] On November 27, 2018, a privacy officer at another hospital notified hospital staff that a nurse (the Nurse) had accessed her own health information without authorization. A hospital audit confirmed this, and the hospital staff advised the Nurse that such accesses were inappropriate. The hospital directed the nurse to access her medical information via the Health Records Department instead. Six months later, the same outside privacy officer again notified the hospital of further unauthorized self-lookups by the Nurse.

[8] In response, the hospital conducted an audit of all of the Nurse's EMR accesses from September 2017 to February 2019, finding 41 unauthorized accesses to five patients' personal health information. The hospital also found that the Nurse had accessed her own file 23 times. The Nurse had signed a confidentiality agreement when

she was hired in 2012, and had twice completed a privacy training module: first in 2012 and again in 2017.

[9] During a meeting with the hospital, the Nurse confirmed making the accesses, stating that she did so for family members whom she "was trying to expedite or ensure [they] received timely care." The Nurse also expressed remorse, stating that she "did not realize the impact and the consequences of her actions and understands clearly this was wrong."

[10] The hospital determined that while the Nurse's actions were inappropriate, she had no malicious intent. Following its internal guidelines for sanctions in privacy breaches, the hospital reported the breach to the College of Nurses of Ontario, and suspended her for five days without pay. The hospital assessed that it was not necessary to remove the Nurse's EMR access rights as it did not believe she would make further unauthorized accesses, based on her level of remorse and lack of malicious intent. Since this time, the Nurse received privacy training multiple times, including reviewing the confidentiality agreement and the hospital's Patient Privacy Policy.

PRELIMINARY ISSUES:

[11] There is no dispute that the hospital is a "health information custodian" and that both the Clerk and the Nurse were "agents" of the hospital under the *Act*. There is similarly no dispute that the records accessed by the Nurse and the Clerk were records of "personal health information" within the custody or control of the hospital.

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

- the hospital is a "health information custodian" under paragraph 4.i of section 3(1) of the *Act*;
- the Clerk and the Nurse were "agents" of the hospital, as that term is defined in section 2 of the *Act*;
- the records at issue contained "personal health information" under section 4(1) of the *Act*, which were in the custody or control of the hospital; and
- the hospital, via the accesses made by its agents the Nurse and the Clerk, used personal health information contrary to section 29 of the *Act*.

ISSUES:

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

1. Did the hospital take reasonable steps to protect personal health information?

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

RESULTS OF THE INVESTIGATION:

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

[14] Health information custodians, when confronted with a breach of personal health information, should take appropriate steps in response. These include containment of the personal health information involved, notification of those affected, and investigation and remediation of the breach.

[15] In the matters at hand, the hospital identified the scope of both breaches. It notified the patients affected by the unauthorized accesses via letter, and notified the College of Nurses of Ontario that the Nurse had made unauthorized accesses. As such, the remainder of my analysis focusses on the steps the hospital took to remediate the breaches, and in particular, the guidelines and practices it has put in place to protect patients' personal information as required under section 12(1) of the *Act*.

[16] Section 12(1) of the *Act* sets out institutions' obligations to protect the security of personal health information, stating as follows:

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

[17] In Order HO-010, the IPC stated that measures or safeguards must be reviewed from time to time to ensure that they continue to be "reasonable in the circumstances" in order to protect personal health information from theft, loss, and unauthorized use or disclosure and to protect records of personal health information against unauthorized copying, modification, or disposal.

[18] The need to have proper safeguards in place was set out more recently in PHIPA Decision 163 as follows:

> Administrative and technical measures and safeguards are critical to protecting personal health information. The IPC has previously stated that, in order to comply with the requirements in section 12(1) of the *Act* and to take steps that are reasonable in the circumstances to protect personal health information, 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.[1]

[19] As part of my investigation, I reviewed the hospital's policies, procedures, training materials, and other informational materials.

Policies

[20] The hospital states that its policies, procedures, and guidelines are available to staff through the Document Manager on the hospital's intranet. The hospital sends communications to managers when it publishes new or revised policies; when needed, they circulate a memo about such policies. If the policy requires attestation, the hospital's system auto-generates emails to staff to remind them of this requirement.

[21] The hospital has a Patient Privacy Policy (the Policy) that applies to all hospital staff. It defines a privacy breach as "[a]ny intentional or unintentional collection, use or disclosure of personal health information, including loss or failure to protect such information." It specifically addresses unauthorized accesses, stating:

> Any [hospital] staff who has unauthorized access to a patient's PHI will be investigated by the [the hospital's] Privacy Office. This violation includes but is not limited to snooping on a patient's file for non-work-related purposes.

[22] The Policy states that violation of it could result in dismissal and that "privacy breaches involving regulated health professionals will be reported to regulatory bodies as per legislative requirements and individual College requirements." In its "Use and Disclosure" section, the Policy states that "[hospital] staff will not disclose PHI on any personally-run social media outlet."

[23] The Policy also includes a five-page "Policy Highlights" section and concludes with the following reminder:

REMEMBER

- All patients have the right to keep information about themselves private.
- It is your responsibility, as [a hospital] employee, to protect their PHI.
- You can do so by:
    - Not accessing health records for which you are not part of the circle of care
    - Locking your workstation when it is left unattended

[1] PHIPA Decision 163 at paragraph 23.

- Do not discuss patients with those who are not in the circle of care
- Do not leave documents with PHI unattended and dispose of them in approved confidential waste bins

[24] The hospital's "Process for Investigating Privacy Breaches and/or Complaints" (Breach Process) gives instructions on the steps to take when the hospital learns of a breach. The hospital's Chief Privacy Officer can immediately suspend employee access to all systems, when appropriate. Alternatively, they may notify the employee of the situation, and advise them that they are conducting an investigation, including monitoring their access. The hospital will then conduct an audit and an investigation, including holding an interview with the employee involved in the breach. If the hospital confirms that there was a privacy breach, the Chief Privacy Officer will notify the appropriate manager, and they will review the findings and determine the appropriate disciplinary action. They may also notify the IPC or a regulatory college of the breach.

[25] The hospital followed the steps set out in the Breach Process in its investigations of both the Nurse and the Clerk. Once alerted to possible unauthorized accesses, it conducted preliminary investigations, followed by more thorough audits of the employees' accesses and interviews with the employees. It also notified the patients affected by the unauthorized accesses, as well as the relevant regulatory college, in the case of the Nurse.

[26] I note that the hospital did not suspend the EMR access privileges for either the Nurse or the Clerk. In the case of the Nurse, this decision was consistent with the hospital's "Sanction Guidelines for Privacy and Security Breaches," which categorize breaches into "accidental or inadvertent", "intentional, non-malicious", or "intentional and malicious". These guidelines set out the disciplinary actions and other consequences that may result from privacy breaches, and included a list of aggravating and mitigating factors that may be considered. The hospital states that it found the Nurse's intentions were not malicious and assessed that further unauthorized accesses were unlikely. It therefore decided it was unnecessary to suspend her EMR accesses.

[27] In contrast, the hospital did not suspend the Clerk's access privileges because it determined that placing her on administrative leave *de facto* curtailed her ability to access the EMR. This was due to the Clerk not being present at the hospital while on leave and not having remote access to the EMR system. There is no indication that the Clerk obtained any access during this time.

[28] However, remote work has since become more prevalent and placing an employee on administrative leave may no longer have the effect of removing her access to the hospital's EMR. The hospital has committed to addressing this gap and adjusting its process to reflect that it can no longer rely on placing an individual on administrative leave as a method of limiting EMR access. Given this commitment, I am satisfied that both the privacy policies in place, and the hospital's adherence to them, are adequate.

Training

[29] The hospital states that all physicians and employees receive privacy training upon hire. Since 2017, that training includes a presentation, an e-learning module, and a quiz.

[30] The copy of the general orientation privacy presentation that the hospital provided addresses unauthorized accesses, stating "DO NOT access the personal health information of individuals to whom you are not providing health care." It includes an example of snooping on a neighbour's personal health information to illustrate what an intentional privacy breach may look like. This presentation specifically addresses social media, and explains how an employee can breach a patient's privacy via social media posts even if their name is not disclosed, as they could be identified by other details. While the hospital was not able to substantiate allegations that the Clerk posted personal health information on social media, I am satisfied that the hospital's current privacy training materials clearly set out that such an action is not permitted.

[31] The hospital has increased the frequency of its privacy training, which it now provides annually as part of its Privacy Month, the first of which occurred in February 2020. This annual training includes a review of the Patient Privacy Policy, with an accompanying slide deck presentation. Privacy Month activities also include walkarounds, which are conducted for a dual purpose: to identify unsecured personal health information and to give staff an opportunity to ask questions of the hospital's privacy staff.

[32] The hospital has also committed to providing reminders to its staff of their privacy obligations under the *Act*. The hospital holds department-specific training sessions throughout the year to provide refreshers on the privacy policy and address each department's specific questions and concerns. It also provides privacy lunch and learn sessions.

[33] The hospital did not previously require employees to provide attestation that they had completed their privacy training, but has since implemented an attestation requirement. This is now possible because the hospital has recently put in place Policy Medical software that includes an attestation feature, permitting management to request, via an automated email notification system, that its employees read (and then attest to reading) the annual privacy training documents. This software also provides reminders to staff who have not completed this training, and allows management to track who has done so.

Confidentiality Agreements

[34] The hospital provided the IPC with copies of its "Confidentiality Undertaking and Non-Disclosure Agreement". This undertaking states that the staff member will not "[disclose], use, alter, destroy, copy or print" personal health information without authorization, and that to do so could result in discipline, termination, or legal action.

[35] The hospital previously required new employees to sign confidentiality agreements at hiring, but has now committed to having staff execute these on an annual basis. As with the privacy training attestation, the hospital is now able to both track execution and provide reminders of the need to review and sign the confidentiality agreements each year.

Privacy Warning Flags

[36] Previously, the hospital stated that its EMR system only had warning flags in place for the small subset of medical records that were under a consent directive. That meant that these warning flags only appeared on the records of patients who had given the hospital direction as to who may access those records. The hospital committed to putting warning flags in place prior to employees accessing any records of personal health information, not just those subject to a consent directive.

[37] In August 2020, the hospital fulfilled this commitment by adding a warning message to its EMR login screen. This warning appears to all staff logging into the system. The warning message displays in both French and English, occupies more of the screen than the login portion itself, and reads as follows:

> Respect Patient Privacy
>
> I will not access any personal health information other than that required to carry out my duties. Failure to comply with privacy obligations may result in termination of employment or loss of privileges. Unauthorized access to patient information will not be tolerated.

[38] The hospital also sent out a memo alerting staff to this change and providing a general reminder regarding patient privacy.

Audit Functionality

[39] The hospital has committed to conducting random and scheduled audits going forward, stating that since it implemented its new electronic record system in June 2019, it now has a more thorough understanding of its auditing capabilities.

[40] Each month, the hospital generates a report of all employees who have searched for patients with the same last name as their own. Since May 2020, it also runs random access audits. In both cases, the hospital then analyzes the lists of accesses for several types of suspicious activities, such as:

- Accesses to health information regarding patients who did not visit the hospital during the time of the access;
- Accesses to health information of employees of the hospital; and
- Accesses to the health information of an individual on multiple dates and times, or to individuals with the same last name on the same day.

[41] In addition, the hospital runs user-based and patient-based access reports if any suspicious activity is reported or suspected, or if a patient requests that they do so.

[42] The hospital states that it is looking into options for purchasing a third party system that would be able to verify a larger volume of accesses, and automatically detect suspicious patterns and accesses.

Analysis

[43] These breaches came to the attention of the hospital for two very different reasons, and the hospital has a responsibility to demonstrate that it has taken steps to help prevent similar situations arising in future. These instigating incidents provide a useful frame to help determine if the hospital has met its obligation to take reasonable steps to protect personal health information.

[44] The allegation that the Clerk posted personal health information to social media, while not substantiated, shows the need for the hospital's present-day policies to clearly state that any disclosure of that nature is strictly prohibited. This is in addition to setting out when accesses to personal health information are permitted, and when they are not.

[45] With that in mind, my review of the Patient Privacy policy found a document that communicates the need to protect patients' privacy, and directs employees not to access health records unless they are within the circle of care. The hospital's training resources, including its orientation presentation, also clearly communicate that viewing an acquaintance's personal health information and posting patient information to social media are not acceptable, and could result in serious consequences to any employee who does so. I am satisfied that the hospital's privacy policy and training documents clearly set out employees' obligations to only access personal health information when necessary in the course of their jobs.

[46] However, my review includes not only whether the hospital has adequate privacy policies and training documents in place, but also how it communicates this guidance to employees. The Nurse's breach demonstrates the importance of this communication, as she stated that she did not know that the accesses she made were not permitted. Indeed, the hospital agreed that she did not have malicious intent in doing so. This indicates that the hospital failed to adequately inform the Nurse when she was allowed to access personal health information under the *Act*. Policies and training materials only help protect patient privacy if employees read them, and it was not clear that the hospital employees were being given sufficient reminders of their privacy obligations.

[47] Since the time of the breaches, the hospital has been providing increased privacy training, and documenting that the training has been provided. The hospital now provides training annually as part of its Privacy Month initiative, and requires that employees both attest to that training and re-execute their confidentiality agreements. The hospital also provides privacy reminders throughout the year, through presentations to departments and lunch and learns. Moreover, employees are now

reminded of their privacy obligations each time they log in to the EMR, due to the privacy warning flag displayed on the log in screen.

[48] The gaps in the training provided at the time of the breaches allowed for an employee without malicious intent, such as the Nurse, to breach patients' privacy without understanding that she was doing so. The training it provides now clearly communicates employees' privacy obligations, in an understandable way, and provides refreshers on these obligations annually. Given the hospital's improvements to their training, processes, and EMR system capabilities, I am satisfied that the hospital has adequately addressed the privacy concerns raised by these breaches.

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

[49] 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.

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

DECISION:

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

Original signed by: March 18, 2022

Jennifer Olijnyk
Investigator