Information and Privacy Commissioner,
Ontario, Canada

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

PHIPA DECISION 204

Complaint HI22-00001

A Public Hospital

April 4, 2023

Summary: A public hospital (the hospital) reported three separate privacy breaches under the *Personal Health Information Protection Act, 2004* (the *Act*) to the Information and Privacy Commissioner of Ontario. Each breach involved unauthorized access to patients' personal health information by an employee of the hospital. In light of the steps taken by the hospital to address the breaches, no formal review of this matter will be conducted under Part VI of the *Act*.

Statutes Considered: *Personal Health Information Protection Act, 2004*, S.O. 2004, c. 3, sections 2, 3(1), 4(1), 10(1), 12(1) and 29.

BACKGROUND:

[1] Under the *Personal Health Information Protection Act* (the *Act* or *PHIPA*), a public hospital (the hospital) reported three separate privacy breaches to the Information and Privacy Commissioner of Ontario (the IPC or this office) that occurred in 2020 and 2021. All three breaches involved an employee of the hospital who had looked at the personal health information (PHI) of patients for a non- work-related purpose, that is, "snooped" in their health records.[1]

[2] For each breach, this office opened a Custodian-Reported File at the Intake

[1] "Snooping" is a type of inappropriate use of information in which the affected individual's PHI is looked at without authorization. See "Reporting a Privacy Breach to the IPC."

Stage of the IPC's *PHIPA* complaint process.[2] However, because the breaches were similar, this office was concerned that there might be a systemic issue relating to snooping by the hospital's staff that needed to be addressed. More specifically, this office had concerns that the information practices in place at the hospital to detect, prevent and reduce the risk of unauthorized access to PHI by its staff might not be in accordance with the *Act*.

[3] For these reasons, this office opened a Commissioner-Initiated File at the Investigation Stage of the IPC's *PHIPA* complaint process. As part of my investigation, I requested and received written representations, discussed below, from the hospital.

The Reported Breaches

Reported Breach #1:

[4] The hospital advised this office that, after the publication of a local media story on September 4, 2020, on the same date, it performed an ad hoc audit of the accesses to the electronic health record (EHR) of the patients named in the story. The hospital also advised that this audit revealed eight suspected unauthorized accesses to the EHR of these patients by a Patient Accounts Clerk (the accounts clerk) employed by the hospital.

[5] In response to the suspected breach, the hospital advised that it performed a second audit, for the period of June 1, 2020 to September 4, 2020, which reviewed all of the EHR accesses by the accounts clerk. The hospital also advised that it performed a third audit, for the period of January 1, 2020 to September 4, 2020, that looked specifically at all of the accesses by the accounts clerk to the EHRs of the accounts clerk's spouse and, any patients with the same last name as the accounts clerk or the same last name of the accounts clerk's spouse.

[6] The hospital reported that the three audits revealed that the accounts clerk had, in total, potentially accessed the EHRs of 28 patients without authorization for the period of January 1, 2020 to September 4, 2020. Further, the hospital advised that the accounts clerk searched specifically for the EHRs of these affected patients and that the PHI that was accessed without authorization included some or all of the following for each patient: name, address, telephone number, date of birth, sex, health card number, employer information, reason for visit, diagnosis, discharge disposition, admitting, attending and family physician, next of kin, person to notify, guarantor name, most recent room assignment, and the hospital's account charges, statements and insurance billings.

[7] The hospital advised that the accounts clerk began working at the hospital on September 9, 1991 and had signed a Statement of Confidentiality at that time, as well

[2] See the IPC's "Code of Procedure for Matters under the *Personal Health Information Protection Act, 2004*".

as during the hospital's annual privacy refreshers on November 19, 2019 and May 19, 2020. As part of its investigation into the breach, the hospital advised that, on September 8, 2020, it confirmed with the manager of the accounts clerk that there was no work-related reason for the accounts clerk to have accessed the affected patients' EHRs.

[8] To contain the breach, in accordance with its policy and privacy breach protocol relating to the unauthorized access of PHI, the hospital advised that it placed the accounts clerk, who was not a member of a regulatory college, on administrative leave and disabled all of their access to its EHR on September 8, 2020.

[9] However, the hospital also advised that the accounts clerk retired before it could impose any further discipline. Despite this, the hospital advised that it sent the accounts clerk a letter on February 11, 2021 that emphasized the importance of not disclosing any of the information that they had inappropriately accessed.

[10] To notify the affected patients of the breach, the hospital advised that it first attempted to do so by telephone and then by letter. The hospital confirmed that notification began on October 29, 2020 and that all but one patient was notified by November 16, 2020. The hospital explained that it was unable to contact this remaining patient by phone and that their notification letter was returned due to an invalid mailing address. As an alternative measure, the hospital advised that it made a note on the patient's file for its Registration Department to contact its Privacy Office should they return to the hospital.

[11] Further, regarding the delay in notifying the affected patients, the hospital explained that this was due to the time it took to complete and investigate the audits, as well as investigate the circumstances surrounding the breach, which resulted in the decision to delay notification for compassionate reasons. The hospital confirmed that it always notifies affected patients as soon as possible, but in this case, it did not do so before completing its investigation into the breach.

[12] To detect and deter unauthorized access to PHI, the hospital advised that it has ongoing procedures in place to safeguard PHI. The hospital explained that its Confidentiality Policy requires that all new staff sign a Statement of Confidentiality and attend a General Orientation session, which includes privacy training. In addition, the hospital explained that all of its staff must complete its annual, mandatory privacy refresher, which includes resigning a Statement of Confidentiality.

[13] The hospital also advised that its Privacy Office takes part in the annual Privacy Awareness Week (PAW)[3] by sending out a week-long PAW email blitz to its staff and reaching out to all of its units and departments to offer in-service privacy sessions for their teams. The hospital explained that its Privacy Office provides these sessions

[3] http://www.appaforum.org/paw/.

whenever there is new information that needs to be communicated to staff or as requested by their units and departments.

[14] Moreover, the hospital advised that, before any employee accesses a PHI record in its (Meditech) EHR system, a "Privacy Advisory" is displayed on-screen that reads:

> This system contains personal information about our patients and staff. Access to this information is permitted only for patient care purposes and/or for the performance of work duties. Access to information in this system is audited regularly. Inappropriate access may result in suspension or termination of access privileges and disciplinary action up to and including termination of employment or affiliation. Privacy and Confidentiality policies must be reviewed and understood before entering the system. Respond 'Y' to acknowledge acceptance/agreement to above terms. Respond 'N' to exit.

[15] In addition, the hospital explained that it performs both routine and ad hoc audits. Regarding its audit policy, the hospital advised that audits are completed monthly and that, typically, these audits examine accesses of patient PHI in its EHR based on name matching or more narrowly if there is a specific concern. According to the hospital, on occasion, the audits also examine other patterns of access to patient PHI, such as obstetrical staff looking at the records of male patients, staff looking at the records of patients named in the media or confirming that research auditors are only accessing the records of patients who are participating in clinical research.

[16] Regarding remediation, the hospital advised that it reviewed how it processed the breach and decided to end its discretionary practice of delaying notification for compassionate reasons with respect to family members of deceased patients. Further, the hospital advised that, going forward, notification will be made as soon as possible and that its Privacy Office will be working closely with the Human Resources department to ensure a consistent approach to privacy investigations.

Reported Breach #2:

[17] The hospital advised that its Patient Experience Department received a call on May 26, 2021 from a patient who had concerns that their EHR may have been accessed without authorization by their relative who was employed by the hospital as an Admitting Clerk (the clerk).

[18] In response to the call, the hospital advised that this department contacted the hospital's Privacy Office on June 3, 2021 and an ad hoc audit of the clerk's accesses to the EHR for the period of May 1, 2021 to June 4, 2021 was conducted. This audit revealed a suspicious access by the clerk of the patient's EHR.

[19] In response to the suspected breach, the hospital advised that it performed a second audit of the clerk's accesses to its EHR for the period of December 1, 2020 to

June 4, 2021. The hospital reported that this audit revealed that the clerk had accessed the EHRs of five patients in total between December 24, 2020 and May 20, 2021 without authorization.

[20] Further, the hospital reported that the clerk searched specifically for the EHRs of the affected patients and that the PHI accessed without authorization included some or all of the following for each patient: name, date of birth, age, sex, Ontario Health Insurance Plan (OHIP) number, address, telephone number, marital status, language, religion, email address, mother's name, next of kin's name, telephone and address, person to notify's name, telephone number and address, guarantor's name, telephone number and address, employer, employment status and information, reason for visit, visit history, attending, family and referring physician, disease site, insurance information, scheduler's notes, Infection Prevention and Control screening answers (the screening answers), patient flow details, and admission source and details.

[21] The hospital advised that the clerk has worked at the hospital since March 2000 and is not a member of a regulatory college. The hospital also advised that the clerk completed its annual privacy training on December 9, 2019, March 26, 2020, February 5, 2021 and April 13, 2021, which included the signing of a Statement of Confidentiality.

[22] As part of its investigation into the breach, on June 4, 2021, the hospital confirmed with the clerk's manager that there was no work-related reason for the clerk to have accessed the affected patients' EHRs. The hospital confirmed that the accesses were inappropriate after holding investigation meetings regarding the matter on June 14 and 30, 2021. Moreover, the clerk confessed to inappropriately accessing only one of the affected patients' EHRs and explained that they did so to confirm this patient's mailing address in order to send them a personal note.

[23] To contain the breach, in accordance with its policy and privacy breach protocol relating to unauthorized access of PHI, the hospital placed the clerk on administrative leave on June 4, 2021, disabled their access to its EHR and, ultimately, terminated their employment.

[24] To notify the affected patients of the breach, the hospital advised that it first attempted to do so by telephone and then by letter. The hospital confirmed that notification began on June 30, 2021 and concluded by July 19, 2021.

[25] Regarding remediation and, to deter and detect unauthorized access to PHI, the hospital advised that it had in place the same policy, procedures and measures described above under Reported Breach #1 in place.

Reported Breach #3:

[26] The hospital advised that its Privacy Office received a call on March 11, 2021 from a patient, who is also one of its employees, in which they raised concerns that their EHR may have been accessed without authorization by another employee since

January 1, 2019.

[27] In response to the call, the hospital immediately performed an ad hoc audit of the patient's EHR dating back to January 1, 2019. The audit revealed a suspicious access of the patient's EHR by a Radiology Assistant (the assistant) employed by the hospital.

[28] In response to the suspected breach, the hospital also performed a second audit of the assistant's accesses of its EHR for the period of September 1, 2020 to March 11, 2021. Collectively, both audits revealed that the assistant had potentially accessed the EHRs of 11 patients in total without authorization between February 27, 2019 and February 24, 2021.

[29] Further, the hospital reported that the assistant searched specifically for the EHRs of the affected patients and that the PHI that they accessed without authorization included some or all of the following for each patient: name, date of birth, age, sex, OHIP number, address, telephone number, marital status, language, religion, email address, mother's name, next of kin's name, telephone and address, person to notify's name, telephone number and address, guarantor's name, telephone number and address, employer, employment status and information, reason for visit, visit history, attending, family and referring physician, disease site, insurance information, scheduler's notes, the screening answers, patient flow details, admission source and details, and resulted diagnostic imaging reports.

[30] The hospital advised that the assistant has worked at the hospital since July 2002 and is not a member of a regulatory college. The hospital confirmed that the assistant last completed its annual privacy training on December 11, 2019, which included signing a Statement of Confidentiality.

[31] As part of its investigation into the breach, the hospital advised that, on May 17, 2021, it held a meeting with the assistant who returned from a long-term leave of absence on this date. The assistant claimed that they did not recall the inappropriate accesses and denied searching for and/or knowing the affected patients.

[32] To contain the breach, in accordance with its policy and privacy breach protocol relating to unauthorized access of PHI, on May 18, 2021, the hospital suspended the assistant without pay for 45 days and disabled their access to the EHR. When the assistant returned to work, they were reassigned to a new position in which they do not have access to patients' PHI. Moreover, the hospital advised that subsequent audits have confirmed that the assistant has not accessed PHI since starting their new position in September 2021.

[33] To notify the affected patients of the breach, the hospital advised that it first attempted to do so by telephone and then by letter. The hospital confirmed that notification began on July 20, 2021 and concluded by July 27, 2021.

[34] With respect to the delay in reporting this breach to the IPC, completing its investigation and notifying the affected patients, the hospital explained that the delay was due to the assistant being on a long-term leave of absence and, as a result, the hospital was unable to take these steps until they returned to work on May 17, 2021.

[35] Regarding remediation and to deter and detect unauthorized access to PHI, the hospital advised that it had in place the same policy, procedures and measures described above under Reported Breach #1 in place.

ISSUES:

[36] The hospital does not dispute that, under the *Act*, it is a "health information custodian" and that the accounts clerk, the clerk and the assistant were, at all material times, "agents" of the hospital.

[37] Further, there is no dispute that, without authorization, these agents accessed records of "personal health information" under the *Act* that was in the custody or control of the hospital.

[38] Therefore, as a preliminary matter, I find that:

- the hospital is a "health information custodian" under paragraph 4.i of section 3(1) of the *Act*;
- the records that were accessed without authorization and in the custody or control of the hospital contained "personal health information" within the meaning of section 4(1) of the *Act*;
- the accounts clerk, the clerk and the assistant were "agents" of the hospital as defined in section 2 of the *Act*; and
- the hospital, as a result of the unauthorized accesses by the agents, used PHI contrary to section 29 of the *Act*.

[39] As such, this decision addresses the following issues:

1. Did the hospital take reasonable steps to protect personal health information?
2. Is a review warranted under Part VI of the *Act*?

DISCUSSION:

Issue 1: Did the hospital take reasonable steps to protect the personal health information?

[40] In addition to having a privacy breach protocol in place, when a privacy breach occurs, this office has recommended that health information custodians immediately notify appropriate staff, identify the scope of the breach, take steps to contain, investigate and remediate the breach, as well as notify the affected individuals (and regulatory colleges, if applicable).[4]

[41] In this matter, for each breach, the hospital took a number of recommended steps. More specifically, the hospital:

- identified the scope of the breach and the nature and quantity of PHI that was affected;
- ensured that no copies of PHI were made or retained;
- suspended the agents' access rights to PHI; and
- notified the affected individuals.

[42] As such, the remainder of this discussion focusses on the practices the hospital has put in place to protect PHI as required under section 12(1) of the *Act*. This section states:

> 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.

[43] Further, under section 10(1) of the *Act*, custodians that have custody or control of PHI must "have in place information practices that comply with the requirements of this Act and its regulations." The term "information practices" is defined in section 2 of the *Act*, in part, as follows:

> "information practices", in relation to a health information custodian, means the policy of the custodian for actions in relation to personal health information, including,
>
> …

[4] See the IPC's "Responding to a Health Privacy Breach: Guidelines for the Health Sector".

> (b) the administrative, technical and physical safeguards and practices that the custodian maintains with respect to the information;

[44] This office has found that section 12(1) requires that health information custodians review their measures or safeguards from time to time to ensure that they continue to be reasonable in the circumstances to protect PHI in the custodians' custody or control.[5]

[45] Further, this office has stated that, in order to comply with the requirements in section 12(1) and to take steps that are reasonable in the circumstances to protect PHI, custodians must implement administrative and technical measures or safeguards, including privacy policies, procedures and practices, audit functionality, as well as privacy training and awareness programs and initiatives.[6]

[46] In this matter, to determine whether the hospital has taken reasonable steps to ensure that PHI in its custody or control is protected against unauthorized use, the IPC's "Detecting and Deterring Unauthorized Access to Personal Health Information" guidance document (the Preventing Unauthorized Access to PHI Guide)[7] is informative.

[47] The Preventing Unauthorized Access to PHI Guide recommends that custodians implement the following measures to prevent or reduce the risk of unauthorized access:

- privacy polices and procedures;
- privacy training and awareness;
- privacy notices and privacy warning flags;
- confidentiality agreements;
- access management;
- logging, auditing and monitoring;
- privacy breach management; and
- discipline.

[48] As part of my investigation, I reviewed the hospital's PHI privacy and protection policy (the Privacy Policy), Confidentiality Policy, Statement of Confidentiality, training materials and other informational materials.

---

[5] Orders HO-010 and HO-013, PHIPA Decisions 64 and 70
[6] Order HO-013.
[7] https://www.ipc.on.ca/wp-content/uploads/Resources/Detect_Deter.pdf.

Policies and Procedures

[49] Regarding the hospital's policies and procedures, the Privacy Policy states:

> [The hospital] is committed to protecting the privacy, confidentiality and security of all personal health information that is collected, used and disclosed by the organization. [The hospital's] staff and affiliates have a legal, ethical, professional and employment/contractual obligation to protect the confidentiality of personal health information.
>
> This policy is based on applicable law and the ten privacy principles which are derived from the Canadian Standards Association's Model Code for the Protection of Personal Information…

[50] The Privacy Policy covers various topics regarding the management of PHI, including access to or use of PHI, as well as the security of PHI. This policy requires that "access to health information is based on a 'need-to-know' basis to provide current and direct patient care or to perform one's duties. Access to [PHI] is limited to that information which is required to fulfil the purpose it was accessed for." It also sets out certain conditions under which PHI might be used and requires that PHI only "be accessed and/or released as permitted/required by law."

[51] Moreover, the Privacy Policy states:

> Access is deemed inappropriate when an individual accesses personal health information when they are not providing care for the patient and none of the circumstances in […] this policy apply.
>
> Inappropriate access includes, but is not limited to, accessing patient information for personal interests, including interpersonal conflicts, curiosity, personal gain, concern about the health and well-being of an individual.
>
> Inappropriate access also includes accessing one's own personal health information or that of a family member or colleague, when the information is not needed to perform one's job.

[52] To keep PHI secure, the Privacy Policy requires that "security applies to the spectrum of physical, technical, and administrative safeguards put into place to protect the confidentiality, integrity, and availability of electronic [PHI]." This policy also sets out the physical safeguards, technical security and administrative procedures that the hospital has in place, as well as the investigation, containment, notification steps that the hospital takes in response to a privacy breach.

[53] The Privacy Policy also requires that PHI "be stored in a secure area and not left unattended in areas accessible to unauthorized individuals". This policy also makes it

"the responsibility of those in possession of Portable Digital device(s) to ensure that all [PHI] is password protected and/or encrypted as a safeguard against unauthorized access…". To that end, the policy refers readers to the hospital's "Security of Portable Digital Devices & Transporting of Confidential Information" policy for further details.

[54] With respect to an unauthorized use of PHI, the Privacy Policy provides that breaches of confidentiality will not be tolerated, subject to disciplinary action and that inappropriate access may constitute an offence under the *Act*. It also requires that individuals who have observed or been made aware of a potential privacy breach immediately report the concern to the hospital's Privacy Office or their Manager/Director.

[55] Moreover, with respect to discipline, the Privacy Policy makes individuals who access PHI without authorization accountable for their actions and provides that "depending on the severity of the actions and impact on the organization, patients, or other systems users, disciplinary action may include a verbal warning, a written warning, mandatory privacy awareness training, suspension, termination of employment or affiliation, loss of hospital privileges, or loss of technology privileges."

[56] Regarding confidentiality, the Confidentiality Policy requires that the hospital's employees hold all PHI in strict confidence. This policy also sets out what constitutes a breach of confidentiality (e.g. unauthorized accessing of PHI) and states:

> Confidentiality is a requirement of employment and must be maintained at all times, both on and off duty. The terms of this confidentiality policy and the responsibility of each affiliate will continue after the working relationship with [the hospital] is terminated. All affiliates of [the hospital] must sign the [Statement of Confidentiality] form at the commencement of their relationship with [the hospital] and reconfirm on an annual basis thereafter.

[57] Further, by signing a Statement of Confidentiality, the hospital's employees acknowledge their understanding and agreement to comply with the hospital's confidentiality and privacy policies and procedures.

[58] The hospital advised that its policies and procedures are to be reviewed every three years. Specifically, the hospital advised that the Privacy Policy was reviewed and updated on January 31, 2022 after the three privacy breaches occurred and that the Confidentiality Policy will be reviewed by the end of April, 2023.

Audits

[59] With respect to audits, the Privacy Policy provides that "privacy audits will be performed to determine whether there has been a violation of privacy through inappropriate access to electronic patient information."

[60] According to this policy, regular audits are conducted on a monthly basis and ad hoc audits "can be requested by any individual who believes patient information has been inappropriately accessed." This policy also provides that "audit requests and results are treated confidentially by all staff involved in breach investigations and will only be shared on a need to know basis."

[61] Moreover, as indicated above, before an employee accesses a record in the hospital's EHR system, a Privacy Advisory is displayed on-screen. Further, the Confidentiality Policy requires that computer users do the following:

> All computer users must protect any user code(s) or password(s) used to access computer information systems and programs. Employee user codes and/or passwords are the equivalent of their signature and all activities undertaken using such codes and passwords are the responsibility of the employee. User codes and passwords are not to be shared under any circumstances. If at any time the employee feels that the confidentiality of their code or password has been or might be breached, the employee must report the concern to the Information Technology Department to have the password/code changed immediately. No employee shall abuse their privilege of access to gain access to any confidential information for personal reasons.

Staff Training and Awareness

[62] The hospital advised that all new staff attend a general orientation that includes privacy training and that it is mandatory that all staff complete its annual privacy refresher. Further, the hospital advised that all of its policies and procedures are made available to its staff via its Intranet.

[63] Further, the hospital advised that, during this orientation, all staff are made aware of where its policies are kept and how to obtain them. Moreover, the hospital explained that its team that maintains the policies regularly send email messages to all agents noting which policies have been updated.

[64] As mentioned above, the hospital's Privacy Office participates in PAW by providing a week-long PAW email blitz and offering in-service privacy sessions. The hospital advised that it has done so since 2013. My review of the emails sent by the hospital regarding PAW, found that they advise staff that the hospital "continues to support the *global effort* to promote and raise awareness for privacy issues and the importance of protecting personal information through PAW."

[65] These emails contain contact information for the hospital's privacy team and educate staff about inappropriate access (e.g. snooping) and the consequences for accessing PHI without authorization, as well as providing "quick check scenarios" that test the knowledge of its staff about the appropriate actions to be taken to protect PHI.

Further, these emails remind staff of the opportunities to review the hospital's policies and practices in order to understand their privacy obligations.

Analysis

[66] The hospital advised that it complies with section 12(1) by having in place administrative, technical, and physical safeguards to prevent unauthorized use of PHI including the abovementioned measures.

[67] As all of the three breaches involved snooping, with respect to section 12(1), the hospital must demonstrate that it has taken reasonable steps in the circumstances to ensure that PHI is protected against unauthorized use. The hospital must also demonstrate that it has taken steps to help prevent a similar breach from occurring in the future.

[68] Based on my above review of the Privacy Policy, the Confidentiality Policy and the hospital's privacy training and informational materials, I am satisfied that the hospital has the administrative, technical and physical safeguards in place to comply with the requirements in section 12(1).

[69] Further, to prevent similar breaches from occurring, as indicated above, the hospital advised that, after the three breaches, it reviewed the adequacy of its Privacy Policy for protecting PHI. As evidence of its compliance with section 12 and the adequacy of its Privacy Policy, the hospital advised that its snooping cases have consistently gone down over the last few years.[8]

[70] Moreover, the hospital has confirmed to this office that it is committed to taking the following steps in light of the three snooping breaches that occurred in 2020 to 2021:

- review and amend its privacy policies, as well as training, educational and informational materials, in order to target and prevent breaches relating to unauthorized access (i.e. snooping) by its staff members and agents;

- send out quarterly communications (e.g. emails) to its staff and agents relating to unauthorized access (i.e. snooping) and the steps that they must take to prevent this type of breach; and

- provide more snooping examples (such as the breaches that occurred at hospital) in communications to its staff and agents, as well as in training, educational and informational materials, as a deterrent to snooping breaches.

[71] For these reasons, I am satisfied that the hospital has adequately addressed the

[8] The hospital advised that it had 7, 5 and 4 snooping cases in 2019, 2020 and 2021, respectively. It should be noted that this office did not examine every snooping incident discovered by the hospital.

privacy concerns raised by the three breaches.

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

[72] 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 this Act or its regulations and that the subject-matter of the review relates to the contravention.

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

DECISION:

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

Original Signed by: April 4, 2023

John Gayle
PHIPA Mediator/Investigator