Recent PHIPA Decisions

John Gayle, Investigator

Suzanne Brocklehurst, Director of Early Resolution

Office of the Information and Privacy Commissioner of Ontario

Information and Privacy Commissioner of Ontario

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

CELHIN

Dec. 6, 2024

Overview

- PHIPA Decision 260
- PHIPA Decision 264
- Early Resolution – HR23-00282 – Prescribed Entity
- Questions?

PHIPA Decision 260 – What Happened?

- Snooping (i.e. unauthorized use) by a physician at the hospital
- Over 3,900 patient charts accessed without authorization
- Remediation focused on privacy training, confidentiality agreements and privacy policies

PHIPA Decision 260 – Information Practices

- Section 10 of *PHIPA*:

> (1) A health information custodian that has custody or control of personal health information shall have in place **information practices** that comply with the requirements of this Act and its regulations.
>
> (2) A health information custodian **shall comply** with its information practices.

- Section 2 of *PHIPA*:

> "information practices", in relation to a health information custodian, means the policy of the custodian for actions in relation to personal health information, including,
>
> (b) the **administrative**, technical and physical safeguards and practices that the custodian maintains with respect to the information;

PHIPA Decision 260 – Security

- Section 12 of *PHIPA*:

> (1) A health information custodian shall take steps that are reasonable in the circumstances to ensure that personal health information in the custodian's custody or control is protected against theft, loss and **unauthorized use** or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal.

PHIPA Decision 260 – Key Takeaways

- Administrative Safeguards are important for satisfying section 12(1) of *PHIPA*

    - Privacy Policies and Procedures
    - Privacy Training and Awareness
    - Confidentiality Agreements

PHIPA Decision 264 – What Happened?

- Snooping (i.e. unauthorized use) by a radiologist at the hospital
- Health records of patients, including some who were known to the radiologist, accessed without authorization
- Remediation focused on EHR auditing deficiencies

PHIPA Decision 264 – Information Practices

- Section 10 of *PHIPA*:

> (1) A health information custodian that has custody or control of personal health information shall have in place **information practices** that comply with the requirements of this Act and its regulations.
>
> (2) A health information custodian **shall comply** with its information practices.

- Section 2 of *PHIPA*:

> "information practices", in relation to a health information custodian, means the policy of the custodian for actions in relation to personal health information, including,
>
> (b) the administrative, **technical** and physical safeguards and practices that the custodian maintains with respect to the information;

PHIPA Decision 264 – Security

- Section 12 of *PHIPA*:

> (1) A health information custodian shall take steps that are reasonable in the circumstances to ensure that personal health information in the custodian's custody or control is protected against theft, loss and **unauthorized use** or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal.

PHIPA Decision 264 – Key Takeaways

- Technical safeguards are important for satisfying section 12(1) of *PHIPA*
    - Logging, Auditing and Monitoring

HR23-00282 – Prescribed Person – What Happened?

- In May 2023, a prescribed person (registry for perinatal, newborn, and child registry to facilitate quality of care), was subject to a cybersecurity breach
- Breach was caused by a global zero-day vulnerability in the software – MOVEit file transfer program (used to perform secure file transfers)
- 3.4 million may have been affected including, pregnant individuals and children.

Scope of the Breach

- The personal health information that was accessed and exfiltrated was collected on the registry from 242 health care facilities and providers across Ontario regarding fertility, pregnancy, newborn and child health care offered between January 2010 and May 2023.
- The registry contained very sensitive information.
- While data was exfiltrated, there was no evidence of further misuse of the data (for example on the dark web).

Notification Efforts – A Unique Situation

- Prescribed Persons are not required to directly notify individuals of a breach
- The *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities* indicates that:
  - …as a secondary collector of PHI, a PP or PE should not directly notify the individual to whom the PHI relates of a privacy breach. Where applicable, the required notification to individuals must be provided by the relevant custodian(s), unless an alternative decision regarding breach notification to affected individuals is approved by the IPC
- The unique circumstances of this breach called for an alternative approach to notification

Notification

After consultation with the IPC the PP notified as follows:

- Notice to Affected Health Information Custodians
  - Notified on June 6, 2023
  - Update on June 28, 2023
  - Invited to Townhalls and webinars hosted by the PP & Breach Counsel (throughout July, 2023)

Notice

Notice to Affected Individuals:

- Conducted a centralized and coordinated indirect notification process in conjunction with impacted health care providers, to ensure affected individuals received clear, consistent, and safe messaging about the breach, and were provided multiple, equitable avenues for additional information.

Indirect Notice Process

- Public notification using media and health information custodian websites indicating the nature of the incident and direction to visit the prescribed person's incident website.
- Multi-lingual translated incident website for more information, with self identification questions to allow individuals to determine if they were impacted by the incident.
- Hotline for questions (English and French) Monday to Friday 8am-4pm ET.
- Escalation to the prescribed person's agents for more detailed questions, as required.

Key takeaways:

Indirect vs. Direct Notice

- Direct Notice is always preferable
  - More likely to draw the individual's attention to their potential involvement in a breach vs. a posted notice.
- Considerations for Indirect Notice:
  - Significant number of affected parties
  - Likelihood of outdated contact information
  - Is direct notice reasonably likely to pose a risk of harm to individuals

Key takeaways for rolling out Indirect Notice

Need to take reasonable steps to bring the Indirect Notice to the attention of affected parties.

- Multi-media strategy should be considered including:
  - Prominent notices on the landing page of a custodian's website
  - Posts on the custodian's social media accounts
  - Physical on-site posters in high traffic areas
  - Advertisements in newspapers
  - Need to be posted for a length of time that allows affected parties to come into contact with the posting

Questions?

HOW TO CONTACT US

Information and Privacy Commissioner of Ontario

2 Bloor Street East, Suite 1400

Toronto, Ontario, Canada M4W 1A8

Phone: (416) 326-3333 / 1-800-387-0073

TDD/TTY: 416-325-7539

Web: www.ipc.on.ca

E-mail: info@ipc.on.ca

My contact: jesse.campbell@ipc.on.ca

Media: media@ipc.on.ca / 416-326-3965