Information and Privacy Commissioner,
Ontario, Canada

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

PHIPA DECISION 325

Complaint HR23-00383

A Public Hospital

January 20, 2026

Summary: A public hospital became aware of a potential privacy breach following a staff complaint that a physician had accessed personal health information (PHI) without authorization.

The hospital investigated the complaint and determined that the physician had accessed the health records of three patients without authorization and, in one case, disclosed PHI relating to one of those patients to other staff members. The hospital concluded that this conduct breached the privacy of the affected individuals under the *Personal Health Information Protection Act, 2004* (*PHIPA*) and reported the matter to the Office of the Information and Privacy Commissioner of Ontario (the IPC) on the basis that the physician knew or ought to have known that he was using and disclosing PHI without authority.

Following the breaches, the hospital investigated the matter, audited the physician's electronic health record accesses and implemented a number of remedial measures. These steps were generally consistent with the IPC's guidance on responding to privacy breaches. However, I was not satisfied that the hospital notified affected individuals at the first reasonable opportunity, as required by section 12(2)(a) of *PHIPA*.

I also find that, at the time of the breaches, gaps in physician privacy training and deficiencies in the hospital's confidentiality agreements and disciplinary policies meant that it did not take steps that were reasonable in the circumstances to protect PHI against unauthorized use or disclosure, as required by section 12(1) of *PHIPA*.

As these deficiencies were subsequently addressed through the hospital's remedial actions, and in light of the corrective measures implemented to reduce the risk of similar breaches occurring in the future, I conclude that a review of this matter under Part VI of *PHIPA* is not warranted.

Statutes Considered: *Personal Health Information Protection Act, 2004*, S.O. 2004, c. 3, sections 2, 3(1), 4(1), 12(1) and (2), 29 and 58(1).

BACKGROUND:

[1] A public hospital received a privacy complaint from its staff alleging that, in January 2023, a physician working in its intensive care unit (ICU) and general surgery unit had inappropriately viewed the health records of a patient's wife, who had been admitted to another related hospital, and disclosed details about the reasons for her admission to multiple staff members.

[2] In response to the complaint, the hospital interviewed the physician and audited his record accesses in its electronic health record (EHR) system. The hospital determined that the physician had used the personal health information (PHI) of three patients and, in one case, disclosed PHI relating to one of those patients, without authorization.

[3] The hospital concluded that the physician's conduct breached the affected individuals' privacy under the *Personal Health Information Protection Act, 2004* (*PHIPA*) and reported the matter to this office on the basis that the physician knew or ought to have known that he was using and disclosing PHI without authority.

[4] The matter proceeded to the Investigation Stage of the IPC's complaint process[1] because this office had concerns about whether, in the circumstances, the hospital had implemented information security practices that were reasonable to protect PHI against unauthorized use and disclosure by its agents.

[5] As part of my investigation, I requested and received written representations from the hospital, which I have considered in making this decision.

PRELIMINARY MATTERS:

[6] The hospital does not dispute, and I find, that:

- it is a "health information custodian" within the meaning of section 3(1) of *PHIPA*;
- the physician is an "agent" of the hospital within the meaning of section 2 of *PHIPA*;
- the affected health records contain "personal health information" within the meaning of section 4(1) of *PHIPA* and were in the hospital's custody or control; and

[1] This office opened a Custodian-Reported File to address this matter. See this office's "Code of Procedure for Matters under the *Personal Health Information Protection Act, 2004"* available at: https://www.ipc.on.ca/en/resources-and-decisions/code-procedure-matters-under-personal-health-information-protection-act-2004.

- the physician's unauthorized viewing and disclosure of this PHI was a "use" and "disclosure" by the hospital, within the meaning of section 2 of *PHIPA*, contrary to section 29 of *PHIPA*.[2]

ISSUES:

1. Did the hospital take reasonable steps to protect PHI in its custody or control against unauthorized use and disclosure?

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

DISCUSSION:

Issue 1: Did the hospital take reasonable steps to protect PHI in its custody or control against unauthorized use and disclosure?

[7] Section 12(1) of *PHIPA* requires that custodians take steps that are reasonable in the circumstances to protect PHI in their custody or control, 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.

Breach Response:

[8] In this matter, the physician's conduct breached the affected individuals' privacy. The IPC has held that section 12(1) includes a duty for custodians to respond adequately to a privacy breach.[3] The standard under this section is one of "reasonableness" and does not require perfection.[4]

[9] As set out in the IPC's "Responding to a Health Privacy Breach: Guidelines for the Health Sector" (the IPC's Privacy Breach Guidelines),[5] an adequate response to a privacy breach includes containment, investigation, notification and remedial measures to prevent recurrence.

Containment

[10] Between January 24 and 31, 2023, the hospital escalated the privacy complaint to

---

[2] See sections 2 [definitions], 3(1)4i [health information custodian], 4(1)(a) [personal health information], 17 [agents and information] and 29 [requirement for consent] of *PHIPA*.
[3] PHIPA Decision 44 at para. 140.
[4] PHIPA Decision 44 at para. 141.
[5] The IPC's Privacy Breach Guidelines is available at: https://www.ipc.on.ca/en/resources-and-decisions/responding-health-privacy-breach-guidelines-health-sector.

senior leadership, reviewed the audit findings related to the physician's EHR accesses, and advised him that the matter would be investigated.

[11] Regarding the privacy complaint, the audit revealed that, in January 2023, the physician accessed the health records of an ICU patient's wife who had been admitted to another hospital. During this access, he viewed her transcription, radiology and departmental reports, patient care inquiry and notes, and emergency department data, and, subsequently, disclosed information from these records to other staff members.

[12] The hospital determined that this access and disclosure were unauthorized because the physician was not providing the affected individual with active health care and did not have her consent to use or disclose her PHI.

[13] The audit also revealed that, in the same month, the physician accessed the health records of two deceased individuals who were former patients of his and spouses of ICU patients under his care. In these instances, he accessed their transcription reports and patient care inquiry information. The hospital determined that these accesses were unauthorized uses of PHI.

[14] The hospital confirmed that the physician did not make or retain any unauthorized copies of the affected PHI. Although, the hospital considered suspending the physician's access to its EHR system, it determined that doing so would pose a clinical risk within the ICU.

Investigation and Remediation

[15] The hospital interviewed the staff members who made the complaint and the physician, reviewed relevant patient health records, and audited the physician's EHR accesses.

[16] Through this investigation, the hospital determined that the physician believed it was permissible, from a privacy perspective, to access records he had previously authored to refresh his recollection of prior patient encounters and associated family relationships.

[17] To address the breaches, the hospital followed its disciplinary process and provided coaching and education to the physician regarding privacy obligations under *PHIPA*, including consent requirements and authorization to collect, use and disclose PHI. At the request of one affected individual, the hospital applied a "lock-box" to restrict access to that individual's records. [6]

[18] The hospital also took the following remedial steps:

---

[6] Certain provisions in *PHIPA*, in certain circumstances, allow individuals to withhold or withdraw their consent to the collection, use or disclosure of their PHI for a particular purpose, as well as provide express instructions to custodians not to use or disclose their PHI for health care purposes without consent. 'These provisions have come to be referred to as the "lock-box" provisions, although the term is not defined in *PHIPA*. For more information, please see the IPC's "Lock-box Fact Sheet".

- reviewed and updated relevant policies, procedures and agreements, with a focus on enhancing privacy training, awareness and risk management;
- launched a new privacy e-learning module for all agents, which includes an annual confidentiality agreement called the "privacy pledge";
- facilitated a privacy discussion with ICU staff; and
- in January 2024, incorporated annual privacy training, including the circumstances of this case, into the annual physician credentialing process.

Notification

[19] Section 12(2) of *PHIPA* requires custodians to notify affected individuals at the first reasonable opportunity of an unauthorized use or disclosure of their PHI and to include a statement of the individual's right to complain to the IPC.

[20] Section 12(2) states:

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

[21] The hospital notified the affected individuals by telephone and/or by letter in September 2023. I reviewed the notification letter and found that it complied with section 12(2)(b) of *PHIPA* and the IPC's Privacy Breach Guidelines.[7]

[22] However, the hospital became aware of the unauthorized uses and disclosure in January 2023 but did not notify the affected individuals until approximately nine months later.

[23] The hospital advised that, in two instances, notification was delayed due to concerns about the affected individual's personal circumstances. The hospital also advised that staffing changes within its privacy office during 2023 further contributed to the delay.

[24] This office has found that section 12(2)(a) of *PHIPA* does not permit extended

[7] See "Direct Notification to Affected Individuals" under step 3 in the IPC's Privacy Breach Guidelines in footnote 5.

delays once a breach has been identified.[8] In the circumstances of this case, while I accept that the hospital considered the potential impact of notification on the affected individuals, I am not satisfied that a delay of approximately nine months met the requirement to notify at the first reasonable opportunity.

Information Security Practices:

[25] The IPC has held that, under section 12(1), custodians have a related duty to implement and comply with information practices relating to PHI in their custody or control. These practices include administrative, technical and physical safeguards or measures, such as privacy policies, procedures and practices, audit functionality, and privacy training and awareness programs.[9]

[26] The hospital reported the breaches to this office on the basis that the physician knew or ought to have known that he was using and disclosing PHI without authority. In assessing the hospital's compliance with section 12(1), it is therefore necessary to consider the administrative, technical, and physical safeguards the hospital had in place to protect PHI against the risk of unauthorized use and disclosure by its agents.

[27] To that end, I reviewed the hospital's relevant information security policies, procedures declarations and agreements relating to privacy training and awareness, confidentiality, auditing and discipline.

Analysis

[28] While the hospital's containment, investigation and remedial steps were generally consistent with the IPC's Privacy Breach Guidelines[10], I am not satisfied that notification occurred at the first reasonable opportunity, as required by section 12(2)(a). Accordingly, I find that the hospital did not respond adequately to the breach.

[29] In determining whether the hospital took steps that were reasonable in the circumstances to protect the affected PHI against the risk of unauthorized use and disclosure by its agents, I considered the IPC's "Detecting and Deterring Unauthorized Access to Personal Health Information" paper, which provides guidance to custodians on minimizing the risk of unauthorized access by their agents.[11]

[30] Based on my review of the hospital's materials, I find that its information security practices are generally consistent with the recommended practices set out in this IPC

---

[8] See PHIPA Decisions 205 and 255, in which this office found that delays of over one year in notifying affected individuals did not meet the requirement in section 12(2)(a) to provide notice at the first reasonable opportunity.

[9] See PHIPA Decisions 69, 70, 74 and 80 and 110. Sections 10(1) and (2) of *PHIPA*, impose a duty on custodians to put information practices in place and comply with them. The term "information practices" is defined in section 2 of *PHIPA* to include "the administrative, technical and physical safeguards and practices that the custodian maintains with respect to the information."

[10] See steps 1, 2 and 4, as well as "How to Minimize the Risk of a Privacy Breach" in the IPC's Privacy Breach Guidelines in footnote 5.

[11] The IPC's Detecting and Deterring Unauthorized Access to Personal Health Information.

guidance.

[31] However, at the time of the privacy breaches, the hospital advised that its physicians were not required to complete annual privacy training. In my view, this gap in training is reflected in the physician's mistaken belief that authorship of a record permitted later access.

[32] Further, the hospital's confidentiality agreement did not contain the following elements that IPC guidance recommends be included:

- set out the purposes for which agents are permitted to collect, use and disclose PHI, as well as any limitations, conditions or restrictions placed on such collection, use and disclosure;
- prohibit agents from collecting, using or disclosing PHI if other information will serve the purpose and from collecting, using or disclosing more PHI than is reasonably necessary to meet the purpose;
- specify that random audits will be conducted; and
- require agents to comply with *PHIPA* and its regulations.[12]

[33] Moreover, the hospital's disciplinary policies did not clearly set out, as recommended by IPC guidance, the potential consequences that may be imposed on agents who collect, use or disclose PHI without authorization under *PHIPA* or in contravention of the hospital's privacy-related policies and procedures.[13]

[34] These shortcomings limited the hospital's ability to effectively prevent and deter unauthorized access to PHI by its agents. Accordingly, I find that, at the time of the breaches, the hospital did not take steps that were reasonable in the circumstances to protect PHI, as required by section 12(1).

[35] However, there is no evidence of an ongoing risk to PHI arising from the physician's conduct. Further, as outlined above, the hospital has since strengthened its information security practices, particularly, its privacy training and awareness for its agents.

[36] In the circumstances and having regard to the hospital's corrective actions and improvements to its privacy framework, I am satisfied that the hospital has taken reasonable and meaningful steps to address the breaches and reduce the risk of similar incidents occurring in the future.

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

[12] See footnote 13 at page 16, which discusses confidentiality agreements and minimum recommended content.
[13] See footnote 13 at page 25, which sets out information that agents should be made aware of under a custodian's policy and procedures relating to discipline.

[37] 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 *PHIPA* or its regulations and that the subject-matter of the review relates to the contravention.

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

RECOMMENDATION:

In light of my finding that the hospital did not notify affected individuals at the first reasonable opportunity, I recommend that, in future privacy breaches involving the theft, loss, or unauthorized use or disclosure of PHI in its custody or control, the hospital ensure that affected individuals are notified in accordance with 12(2)(a).

Original Signed by: January 20, 2026

John Gayle
PHIPA Mediator/Investigator