Information and Privacy Commissioner,
Ontario, Canada

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

PHIPA DECISION 306

Complaint HR23-00076

A public hospital

October 23, 2025

Summary: A public hospital (the hospital) reported privacy breaches under the *Personal Health Information Protection Act, 2004* (the *Act*). A patient registration clerk inappropriately disclosed patients' personal health information to a security guard that was stationed on premises. The clerk also viewed without authority health records of a patient. The investigator finds that although at the time of these incidents, the hospital lacked reasonable measures to protect patients' personal health information, it has responded adequately to the breaches. The investigator finds that no further review of this matter under Part VI of the *Act* is warranted.

Statutes Considered: *Personal Health Information Protection Act, 2004*, S.O. 2004, c. 3, Sched. A, as amended, sections 2, 3(1), 4(1), 6, 10(1), 10(2), 12(1), 12(2), 58(1); O. Reg. 329/04, sections 6.3(1), 6.3(3)

BACKGROUND:

[1] In February 2023, a public hospital (the hospital) reported privacy breaches to the IPC under the *Personal Health Information Protection Act, 2004* (the *Act*) regarding a patient registration clerk (the clerk) and a security guard stationed on premises. The hospital submitted that according to the staff reports received, the clerk "left [her] computer open and accessible for security staff to access" personal health information (PHI) of patients. It was also submitted that the clerk shared with the security guard PHI of patients, including those whom she was not involved in registering.

[2] The IPC opened a file to address the reported breaches at the Early Resolution

stage of the IPC's processes.

[3] The hospital launched an internal investigation immediately after its staff came forward regarding the potential breaches. The hospital suspended the clerk's access to the electronic health information system (the HIS) and instructed her not to report to work pending completion of the investigation.

[4] Based on its investigation which included interviews with the clerk, the hospital determined that unauthorized disclosure did occur. It imposed disciplinary measures against the clerk which included completion of training on privacy and the hospital's Code of Conduct. The security guard was relieved of his duties at the hospital. In addition, the hospital advised the IPC that it will update its staff orientation to include lessons learned from the incidents and explore additional discussion as part of the hospital's internal communications.

[5] The hospital could not identify the individuals affected by the disclosure, and neither the clerk nor the security guard could recall whose PHI they viewed. After discussions with the IPC, the hospital agreed to issue a general notice regarding the privacy breach.

[6] Around this time, the hospital also implemented a privacy warning in the HIS further to the IPC's questions about its privacy practices. On its login page, the HIS states that "*Your access of Patient data in the EHR [electronic health record] is monitored. Unauthorized use, collection or disclosure of patient data is a serious breach that may result in disciplinary action and/or other serious consequences*."

[7] Separate from the issue of unauthorized disclosure, the hospital also reported that the clerk viewed certain patient records without authorization. The hospital submitted that, when interviewed by the hospital's privacy specialist, the clerk admitted to the unauthorized access.

[8] The hospital noted however that it could not identify any unauthorized access from the audit results obtained during its investigation.

[9] When the IPC sought clarification, the hospital submitted that the clerk's access of patient health records may have been appropriate. The hospital did not provide details about what records were accessed or for how long, although it acknowledged there were numerous instances of access according to the Manager of Health Records.

[10] Despite the steps the hospital took in response to the privacy breach, the information provided to the IPC raised several concerns. It was unclear whether the hospital conducted adequate investigation into the circumstances of the breach. The hospital also supplied the IPC with conflicting information about whether the clerk inappropriately accessed patients' PHI, which is relevant in determining whether the hospital has the corresponding duty under the *Act* to notify these patients.

[11] Consequently, this matter proceeded from the Early Resolution stage to the Investigation stage of the IPC's processes. As the Investigator assigned, I received and reviewed written submissions from the hospital.

PRELIMINARY ISSUES:

[12] It is not in dispute, and I find, that all electronic health records of patients at issue are records containing PHI as defined in section 4(1) of the *Act.*

[13] It is also not in dispute, and I find, that the hospital is a "health information custodian" within the meaning of section 3(1) of the Act and that the clerk is the hospital's "agent" within the meaning of section 2 of the Act.

[14] As a preliminary matter, I find that the clerk's access and viewing of patients' PHI in their electronic health records is a "use" of PHI within the meaning of sections 2 and 6 of the Act.

[15] The hospital acknowledged that the clerk inappropriately disclosed PHI of patients by sharing and discussing it with the security guard and leaving her computer unsecured, allowing the guard to view health records of patients. I agree and find that unauthorized disclosure of PHI occurred and that it was a breach under the Act.

ISSUES:

[16] This decision addresses the following issues:

1. Did the hospital comply with the notification requirement under section 12(2) of the *Act*?
2. Did the hospital take reasonable steps to protect personal health information?
3. Is a review warranted under the *Act*?

RESULTS OF THE INVESTIGATION:

Issue 1: Did the hospital comply with the notification requirement under section 12(2) of the *Act*?

[17] Section 12(2) of the *Act* states as follows:

> 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.

[18] Below, I consider whether PHI in the custody or control of the hospital was "used or disclosed without authority" such that the hospital had a duty to notify the affected individuals under section 12(2). I then consider whether the hospital complied with this duty.

Unauthorized disclosure

[19] When the hospital first contacted the IPC, no notification regarding the unauthorized disclosure had been issued. During the Early Resolution stage of this file, the hospital prepared a draft notice, which was later finalized during the Investigation stage after further discussions with the IPC. The notice was posted in June 2024 in the Patient Registration area and online on the hospital's website for six months.

[20] The notice states that, between January and May of 2022, the clerk left her computer open and allowed a contracted security guard to view patients records both at and away from her desk, as well as discussing patient cases with the guard.

[21] The notice shares that the security guard would have been able to view the following types of patient information:

- Names and contact information (like home address and phone numbers);
- Hospital room numbers;
- Dates of admission and discharge;
- Department or unit of the hospital for admission;
- OHIP numbers; and
- Information about diagnosis or health history.

[22] The notice acknowledges that the disclosure was not necessary and was contrary to the security guard's role and hospital policies. It states that the hospital took disciplinary actions against both the clerk and the security guard, and that new policies were implemented regarding disclosure of PHI. It also provides the hospital's contact information to address any inquiries, and notes that patients are entitled to contact the IPC regarding the incident.

[23] Notably, this notice does not acknowledge any unauthorized access of PHI by the clerk. It states that the clerk was allowed to access patient records as part of her job.

[24] The notice appears to include the necessary information related to the unauthorized disclosure involving the clerk and the security guard, consistent with the IPC's guidance document *Responding to a Health Privacy Breach: Guidelines for the Health Sector.*[1] Ideally, a custodian should directly notify every individual affected. However, since the hospital could not identify the individuals affected, I find that a general notice was appropriate in this case.

[25] However, the hospital delayed significantly in notifying the individuals affected. I note that approximately ten months elapsed between April 2022, when the hospital's privacy officer at the time first received the staff reports, and February 2023, when the matter was brought to the IPC's attention. Although the notice was not issued until June 2024, this was after multiple discussions with the IPC regarding the breaches and potential notification.

[26] The hospital explained that it conducted its privacy investigation after contacting the IPC. However, according to the hospital's own timeline of events, its initial investigation and remediation (including disciplinary actions) were completed by May 2022. It was not until February 2023 before the IPC was eventually contacted, during which time the hospital did not take steps to notify the affected individuals.

[27] Based on this information, I find that the hospital failed to notify the affected individuals at the first reasonable opportunity as required under section 12(2)(a) of the *Act*.

[28] I also asked the hospital regarding the timing of its reporting to the IPC. The hospital's privacy officer acknowledged the delay in notifying the IPC of the breach, explaining that the expected procedure of documenting the discovered breach was not followed, although the rationale could not be identified. It was noted that the privacy officer at the time, their supervisor and CEO who were privy to the details of the breaches are no longer with the hospital. The privacy officer advised that going forward, the hospital will ensure that all reportable breaches are reported to the IPC at the first reasonable opportunity in compliance with its statutory obligation.

[29] Under section 6.3(3) of the Ontario Regulation 329/04 under the *Act*, health information custodians are required to "notify the Commissioner of the existence of a circumstance set out in subsection (1) at the first reasonable opportunity". Section 6.3(1) of the regulation outlines the specific circumstances where the IPC must be notified of a breach pursuant to section 12(3) of the *Act,* including where the custodian has reasonable grounds to believe that PHI was "used or disclosed without authority by a person who

[1] Information and Privacy Commissioner of Ontario (October 2018), *Responding to a Health Privacy Breach: Guidelines for the Health Sector*, retrieved from <https://www.ipc.on.ca/en/resources-and-decisions/responding-health-privacy-breach-guidelines-health-sector>.

knew or ought to have known that they were using or disclosing the information without authority". These provisions are also addressed in the IPC's guidance document, *Reporting a Privacy Breach to the IPC: Guidelines for the Health Sector*.[2]

[30] It is the IPC's expectation that custodians promptly notify the IPC of privacy breaches that they have identified. Timely reporting enables the IPC to provide the custodians with guidance on responding to the breaches, including containment and notification of affected individuals. Custodians can provide the IPC with further updates as they complete further investigation and remediation as appropriate.

[31] To that end, I recommend the hospital to ensure that, in the event of a future breach, it notifies the IPC at the first reasonable opportunity.

Unauthorized use

[32] The hospital's position on whether unauthorized access of PHI occurred evolved during the course of the IPC's investigation of this matter.

[33] Initially, the hospital explained that patient registration clerks are authorized to access patients' PHI for the purposes of patient registration and for record-related clerical tasks such as filing, chart combining, chart tracking and daily inpatient census reporting. The hospital's position was that the clerk may have viewed patient records which she was authorized to view. This could not be verified by audit results or the reports received from staff.

[34] However, the hospital also observed that the clerk viewed laboratory results and patient summary information. It noted that clerks have no need to go into these parts of the HIS while performing their role. Accordingly, the hospital undertook additional investigation.

[35] The hospital later submitted that not only the clerk at issue, but also other patient registration clerks routinely accessed health records of patients whom they did not register, as part of their clerical duties and to support hospital operations. The hospital discovered from its investigation that this was a general practice put in place by its previous management to assist clinical staff in times of staff shortage or high work volume.

[36] The hospital confirmed that it has since instructed clerks not to look up PHI of patients (including chart records) as part of their duties. The hospital provided this instruction to clerks by email in November 2024 and again in September 2025.

[37] The hospital identified six patients whose health records the clerk accessed

---

[2] Information and Privacy Commissioner of Ontario (September 2019), *Reporting a Privacy Breach to the IPC: Guidelines for the Health Sector*, retrieved from <https://www.ipc.on.ca/en/resources-and-decisions/reporting-privacy-breach-ipc-guidelines-health-sector>.

between January and April 2022, for reasons such as changing the health card number and census reporting activities. The records accessed contained PHI such as health card number, orders, medications and discharge instructions. The hospital submitted that these accesses were authorized activities because they are part of the general practice that was supported by the hospital's previous management. The hospital also noted, contrary to its initial submission, that the clerk did not admit to any unauthorized access outside of her role.

[38] Nevertheless, after discussions with the IPC, the hospital directly notified the six patients in writing. The notices acknowledge that unauthorized access occurred and describes the types of PHI implicated. However, five of these notices also state that the clerk accessed the records as part of her job.

[39] The hospital also posted a second general notice both physically on the premises and its website. The notice highlights the hospital's conclusion that patient registration clerks may access patient records as part of their job when the need arises. However, the notice also states that the hospital provided privacy and confidentiality training to clerks and that going forward, clerks will document the reason for accessing health records if they go beyond their normal scope of practice.

[40] The hospital identified one other patient whose records the clerk accessed but she could not recall the reason for the access. The records contained PHI including procedural information, staging and pathology, plan of care, discharge information, medication lists and orders. The hospital notified this patient in writing. The notice describes the PHI accessed, acknowledges the breach and states that patient registration clerks must now document the task they are performing when accessing health records.

[41] I am satisfied that the unauthorized use of PHI occurred with respect to this patient. Overall, the notice provided contains the necessary information in keeping with the statutory requirements under section 12(2) and the IPC's guidance on notification.

[42] As for the broader practice that was in place for patient registration clerks to view PHI of patients, it is apparent from the information provided that the hospital was unaware that this was put in place by the previous management. In my view, the hospital lacked adequate institutional knowledge about the information practice pertaining to the clerks, demonstrating a disconnect between management and these employees and/or their immediate manager about what scope of record access is appropriate for their role. This, in my view, constitutes a gap in the hospital's management of its information practices.

[43] I note that during early stages of this matter, the hospital appears to have changed, on multiple occasions, its stance on whether the clerk engaged in unauthorized access. I recognize however that, through further inquiries, it was able to obtain additional facts which informed its understanding of the circumstances and share its findings with the IPC.

[44] I also recognize that the hospital took the opportunity to inform the patients and the public about its privacy practices and the steps it is taking to improve them.

[45] The hospital advised that although the clerks no longer access health records of patients, the hospital may in the future need to change the clerks' job description from time to time, to accommodate the hospital's workload needs and sustainable operation. The hospital expressed its commitment to updating the patient registration clerks' job description accordingly and that the manager is meeting with the clerks to clarify the job duties, changes in scheduling and the importance of confidentiality and responsibilities to keep PHI safe and secure.

[46] I recommend that the hospital take steps necessary to ensure that any changes made to the scope of access is properly documented and communicated internally.

Issue 2: Did the hospital take reasonable steps to protect personal health information?

[47] Section 12(1) of the *Act* requires health information custodians to take reasonable steps to protect the security of personal health information in their custody or control. This requirement includes a duty to respond promptly and adequately to a privacy breach.

[48] A related obligation is the duty to have in place and to comply with information practices, including administrative, technical and physical safeguards and practices with respect to personal health information in their custody or control [sections 10(1) and 10(2)].

[49] During this investigation, the hospital provided details of its privacy practices as well as improvements made to address the gaps identified during its breach response. Below, I highlight the relevant details considered in determining whether the hospital took reasonable steps to protect PHI of its patients.

Third party security service provider

[50] During my investigation, I asked the hospital to outline findings from its interview with the security guard involved in the unauthorized disclosure of PHI. I also inquired whether the guard was advised not to use or disclose any information that he inappropriately accessed, viewed or received in the circumstances of the breach.

[51] The hospital submitted that it could not interview the guard because he was immediately relieved of his duties, removed from the premises and instructed not to return. The hospital noted that in hindsight, it would have arranged an interview with the assistance of the security company that employed the guard.

[52] However, the hospital also noted that, according to the company, the guard was provided remedial privacy training and assigned to a non-healthcare setting. In addition, the company confirmed the guard was specifically advised to refrain from using or

disclosing any PHI that he may have learned during his time at the hospital.

[53] The hospital discussed the incident and relevant privacy practices with the company. The company noted that security guards sign a confidentiality agreement when hired but did not otherwise sign a policy specific to the hospital. However, pursuant to the Code of Conduct regulation[3] under the *Private Security Investigative Services Act, 2005*, security guards are required to keep confidential all information learned while on duty.

[54] Notwithstanding the above, the hospital confirmed that, in remediation of the disclosure breach in this case, it now requires contracted security guards to also sign the hospital's confidentiality agreement.

Privacy training

[55] The hospital submitted that privacy training is provided to staff upon hire and annually.

[56] The hospital noted that while the clerk at issue has received annual privacy training, it was inadvertently missed in 2021 due to a corporate upgrade on the associated learning management system.

[57] Following the breaches, the hospital implemented lessons learned into the orientation training by instructing staff to be always aware of their surroundings and to ensure that no unauthorized access of PHI occurs while they are working. Staff were also reminded to lock their computer to protect PHI from unauthorized access and to secure PHI at their workstations.

[58] The hospital advised that annual completion of privacy training is tracked via its learning management system. The hospital also noted that its Privacy department will issue additional training materials in the event of a future breach that involves its employees.

Confidentiality agreement

[59] During this investigation, the IPC initially received conflicting information about the confidentiality agreement signed by staff. It was submitted that employees are required to sign a confidentiality agreement upon hire and annually. However, the hospital also noted that according to its Human Resources department, employees were no longer required to sign a confidentiality agreement, since such an agreement is implied through completion of the e-learning modules and quiz.

[60] I received and reviewed a copy of the existing confidentiality agreement. It highlighted the importance of respecting the privacy, confidentiality and dignity of

[3] O. Reg. 363/07.

individuals including patients. The signees would agree to several privacy requirements, including that they only access, process and transmit confidential information (which includes personal health information) as required by the duties of their role, and that they refrain from collecting, using or disclosing any confidential information without appropriate authorization.

[61] I noted for the hospital that, while the agreement defines "personal health information", it does not align with the definition as set out in the *Act,* nor does the agreement acknowledge the privacy obligations which the legislation imposes on health information custodians and their agents. I recommended the hospital return to using such an agreement but that it review and amend the agreement to ensure compliance with the *Act.*

[62] In response, the hospital prepared a new confidentiality agreement which the staff must sign annually. The agreement now includes explicit acknowledgement that the hospital is a health information custodian under the *Act* and that the signee must comply with the *Act.* It also refers to the definition of PHI pursuant to the *Act.*

[63] The agreement also adds new requirements and clarifications to bolster privacy compliance. For instance, it reinforces the importance of adhering to the scope of information access appropriate for the signee's role, noting that staff are allowed to collect, use and disclose PHI on a "need to know basis" and only the minimum amount required, as authorized in writing or as required by law.

[64] The hospital advised that the clerk has signed the new confidentiality agreement. It further confirmed that annual completion of the confidentiality agreement is tracked electronically via its learning management system.

Documentation of staff access to health records

[65] In my investigation, I asked the hospital to describe the steps it will take to remediate the issue of unauthorized access, including implementation of procedures to ensure that employees document instances where employees would be authorized to access patient records outside their standard scope of responsibilities.

[66] The hospital advised that going forward, staff will be expected to document in the "chart accessed by" field in the electronic health record the reasons for their access. To reinforce this requirement, the hospital circulated to its staff detailed instructions for completing the field, including a Q&A document. The hospital also issued related enhanced privacy training for all patient registration clerks.

Breach management framework

[67] Following the breaches in this case, the hospital implemented a new Privacy Breach Reporting and Management Framework policy. The hospital noted that the policy was prepared in March 2025 and implemented in September 2025.

[68] As part of this investigation, I received and reviewed a copy of the policy. It expressly recognizes the responsibility of all users of electronic health record databases to use them in accordance with the *Act.* It emphasizes that access to PHI is based on "the need to know" basis to provide current and direct patient care, or to perform one's duties.

[69] The document outlines procedural steps that the hospital and its staff will undertake in the event of a privacy breach, including assessment and containment of the scope of the breach (including collection of evidence), containment, notification of the individuals affected by the breach, reporting to the IPC, investigation, and taking measures to reduce the risk of future privacy breaches.

[70] The policy states that interview of appropriate staff/affiliates will be conducted as part of the internal investigation following containment and initial review of a breach.

[71] Under section 5.8, the policy outlines the types of privacy breaches which the hospital has statutory obligations to report to the IPC. In this regard, further to my recommendation above on notifying the IPC of a privacy breach in a timely manner, I also recommend that this section be revised to state that, pursuant to Ontario Regulation 329/04 under the *Act,* the mandatory reporting to the IPC must be completed at the first reasonable opportunity.

[72] In terms of notifying the affected individuals, section 5.6 of the policy provides that whether notification occurs before or after the Investigation stage will be dependent on the circumstances of the breach. It further notes that the Privacy Officer/delegate will determine the timing and the most appropriate way to inform the affected individuals. In recognition of the hospital's statutory obligation, I recommend also that this section be amended to include a statement that, pursuant to the *Act,* notification to the affected individuals should be completed at the first reasonable opportunity.

[73] Finally, I note that the policy document does not indicate its effective date of implementation. To ensure that the hospital keeps an accurate record of its information practices, I recommend the document be amended to indicate the date on which the policy was put into effect.[4]

Improvement of audit functionality

[74] As part of its internal investigation, the hospital's privacy department obtained an audit of the clerk's activities within the HIS from January 2022 and May 2022. The audit was performed and the results provided by a third party administrator.

[75] The hospital was asked to explain why it could not identify patients where, according to the audit, the clerk looked at certain types of health records she was not

[4] *See* PHIPA Decision 298, paras 59-63 regarding the IPC's expectation of "demonstrable accountability" for information practices of health information custodians, to ensure compliance with section 10 of the *Act.*

supposed to view, such as lab results. The hospital acknowledged that audit results related to laboratory views and patient summary views could not be linked to specific patients. This was explained as a limitation with the audit functionality of the HIS software.

[76] The hospital contacted the third party administrator to address this issue. Eventually, the hospital confirmed that the administrator has worked with the software developer to implement changes so that, going forward, the audit reports will display patient identifiers associated with viewings into the electronic health records.

Discussion

[77] The unauthorized use and disclosure of PHI in this case arise primarily from the individual actions of the clerk and the security guard. However, it also became clear – from the hospital's response to these breaches and to the IPC's inquiries – that there were notable gaps in the hospital's information practices.

[78] The lapse in the clerk's annual trainings as well as the conflicting information provided about the annual completion of confidentiality agreement overall suggest, in my view, an issue with the hospital's ability to accurately track these requirements, including proper communications within the organization to navigate changes that could impact these requirements, such as an improvement to the existing learning management system. At the time of the breaches, the existing confidentiality agreement also fell short by not including acknowledgement of relevant privacy obligations under the *Act.*

[79] In terms of staff access to electronic health records, the hospital did not previously have a procedure in place to document access made outside of the staff's usual scope of practice, which would be instrumental for future audits and breach management to determine whether an unauthorized access has occurred. Furthermore, the HIS did not previously show a privacy warning to users to remind them of privacy requirements and the implications of unauthorized viewing of PHI.

[80] Furthermore, the deficiency in the audit functionality prevented the hospital from identifying patients associated with certain viewing activities, thus interfering with the hospital's breach management and its efforts to identify and notify the affected patients.

[81] In light of the above gaps and considering the specific circumstances of this case, I find that the hospital did not take reasonable steps to protect PHI of its patients, contrary to section 12(1).

[82] Nevertheless, I acknowledge that the hospital has taken significant steps to identify and remediate these gaps following discussions with the IPC. I am therefore satisfied that the hospital has responded adequately to the breaches in this case.

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

[83] Section 58(1) of the *Act* establishes the Commissioner's discretionary authority to conduct a review under the *Act,* 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.

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

CONCLUSION:

[85] This case highlights for health information custodians that cultivating privacy awareness of staff must be an integral part of the overall privacy frameworks aimed at mitigating the risk of unauthorized access or disclosure. This case also reminds custodians to report a privacy breach to the IPC in a timely manner and to ensure that the scope of PHI access authorized to staff is appropriate for their assigned duties and is properly documented and communicated internally.

[86] Based on the information before me, I find that unauthorized disclosure of PHI occurred when the security guard assigned on the hospital premises obtained access to PHI of patients and discussed it with the clerk in multiple instances.

[87] Further to the IPC's recommendation and in keeping with section 12(2) of the *Act*, the hospital notified the affected patients by way of a general notice. While I find that the notice has the requisite elements, I also find, in the circumstances of this case, that the notification was not made at the first reasonable opportunity as required under section 12(2)(a).

[88] I also find that unauthorized access occurred when the clerk accessed PHI of one patient without legitimate reasons related to her role, and that the patient was appropriately notified in keeping with section 12(2).

[89] Finally, I find, based on the gaps identified in the hospital's practices, that it did not take reasonable steps to protect PHI of its patients, contrary to section 12(1) of the *Act.* However, the hospital has acknowledged and took steps to address these gaps and improve its privacy practices. Accordingly, I am satisfied that that the hospital has responded adequately to the breaches in this case and find that no further review under Part VI of the *Act* is warranted in this case. However, in the foregoing sections, I have also provided recommendations for the hospital to further improve its information

practices.

NO REVIEW:

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

RECOMMENDATIONS:

I recommend that the hospital

- ensure, in the event of a future breach, that it notifies the IPC at the first reasonable opportunity;
- take steps necessary to ensure that any future changes made to the patient registration clerks' authorized scope of access to records of personal health information is properly documented and communicated internally;
- amend section 5.6 of its Privacy Breach Reporting and Management Framework policy to state that, pursuant to the *Act,* notification to the affected individuals should be completed at the first reasonable opportunity;
- revise section 5.8 of its Privacy Breach Reporting and Management Framework policy to state that, pursuant to Ontario Regulation 329/04 under the *Act,* the mandatory reporting to the IPC must be completed at the first reasonable opportunity; and
- amend its Privacy Breach Reporting and Management Framework policy to indicate the date on which the policy was put into effect.

Original Signed by: October 23, 2025

Francisco Woo
Investigator