HEALTH

JANUARY 2024

Administrative Monetary Penalties: Guidance for the Health Care Sector

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

As a modern and effective regulator, the Information and Privacy Commissioner of Ontario (IPC) can help build trust in the health system with flexible and balanced approaches that meaningfully address non-compliant behaviours while promoting and encouraging accountability, learning, and continuous improvement.

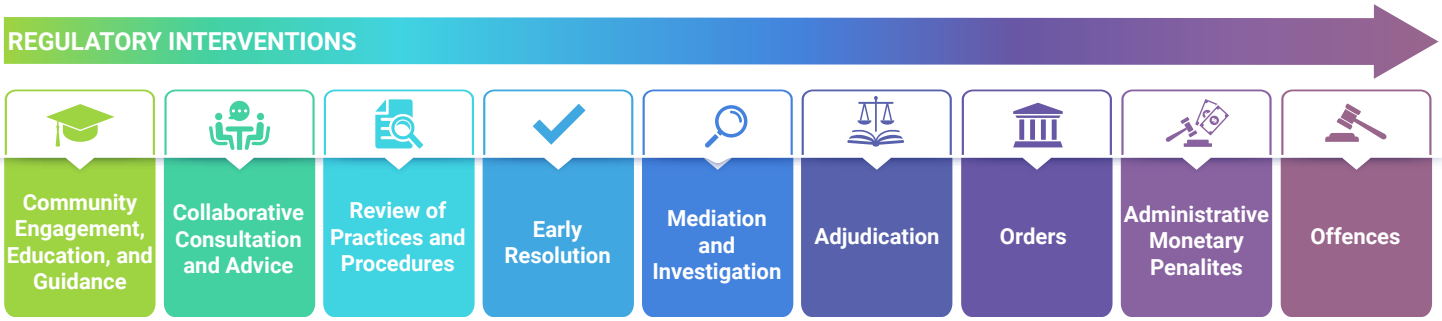
In 2020, the Ontario legislature amended the *Personal Health Information Protection Act* (PHIPA) to provide the IPC with additional enforcement powers that would allow it to impose administrative monetary penalties (AMPs) on organizations or individuals that contravene the act or its regulations.[1] AMPs may be issued for the purposes of encouraging compliance with PHIPA or preventing a person from deriving — directly or indirectly — any economic benefit from contravening the law.

The IPC's use of this additional enforcement power is governed by **section 61.1 of PHIPA** and an accompanying **regulation** [O. Reg. 329/04, s. 35] that took effect on January 1, 2024.

AMPs are part of the IPC's broader regulatory toolkit for encouraging compliance with PHIPA in a manner that is flexible, balanced, and progressive. The IPC's ability to directly impose AMPs provides additional flexibility to address contraventions of PHIPA with appropriate and meaningful consequences, depending on their level of severity. AMPs are but one option among the range of escalating actions and interventions available to the IPC, short of referring offences to the Attorney General of Ontario for prosecution (see Figure 1).

The IPC takes a measured and proportionate approach to assessing the most appropriate way of addressing each contravention. Similar to the values and principles underlying a *just culture* approach, we apply our statutory responsibilities in a way that balances the need for accountability and continuous learning. A just culture approach[2] generally emphasizes the value of openly reporting and learning from medical errors that occur in complex systems, while reserving more severe consequences for cases where stronger interventions are necessary to ensure proper accountability.

FIGURE 1. A TOOLKIT OF PROGRESSIVE ENFORCEMENT OPTIONS UNDER PHIPA



This figure illustrates the progressive levels of regulatory intervention in the IPC 'toolkit.' This does not include all the regulatory tools potentially available to the IPC, and all the regulatory tools identified are not available in every situation.

The IPC takes into consideration numerous factors, including risks, impacts, and behaviours, when deciding how best to address a contravention. For example:

- In the vast majority of cases, those who work for and contribute to Ontario's health care system are deeply committed to protecting personal health information. They show a genuine willingness to report, take responsibility for, and remedy errors when they occur. These cases often involve

1 PHIPA clause 61(1)(h.1) and section 61.1

2 "Just Culture", an approach commonly used in the health sector to enhance patient safety, is summarized by David Marx in his seminal paper. Marx DA. *Patient Safety and the "Just Culture": A Primer for Health Care Executives.* New York, NY: Trustees of Columbia University; 2001.

inadvertent errors, one-off contraventions with relatively minor impact, or some at-risk behaviours in need of coaching and course correction. In most cases, the individual or organization is highly responsive and cooperative in rectifying the situation. Education, guidance, early resolution, and recommendations for corrective measures are often the only tools the IPC needs to use in such cases.

- In cases where IPC recommendations are not likely to be accepted and implemented, the IPC has the discretion to initiate a formal review under section 57 or 58 of PHIPA and issue non-monetary orders that are binding and enforceable in court. These non-monetary orders may require individuals or organizations to take specific actions to address shortcomings in their practices and policies to be compliant with PHIPA. For example, the IPC might order an individual or organization to change their information practices to strengthen the reasonable safeguards necessary to protect the privacy and confidentiality of the personal health information that they hold.
- In more serious cases, an order imposing AMPs may be a more appropriate consequence for ensuring accountability in accordance with the purposes set out in the law. As with non-monetary orders (above), AMPs can only be imposed after a review is conducted and once issued, they are binding and enforceable. In such cases, the IPC will use the criteria set out in regulation (see Figure 2 below) to guide the amount of the AMP to be imposed, up to the maximum possible ($50,000 for an individual and $500,000 for an organization). Penalty amounts may be less than the maximums, or conversely, the IPC may increase the penalty amounts above these maximums to prevent an individual or organization from economically benefiting from their contravention.
- For the most severe contraventions, the IPC may refer cases to the Attorney General for prosecution where the Commissioner is of the view that there is evidence of an offence having been committed. An individual found guilty of committing an offence under PHIPA can be liable for a fine of up to $200,000, up to one year imprisonment, or both. An organization can be liable for a fine of up to $1,000,000.

WHEN WOULD AN AMP BE APPROPRIATE?

Over the years, cases investigated by the IPC may have been good candidates for an order to impose an AMP. Examples of these contraventions might include:

- **Serious *snooping* into patient records:** Unfortunately, there have been situations where individuals working in the health care system have taken improper advantage of their access privileges and violated the privacy of patients by accessing their health records without authorization for motives completely unrelated to their health care. In serious cases of this nature, the IPC might consider that imposing an AMP on such an individual would be an appropriate consequence to encourage future compliance with PHIPA.
- **Contraventions for economic gain:** In previous cases before the IPC, agents of a hospital were found to be accessing patient records and improperly using and disclosing personal health information without authority for the purpose of selling products or services related to the information. If similar cases were to come before the IPC after January 1, 2024, the IPC could consider imposing AMPs where appropriate to prevent the agent from directly or indirectly deriving any economic benefit as a result of contravening PHIPA.
- **Disregard for individual's right of access:** Individuals have a right of access to records of their own personal health information that are in the custody or control of a health information custodian (HIC), subject to limited and specific exceptions. An AMP may be an appropriate enforcement tool to consider in cases where a HIC has persistently failed to comply with PHIPA

requirements for responding to access requests or has unlawfully destroyed or abandoned health records. In such cases, an AMP could encourage HICs to comply with their legal obligations to protect records of personal health information and provide timely access to the records on request, subject to applicable exemptions.

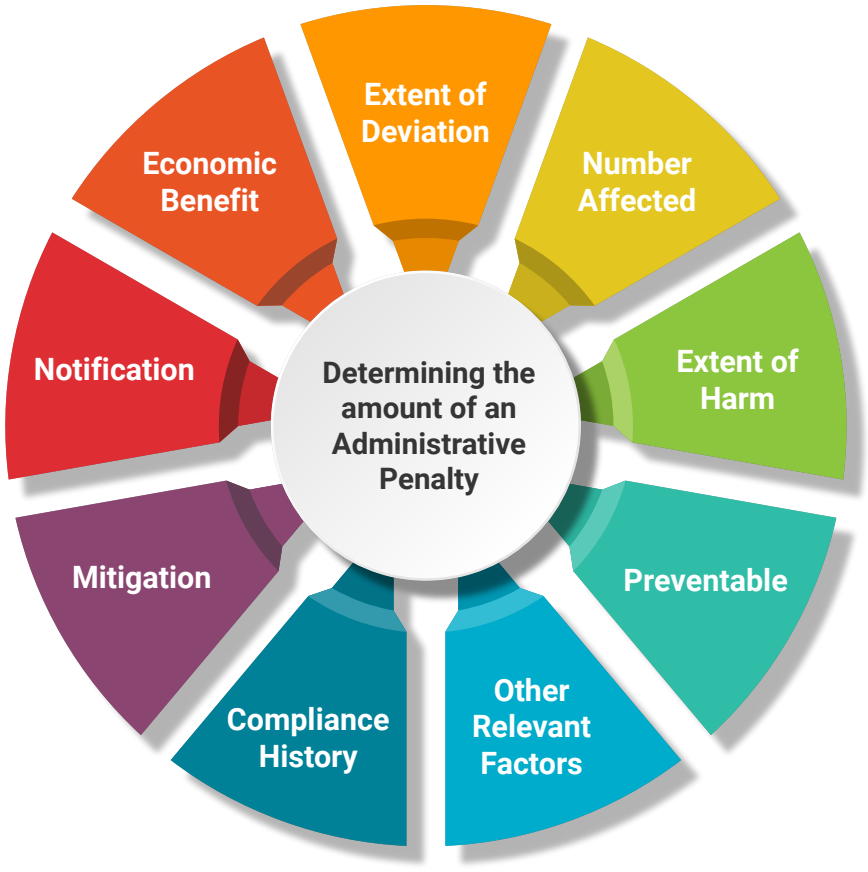
The IPC would not typically consider the use of AMPs in cases involving unintentional errors or one-off mistakes, such as misdirected faxes or emails, provided there is evidence of prompt and reasonable corrective action being taken upon discovery of the error to contain its impact and prevent it from recurring or becoming a more systemic issue.

Similarly, AMPs may not be an appropriate enforcement tool against an organization that, despite having reasonable safeguards consistent with leading best practice, has been the victim of a cyberattack that could not have been reasonably foreseen or avoided, provided it has fully cooperated in containing the harm, notified affected individuals where required, and taken the additional security measures needed to mitigate the risks of a similar attack happening again.

The examples above are not exhaustive and do not limit the circumstances in which the IPC may impose an AMP. The IPC will consider which orders warrant AMPs on a case-by-case basis.

FIGURE 2. DETERMINING THE AMOUNT OF AN ADMINISTRATIVE MONETARY PENALTY

The PHIPA **regulation** requires the IPC to consider certain criteria in determining the amount of an AMP. These criteria help to assess the scope, scale, and impact of a contravention and to evaluate attempts made to correct or contain potential harms. They also consider whether it would have been possible to prevent the contravention and any history of contraventions of the individual or organization on whom the penalty is imposed. The IPC must also consider any potential economic benefit to the individual or organization that might have resulted from the contravention. Specifically, the regulation requires the IPC to assess:



1. The extent to which the contraventions deviate from the requirements of PHIPA or its regulation(s)
2. The extent to which the person could have taken steps to prevent the contraventions
3. The extent of the harm or potential harm to others resulting from the contraventions
4. The extent to which the person tried to mitigate any harm or potential harm or took any other remedial action
5. The number of individuals, health information custodians and other persons affected by the contraventions
6. Whether the person notified the IPC and any individuals whose personal health information was affected by the contraventions
7. The extent to which the person derived or reasonably might have expected to derive, directly or indirectly, any economic benefit from the contraventions
8. Whether the person has previously contravened PHIPA or its regulation(s).

The IPC may also consider any other relevant criteria in determining the amount of an AMP.

Administrative Monetary Penalties: Guidance for the Health Care Sector

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

2 Bloor Street East, Suite 1400
Toronto, Ontario
Canada M4W 1A8

Web site: www.ipc.on.ca
Telephone: 416-326-3333
Email: info@ipc.on.ca

January 2024