Information and Privacy Commissioner,
Ontario, Canada

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

PHIPA DECISION 324

Complaint HI23-00022

A Medical Centre

January 13, 2026

Summary: The Office of the Information and Privacy Commissioner of Ontario (the IPC) became aware of a potential privacy breach following a complaint that a medical centre failed to respond to an access request for paper medical charts stored off-site.

The medical centre later issued a decision advising that the responsive records, which contained personal health information (PHI), had been destroyed as a result of flood damage and no longer existed. The destruction of the records was a loss of PHI within the meaning of section 12(1) of the *Personal Health Information Protection Act, 2004* (*PHIPA*) and, therefore, a privacy breach.

Following the breach, the medical centre confirmed that the records were securely destroyed, and took investigative and remedial steps. While these actions were generally consistent with IPC guidance on responding to privacy breaches, I was not satisfied that the medical centre notified affected individuals in accordance with section 12(2)(b) of *PHIPA*, which requires that notice of a loss include a statement of the individual's right to make a complaint to this office. Accordingly, I find that the medical centre did not respond adequately to the breach.

I also find that the medical centre's contracting arrangements with the storage provider did not adequately address environmental risks, including flood damage, associated with off-site physical storage that were contemplated at the time of contracting. These deficiencies fell short of the recommended practices set out in IPC guidance on contracting with third-party service providers. As a result, I find that the medical centre did not take steps that were reasonable in the circumstances to protect PHI against loss, as required by section 12(1).

However, in light of the corrective measures the medical centre has since implemented to prevent a similar loss, I conclude that a review under Part VI of *PHIPA* is not warranted.

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

BACKGROUND:

[1] The Office of the Information and Privacy Commissioner of Ontario (IPC) became aware of a potential privacy breach under the *Personal Health Information Protection Act, 2004* (*PHIPA*) after receiving a complaint that a medical centre failed to respond to an access request for paper medical charts originally held by a medical practice that the centre had taken over.

[2] The medical centre advised that, following the takeover, it digitized some patient charts into its electronic medical records system. The remaining paper charts, including those responsive to the request, were placed in storage with a third-party service provider (the storage company).

[3] The medical centre further advised that it was initially unable to process the access request because the storage company did not respond to its telephone calls or registered letters.

[4] Eventually, by letter dated June 5, 2023, the storage company informed the medical centre that the stored charts had been destroyed after being damaged by a flood, as follows:

> …the files that are being requested are not available for transfer. The forms/documents that you are requesting were destroyed. Unfortunately, the files were kept in the basement. There was a large flood…All paperwork was completely wet, and boxes were covered in mold. We had no option but to professionally and securely destroy all files.

[5] The medical centre subsequently issued a final access decision advising the complainant that the responsive records had been destroyed and no longer existed.

[6] Although the access complaint was resolved, 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 medical centre had implemented information security practices that were reasonable to protect personal health information against loss.

[7] As part of my investigation, I requested and received written representations from

---

[1] This office opened an IPC-Initiated File to address this potential contravention of *PHIPA*. 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 medical centre, which I have considered in making this decision.

PRELIMINARY MATTERS:

[8] The medical centre does not dispute, and I find that:

- it is a "health information custodian" within the meaning of section 3(1) of *PHIPA*;
- the destroyed medical charts contained "personal health information" (PHI) within the meaning of section 4(1) of *PHIPA* that were in the medical centre's custody or control; and
- the destruction of the charts was a "loss" of PHI within the meaning of section 12(1) of *PHIPA*.

ISSUES:

1. Did the medical centre take reasonable steps to protect PHI in its custody or control against loss?
2. Is a review warranted under Part VI of *PHIPA*?

DISCUSSION:

Issue 1: Did the medical centre take reasonable steps to protect PHI in its custody or control against loss?

[9] 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

[10] The destruction of the paper medical charts as a result of flood damage was a loss of PHI and, therefore, a privacy breach.

[11] The IPC has held that section 12(1) includes a duty for custodians to respond

adequately to a privacy breach.[2] The standard under this section is one of "reasonableness" and does not require perfection.[3]

[12] As set out in the IPC's "Responding to a Health Privacy Breach: Guidelines for the Health Sector" (the IPC's Privacy Breach Guidelines),[4] an adequate response to a privacy breach may include determining the scope of the breach and containing it, notifying affected individuals and, where appropriate, reporting the breach to this office, investigating the cause of the breach, and taking remedial measures to reduce the risk of a similar breach occurring.

Containment

[13] The storage company advised the medical centre that the damaged charts were professionally and securely destroyed. As a result, there does not appear to be any ongoing risk of the affected PHI being collected, used or disclosed contrary to *PHIPA*.

Notification

[14] Section 12(2) of *PHIPA* requires custodians to notify individuals at the first reasonable opportunity of the theft, loss, or unauthorized use or disclosure of their PHI and to include in that notice a statement of the individual's right to complain to the IPC.

[15] 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,
>
> 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.

[16] The medical centre advised that 102 patient charts were affected and that all affected individuals were promptly notified after learning of the destruction. It further advised that notification occurred directly by telephone and through posted notices within

---

[2] PHIPA Decision 44 at para. 140.
[3] PHIPA Decision 44 at para. 141.
[4] 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.

the centre.

[17] Despite my request, the medical centre did not provide me with a copy of the posted notices and I, therefore, did not have an opportunity to review their contents. Also, the medical centre did not confirm whether the affected individuals were informed of their right to make a complaint to this office.

[18] Accordingly, I am not satisfied that the medical centre's notice to affected individuals complied with section 12(2)(b).

Investigation and Remediation

[19] The medical centre undertook several investigative steps, including repeated efforts to obtain information about the flood from the storage company, an internal assessment to identify affected records and patients, and a review of its storage-related contractual arrangements and related policies.

[20] The medical centre's remedial measures included ceasing the use of off-site physical storage and digitizing remaining paper charts. It also updated policies governing record retention, physical security measures and third-party service provider agreements relating to the handling of PHI.

Information Security Practices

[21] 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.[5]

[22] Custodians must also maintain and periodically review these practices to ensure they remain "reasonable in the circumstances", identify privacy risks, take reasonable measures to reduce or eliminate those risks, and mitigate the potential harms that may arise.[6]

[23] Again, the applicable standard is one of "reasonableness" and does not require perfection.[7]

---

[5] 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."

[6] See PHIPA Decisions Decisions 64, 70, 163 and 174; and IPC Orders HO-010 and HO-013.

[7] PHIPA Decision 44 at para. 141.

[24] In this matter, the PHI was lost as a result of flood damage at the storage company. In assessing the medical centre's compliance with section 12(1), it is therefore necessary to consider the administrative, technical, and physical safeguards the medical centre had in place to protect PHI stored off-site.

[25] As part of my investigation, I reviewed the "Storage Agreement For Medical Practice Paper Charts" dated March 1, 2015 (the Agreement) that the medical centre entered into with the storage company to "securely store paper medical charts containing PHI of inactive patients".

[26] The Agreement required compliance with *PHIPA*, stated that the storage area would be maintained to prevent environmental damage, such as flooding, and provided:

> [The storage company] will take all reasonable measures to protect the stored charts. However, in the event of unforeseen circumstances (e.g. natural disasters, flooding), [the storage company] will promptly notify the [medical centre] and collaborate on mitigation measures.

Analysis

[27] With respect to the medical centre's response to the breach, I find that its containment, investigation and remedial steps were generally consistent with the IPC's Privacy Breach Guidelines. [8]

[28] However, because I am not satisfied that the affected individuals were notified in accordance with section 12(2)(b), I find that the medical centre did not respond adequately to the breach.

[29] In determining whether the medical centre took steps that were reasonable in the circumstances to protect the affected PHI from loss, I considered the IPC's guidance on "Privacy and Access in Public Sector Contracting with Third Party Service Providers".[9] While directed primarily at public sector institutions, the recommended practices set out in this guide are informative when assessing the reasonableness of privacy safeguards in third-party service agreements.

[30] Before entering into service agreements, institutions should identify and mitigate potential privacy and security risks, and define, among other things:

- the specific privacy and security requirements to be imposed on the service provider;

---

[8] 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 4.

[9] IPC Guidance: Privacy and Access in Public Sector Contracting with Third Party Service Providers.

- processes for monitoring and evaluating the service provider's compliance with those requirements; and

- how the prospective service provider's capacity to meet those requirements will be assessed and documented.[10]

[31] In addition, institutions should conduct a privacy impact assessment (PIA) and consider whether the prospective service provider should also be required to conduct a PIA.[11]

[32] It is further recommended that the eventual agreement with a third-party service provider define, among other things:

- requirements to test, verify and provide documentation about the security measures in place;

- how privacy and security protections will be monitored to ensure compliance with the agreement; and

- reporting requirements and related documentation that the service provider must provide to demonstrate its compliance with security and privacy policies.[12]

[33] In my view, the Agreement imposed only general obligations on the storage company to comply with *PHIPA* and to take measures to protect the stored charts.

[34] The medical centre did not, before entering into the Agreement, define specific security requirements relating to how the storage area would be maintained to prevent environmental damage. Nor did the medical centre define processes for monitoring or evaluating whether the storage company was taking "all reasonable" protective measures, or assess the storage company's capacity to manage environmental risks.

[35] Further, the Agreement did not require testing or verification of security measures, periodic reporting, or documentation demonstrating compliance with security requirements relating to mitigation of environmental risks.

[36] Moreover, the medical centre advised that neither it nor the storage company conducted a PIA prior to storing the records.

[37] These omissions represent deficiencies in the medical centre's practices when planning for and entering into agreements with service providers. They limited the

---

[10] See section 1.4. "Defining requirements for service providers" in the IPC guidance document referenced in footnote 7.
[11] See section 1.3. "Identifying and mitigating privacy and security risks" in the IPC guidance document referenced in footnote 7.
[12] See section 2.10 "Monitoring the service provider's compliance with the agreement" in the IPC guidance document referenced in footnote 7.

medical centre's ability to identify and manage privacy risks associated with the off-site storage of the affected records, maintain accountability for their protection, and ensure that the Agreement satisfied the security requirements for PHI under section 12(1).

[38] While the existence of the Agreement is relevant, it does not, on its own, establish that the medical centre took reasonable steps to protect the affected PHI from loss resulting from environmental risks, including flooding.

[39] I note that the storage company's letter stated that, "[u]nfortunately, the files were kept in the basement." While I make no findings about the specific storage practices employed by the storage company, this information indicates that the risk of flood damage was not merely theoretical. In these circumstances, it reinforces the need for the medical centre to have ensured that effective safeguards were in place to address environmental risks associated with off-site storage.

[40] I also note that the Agreement was entered into in March 2015. Although the evidence before me does not establish when the flood occurred, section 12(1) requires custodians to ensure that the safeguards protecting PHI remain reasonable in the circumstances over time. As indicated above, this includes an obligation to periodically review and reassess information practices and third-party service arrangements, particularly where records are stored off-site and subject to inherent environmental risks. In the absence of evidence that the medical centre undertook any such review or reassessment of the Agreement or the storage arrangements for the affected PHI after entering it, reliance on the original contractual terms alone is insufficient to demonstrate ongoing compliance with section 12(1).

[41] I further note that the Agreement both required the storage area to be maintained to prevent environmental damage such as flooding, and described flooding as an "unforeseen circumstance." While I make no findings about the drafting of the Agreement or the parties' intentions, this inconsistency shows the importance of clearly identifying foreseeable environmental risks and allocating responsibility for mitigating those risks through specific, verifiable security requirements. In the absence of such clarity, reliance on general contractual assurances is insufficient to demonstrate that reasonable steps were taken in the circumstances to protect PHI against loss.

[42] Moreover, given the environmental risks associated with off-site physical storage that were within the parties' contemplation at the time of contracting, including the risk of flood damage, specific safeguards and oversight mechanisms were reasonably required to protect the affected records.

[43] For these reasons, I find that the medical centre did not take steps that were reasonable in the circumstances to ensure that PHI in its custody or control was protected against loss, as required by section 12(1).

[44] However, in the aftermath of this breach, the medical centre acknowledged these

shortcomings, recognized that failing to digitize all the inactive patients' paper medical charts before storing them off-site introduced the unnecessary privacy risk, and developed a formalized PIA process.

[45] In addition to now prioritizing secure digital solutions, the medical centre advised that, going forward, it will take the following steps when contracting with third-party service providers:

- require that a PIA be conducted before entering into any agreement;
- include explicit privacy breach definitions in the agreement;
- require detailed terms around privacy and security compliance monitoring; and
- schedule periodic performance reviews and compliance checks.

[46] Although I have found that the medical centre did not respond adequately to the breach due to insufficient notification under section 12(2)(b) and did not take reasonable steps to protect PHI against loss, as required by section 12(1), there is no evidence of any ongoing risk to PHI and the affected individuals were informed of the loss, although not in full compliance with section 12(2)(b).

[47] Further, the medical centre took remedial measures consistent with IPC guidance to prevent a similar loss.

[48] In the circumstances and having regard to the medical's centre's corrective actions and improvements to its privacy framework, I am satisfied that the medical centre has taken reasonable and meaningful steps to address the breach and reduce the risk of a similar loss occurring in the future.

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

[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 *PHIPA* 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 *PHIPA*, and for the reasons set out above, I find that a review is not warranted.

RECOMMENDATION:

In light of my finding that the medical centre's notification to affected individuals did not comply with section 12(2)(b) of *PHIPA*, I recommend that the medical centre ensure that, in future privacy breaches involving the theft, loss, or unauthorized use or disclosure of PHI in its custody or control, any notification to affected individuals includes a statement informing them of their right to make a complaint to the IPC, as required by section 12(2)(b).

Original Signed by: January 13, 2026

John Gayle
Investigator