Information and Privacy Commissioner,
Ontario, Canada

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

PHIPA DECISION 163

Complaint HR18-73

A public hospital

October 19, 2021

Summary:

A public hospital (the hospital) contacted the Office of the Information and Privacy Commissioner of Ontario (IPC) to report a privacy breach under the *Personal Health Information Protection Act, 2004* (*PHIPA* or the *Act*). Specifically, a hospital employee inappropriately accessed highly sensitive personal health information (phi) of a family member. In light of the steps taken by the hospital to address the breach, no formal review of this matter will be conducted under Part VI of *PHIPA*.

Statutes Considered: *Personal Health Information Protection Act, 2004, S.O. 2004, c. 3;*

BACKGROUND:

[1] In June 2017, a public hospital (the hospital) received privacy complaints from four family members with a connection to an employee in the Clinical Records Department. The complainants were concerned that the employee had been snooping into their personal health information and had disclosed phi to their (the employee) spouse and to the spouse's sister. These individuals subsequently contacted the IPC and four complaint files were opened.

[2] Subsequent to receiving the above complaints, a fifth family member contacted the hospital in November 2017 to inquire if the same employee had ever accessed their personal health information. This family member was also concerned that their privacy

may have been breached.

[3] In response to the complaints, the hospital conducted an investigation into the five allegations and determined that the employee had inappropriately accessed the personal health information of one of the four original complainants. For the fifth[1], the hospital determined that the employee had accessed this individual's personal health information on two occasions but that neither access was inappropriate. This information was communicated to the complainants.

[4] The four original complainants were not satisfied with the hospital's response and filed a complaint with this office. Those files were assigned to a mediator at the IPC who worked with the parties to attempt settlement of the issues. Subsequent to additional details being provided by the hospital to the complainants during mediation, they withdrew their complaints and their complaint files were closed. However, during the course of the hospital's investigation, the hospital conducted an audit of its electronic medical record (EMR) and it revealed an access to electronic personal health information of another patient by the employee that required further review. As a result of that review, the hospital determined that in 2009, the employee inappropriately accessed the medical records of a sixth family member. The medical records inappropriately accessed included what would be considered to be one of the most sensitive type of personal health information.

[5] On February 21, 2018, the hospital reported this breach to the IPC and this investigation file was opened and assigned to me as the Investigator.

SCOPE OF THE BREACH:

[6] As noted above, the inappropriate access occurred in 2009 but was not discovered by the hospital until 2017. The hospital then reported it to this office in February of 2018. Specifically, the hospital advised that the employee viewed two physician reports, namely a "History and Physical Report" and an "Operative Report" containing extremely sensitive personal health information. The hospital's audit reports showed the access lasted 55 seconds. The hospital indicated that the reports were viewed by the employee nearing the end of her evening shift, when she was working alone.

[7] The hospital reported that it could not identify or verify the reason for the employee's access to those records. When questioned about the access, the employee indicated that she did not know this individual at the time of the access; could not recall the reason for the access and denied that this access was inappropriate. The hospital was not satisfied with the answers that the employee provided about this access.

---

[1] The 5th family member did not submit a complaint to the IPC and was satisfied with the hospital's determination that the access to their phi was appropriate. As such, this access is not at issue in this complaint.

[8] As part of the hospital's investigation, the Coordinator, Freedom of Information & Privacy Unit spoke with the affected patient about the inappropriate access into her personal health information. The patient confirmed that that she knew the employee since before this date and did not express any concern about the access to her personal health information.

[9] According to the hospital, the employee has been employed with the hospital since August 2007, as a "Clerk Typist - Records Processing" (clinical records clerk) in the hospital's Clinical Records Department (the department).

[10] The hospital explained that its patient health records are a hybrid of paper charts and the electronic health information system called Meditech Magic Health Information System (Meditech) and the employee's role required that she routinely use the Meditech 'Patient Care Inquiry' (PCI) and the 'Medical Record Index' (MRI) databases.

[11] The PCI database is a "viewable electronic patient health record" that contains a compilation of electronic health information and scanned copies of paper documentation. PCI contains a radiology reports section called RAD.

[12] The MRI database provides a quick reference to information that is required by the records staff in their work routinely and frequently. The hospital stated that the MRI contains a variety of options including:

- location tracking of the hardcopy clinical records;
- printing of patient list;
- record completion tracking;
- a logging database for the Release of Information office; and
- "View Patient", which is a summary of patient demographics plus a listing of the patient's visits.

[13] The department processes, collects and secures personal health information documented for every episode of care including inpatient stays and outpatient visits. The hospital provided a list of the principal functions of the department, many of which would involve duties that require routine access to paper and electronic patient records. The hospital indicated that clinical records clerks access the paper charts and electronic health information for a multitude of functions and purposes, both in order to perform their job functions and to assist the other clinical records staff to perform their job functions.

[14] According to the hospital, the auditing capability of its electronic health records system at the time of this breach was limited. As a result, the hospital did encounter some difficulties determining whether the accesses by the employee were authorized or

not, due to the fact that the employee had broad and frequent access to records of personal health information.

[15] Because of this, and as part of its strategy to contain the breach, as soon as the hospital became aware of it, the employee was suspended from her position at the hospital and her access to the hospital's electronic health records system was revoked.

[16] Given the extreme sensitivity of the personal health information involved and the pattern of inappropriate accesses displayed in this privacy breach, I worked with the hospital throughout my investigation to implement new policies and to improve their information practices to prevent future breaches of a similar nature.

PRELIMINARY ISSUES:

[17] There is no dispute that the hospital is the "health information custodian" and that the employee is an "agent" of the hospital under the *Act*. There is also no dispute that the employee accessed a record of "personal health information" and that the employee's access to this personal health information amounted to a "use" under the *Act* that was unauthorized.

[18] Based on the information set out above, as a preliminary matter, I find that:

- the hospital is a "health information custodian" under paragraph 4 of section 3(1) of the *Act*,
- the employee is an "agent" of the hospital, within the meaning of section 2 of the *Act*,
- the record at issue contained "personal health information" under section 4(1)(a) and (b) of the *Act,*
- the employee's access was a "use" within the meaning of section 2 and 6 of the *Act*, and
- the employee's use of the phi was unauthorized.

ISSUES:

[19] In this decision, the following issues will be discussed:

1. Did the hospital take steps that were reasonable in the circumstances to protect personal health information in accordance with section 12(1) of the *Act*?
2. Did the hospital comply with section 10 of the *Act*?

3. Did the hospital respond appropriately to the breach?

4. Is a review warranted under Part VI of the *Act*?

RESULTS OF THE INVESTIGATION:

Issue 1: Did the hospital take steps that were reasonable in the circumstances to protect personal health information in accordance with section 12(1) of the *Act*?

[20] Section 12(1) of the *Act* requires that custodians take "reasonable" steps to protect personal health information in its custody and control.

[21] 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.

[22] In *PHIPA* Orders HO-010 and HO-013, and more recently in *PHIPA* Decisions 64 and 70, the IPC held that section 12(1) of the *Act* required health information custodians to review their measures or safeguards from time to time to ensure that they continue to be reasonable in the circumstances to protect personal health information in the custodians' custody or control. Health information custodians are expected to identify risks to privacy and take reasonable measures to reduce or eliminate such risks and mitigate the potential harms that may arise.

[23] Administrative and technical measures and safeguards are critical to protecting personal health information. The IPC has previously stated that, in order to comply with the requirements in section 12(1) of the *Act* and to take steps that are reasonable in the circumstances to protect personal health information, 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.

[24] In *PHIPA* Order HO-013, Commissioner Beamish commented on the importance of auditing, and obtaining analyzable data, for detecting and deterring unauthorized access to personal health information:

> As in other industries, audits play an important role in the health sector. Auditing of electronic information systems is particularly important in ensuring that the privacy of individuals and the confidentiality of personal

> health information are protected. Audits are essential technical safeguards for electronic information systems. They can be used to deter and detect collections, uses and disclosures of personal health information and the copying, modification or disposal of records of personal health information that contravene the *Act*. As such, they help to maintain the integrity and confidentiality of personal health information stored in electronic information systems. The ability to conduct audits of personal health information and the activities of agents or users (referred to in this section as users) in an electronic information system also ensures that a health information custodian is able to respond to requests from patients for information about who has collected, used or disclosed their personal health information.

Administrative and Technical Measures and Safeguards:

Audit functionality:

[25] During the course of the hospital's investigation, it performed targeted audits as well as random audits of the employee's accesses to the PCI and the MRI and identified that there were accesses that could not be determined as appropriate solely on the basis of the audit report. The hospital indicated that this was expected given the nature of the employee's duties and assigned tasks and as such, the hospital also conducted a random audit of another clerical staff in the department for comparison purposes.

[26] With respect to the hospital's audit process, the hospital advised that it looked at a number of different considerations, including but not limited to the timing of each access over time, in relation to scheduled patient activity, the employee's work schedule, time of day, duration of each access, type of information, the extent of information accessed, and whether there were any identifiable patterns.

[27] During the audit analysis, the hospital also compared the type of patient appointment/visit with the type of record(s) accessed and/or if it related to a specific type of test or procedure that the employee is responsible for as part of her role.

[28] I note that the information in the audit report includes the following:

- time and date of access;
- category of record accessed i.e. whether the access was in PCI or MRI;
- type of record and date e.g. "ER physician report dated 17/12/07"; and
- duration of access.

Discussion:

[29] The hospital explained that clinical records clerks continually process information, which requires frequent access to the EMR in order to perform their required job duties, including potential access to any patient record. For this reason, at the time of the breach the clerks were not required to record a reason for accessing a patient record and by doing so, would prohibit the clerks from doing their jobs efficiently. As such, the hospital advised that it could not validate accesses based on the review of audit results and patient history alone.

[30] The hospital's audit analysis determined that the employee's inappropriate access was in PCI. The hospital explained the variety of ways that an employee can look for a record in PCI includes name, medical record number, account umber, health card number, and visit date and that its audit report at the time did not indicate which of these methods were used by the employee to access the individual's record.

[31] At the time of the employee's access, the hospital explained that it was using Meditech, which had been in use since 2000 and that there were auditing and logging limitations with this system. The hospital submitted that the surveillance auditing report functionality of Meditech did not provide sufficient information to validate audit results for staff like clinical records clerks who engage in very broad and varied access to health records as part of their job.

[32] The hospital acknowledged this gap in their EMR's auditing capabilities and in October 2019, it implemented a new Health Information System (HIS) called Meditech Expanse Health Information System (Meditech Expanse). The hospital advised that a component of this new HIS is a new Electronic Medical Record (EMR) module. The hospital explained that while Meditech Expanse has some built-in auditing capabilities, the hospital also purchased a new auditing software from a third party company called Iatrics.

[33] According to the hospital, this auditing software extracts personal health information data from Meditech Expanse, and is able to provide a variety of audit reports.

[34] The hospital also implemented two other changes to assist with validating audit results as follows:

<u>1. Retaining Clinical Record Clerks' Work Lists:</u>

[35] As stated above, the department is responsible for completing various and varied tasks, including ensuring chart assembly and chart completion. The hospital explained that the clinical records clerks had a practice of printing "work lists" through Meditech to identify the paper records that had to be retrieved for chart assembly and completion. At the end of this task, the works lists were being shredded.

[36] However, with the implementation of the new Meditech Expanse, the department is now retaining work lists so that they can be used for auditing verification purposes and the majority of information is now being recorded in the electronic patient record. Any paper documentation and forms that cannot be completed electronically are now scanned into the EMR by the clerks at the conclusion of the patient visit. The hospital confirmed that this practice has limited the handling of paper records.

2. Creation of a Daily Chart Access Log:

[37] A Daily Chart Access Log process has also been implemented which the hospital explained is a handwritten log that is meant to fill as much of a gap as possible to record any access to a patient's electronic personal health information that is not captured elsewhere.

Analysis:

[38] In my view, at the time of the breach, the hospital's previous EMR did have its limitations, which included an inability to validate audit results for staff like clinical records clerks who engage in very broad and frequent access to health records as part of their job. However, despite this, I note it was through this EMR that the hospital was able to detect this breach and report it to the IPC. Additionally, in response to the breach, the hospital made changes to enhance their EMR's capabilities in order to produce quality audit reports, which included:

1. implementing a new EMR and purchasing an auditing software from a third party vendor to obtain detailed audit reports and to validate user accesses;

2. retaining the clinical records clerks' work lists in order to cross reference and validate audit results; and

3. implementing a daily chart access log to account for any personal health information that is not captured elsewhere.

[39] Based on the measures the hospital had in place at the time of the breach and the above additional measures, I am satisfied that the hospital has taken steps that are reasonable to protect personal health information in accordance with section 12(1) of the *Act*.

Issue 2: Did the hospital comply with section 10 of the *Act*?

[40] Section 10 of the *Act* states:

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.

3. A health information custodian that uses electronic means to collect, use, modify, disclose, retain or dispose of personal health information shall comply with the prescribed requirements, if any.

4. A person who provides goods or services for the purpose of enabling a health information custodian to use electronic means to collect, use, modify, disclose, retain or dispose of personal health information shall comply with the prescribed requirements, if any.

[41] Section 2 of the *Act* defines "information practices" as:

> "information practices", in relation to a health information custodian, means the policy of the custodian for actions in relation to personal health information, including,
>
> (a) when, how and the purposes for which the custodian routinely collects, uses, modifies, discloses, retains or disposes of personal health information, and
>
> (b) the administrative, technical and physical safeguards and practices that the custodian maintains with respect to the information

Policies:

[42] During the investigation of this matter, the hospital provided the following policies and procedures to this office:

- Corporate Privacy Policy for Personal Health Information (ADM 3-05) dated February 2011
- Progressive Discipline Policy (HR 4-003) dated November 4, 2015
- Privacy Breach Reporting and Management Policy (ADM-PRIV-005) dated December 6, 2017
- Access to PHI of Family/Former Family Members/Co-Workers by Clinical Records Department Staff (CR-040) dated November 29, 2017

[43] As part of my investigation, I reviewed the policies, practices and procedures provided by the hospital. The information provided included what was in force at the time of this breach, as well as current material. From my review, the policy most relevant to this matter is the one titled "Access to PHI of Family/Former Family Members/Co-workers by Clinical Records Department Staff" (the Policy).

[44] The hospital explained that the Policy was specifically developed and

implemented to address the unique position of clinical records clerks who do not provide patient care but have broad-based access to electronic personal health information for the performance of their job duties.

[45] I note that the Policy clearly defines its purpose as follows:

> The Clinical Records Department staff of the [the hospital] will not work on the electronic personal health information (PHI) or the hard-copy PHI (also known as health records) of family members or former family members, unless it is not possible to transfer the work to a co-corker. When access to a family member/former family member's PHI is unavoidable, the staff member will disclose the access to the Manager, Clinical Records/delegate.
>
> Staff will also disclose accesses to PHI of co-workers to the Manager, Clinical Records/delegate.

[46] Based on my review of the Policy, I am generally satisfied that it adequately provides definitions for family member and former family member as well as clearly outlines for staff the procedure for transferring work concerning anyone in these two categories.

[47] However, I note that none of the hospital's policies and procedures addressed any specific guidance with respect to snooping. As such, upon my recommendation, the hospital created a new snooping policy entitled "Snooping Policy – Unauthorized User Access to Personal Health Information (ADM-PRIV-006)" in February 2021. I have reviewed this new policy and I am satisfied that it adequately sets out the purpose of the policy, addresses the consequences of a snooping privacy breach, and explains the obligations of staff. It also includes other relevant information that is helpful for staff to understand exactly what is expected of them. On February 11, 2021, the hospital also published a snooping article on its internal electronic newsletter to raise awareness regarding snooping and included a hyperlink to the new snooping policy.

Privacy Training and Education:

[48] In *PHIPA* Order HO-013, this office discussed the importance of training and stated the following in part:

> A comprehensive privacy training program is an essential tool to combat the risk of uses and disclosures of personal health information by agents in contravention of the *Act*, including agents who are "curious" or who are motivated by their own interests, such as financial gain.
>
> ...

> Comprehensive and frequent privacy training is essential to the development and maintenance of a culture of privacy within any organization.

[49] The hospital advised that it includes privacy training as part of their new staff orientation for all new employees, which includes an electronic learning module, *PHIPA* refresher course. Since 2016, the hospital requires this course be taken annually.

[50] The hospital reported that the employee received privacy training on five occasions. She received privacy training as part of new staff orientation in 2007 and subsequently successfully completed the online electronic *PHIPA* course on four additional occasions.

[51] In addition, the hospital advised that its clinical records clerks received specific privacy training and education about snooping. This training and education included:

i. In 2015, the IPC launched an educational campaign called, "Snooping Is It Worth It?". Also as part of this campaign, L-shaped infographic monitor wraps were obtained and placed on all computers in the department.

ii. In July 2017, the Manager of Clinical Records spoke to the staff and reiterated that they should only access information that is required to perform their role and addressed the responsibility to maintain the trust placed in staff to respect patient privacy by only accessing health records in connection with their job (i.e. no snooping).

iii. Throughout 2018 and 2019, the Manager of Clinical Records leveraged the weekly department huddles to discuss the upcoming go-live of the new Meditech Expanse. The Manager also invited the Coordinator, FOI and Privacy to attend one of these huddles to discuss privacy. Items that were discussed included reiterating that staff were to access records only for the purpose of their job.

iv. In 2020, the department implemented a Daily Chart Access Log. As part of the implementation, the Manager of Clinical Records provided the background on why it was being implemented and reiterated that the clerks were only to access electronic personal health information as required to perform their role/duties.

v. In February 2021, the Manager of Clinical Records highlighted the Snooping Policy with her staff, instructed each of them to read the policy in detail, and sign off that they had read and understood it.

Confidentiality Agreements:

[52] The hospital advised that staff sign a confidentiality agreement upon hire, and subsequently as part of the Recognition and Development Review (RDR) process, which is reviewed every 2 years for non-management staff and annually for management

staff.

[53] The employee signed the hospital's confidentiality agreement on five (5) occasions, most recently in September 2020.

Code of Conduct Agreements/Respectful Workplace Agreement:

[54] In 2013, the hospital introduced a Code of Conduct Agreement, in which staff agree to adhere to value-based behaviours including "accountability for maintaining privacy and confidentiality". The Code of Conduct Agreement is re-reviewed and re-signed during the RDR process.

[55] Since 2015, the Code of Conduct Agreement has been replaced with a Respectful Workplace Agreement, which is required to be conducted every 2 years. The employee most recently signed the Respectful Workplace Agreement in September 2020.

Audits:

[56] The hospital explained their auditing practices as follows:

[57] Routine Audits:

i. audits of accesses to Meditech PCI within a randomly selected 24-hour time period are conducted at minimum every two weeks;

ii. audits of access to patients who share the same last name as the user who accessed their personal health information are conducted at minimum weekly and encompass all accesses since the date of the previous same last name audit; and

iii. audits of accesses to patients with a "Confidential Patient" flag are conducted at minimum monthly.

[58] Reactive, targeted audits are performed:

i. at the request of managers;

ii. at the request of patients/substitute decision makers;

iii. in response to a suspected or actual privacy breach for which additional information is required; and

iv. upon becoming aware of situations that could lead to inappropriate access (e.g. the admission of a high profile community member; a high profile media report that mentions an individual being hospitalized)

Privacy Warning:

[59] The hospital implemented a privacy-warning screen on its EMR in 2011 which is displayed for all users who access the hospital's electronic patient information system. It states the following:

> Please be aware that access to clinical information is tracked and audited routinely. You are only allowed to view information of those patients to whom you provide care (when part of the circle of care) or when needed to perform your assigned duties.
>
> Failure to comply with the above may result in disciplinary action up to termination. In addition, individual fines up to $100,000 may be imposed. For more information, please refer to our Corporate Privacy Policy.

Analysis:

[60] Based on my review of the hospital's information practices in relation to this matter, I am satisfied that reasonable steps have been taken to remedy the gaps that were found. At the time of the breach, the policies and procedures did not clearly include any information with respect to snooping. However, I find that the hospital has since remedied this issue with the implementation of a new snooping policy. Overall, I find that the hospital's policies are adequate and that the hospital followed their privacy breach protocol with respect to this privacy breach. It is also my opinion that the hospital has adequate and effective training programs in place for its staff, which explain the hospital's privacy and security policies, practices and procedures.

[61] In light of the above, I am satisfied that the hospital is in compliance with section 10 of the *Act*.

Issue 3: Did the hospital respond appropriately to this breach of unauthorized access?

[62] In assessing the adequacy of the hospital's response to this breach, the following steps are most relevant in the circumstances of this case:

1. Investigation and containment
2. Notification of appropriate parties
3. Remediation

1. The hospital's efforts to contain the breach

[63] The hospital submitted that the inappropriate access relevant to this breach was found in the course of an investigation into other complaints that had been submitted

to the IPC. According to the hospital, the inappropriate access occurred on March 16, 2009. The hospital reported that it could not identify or verify the reason for employee's access to that record.

[64] As part of the hospital's investigation, the employee was interviewed on three (3) occasions and questioned about the access to the personal health information of the individual. On all three occasions, the employee denied inappropriately accessing or disclosing personal health information. While she stated that she could not recall the specific purposes for each of the accesses, she maintained that all accesses would have been related to the performance of her job duties. She specifically denied accessing the personal health information for her own purposes. The hospital was not satisfied with the answers that the employee provided about this access.

[65] Upon confirmation of this breach, and as part of its strategy to contain the breach, the employee's access to the hospital's electronic health records system was revoked. The employee was also suspended without pay for six weeks from January to March 2018, and was subsequently reassigned to a role and department that does not work with or handle personal health information.

[66] After having been removed from Clinical Records Department for one year, the employee was returned to her role as a clinical records clerk in January 2019, with the provision that she would be subjected to targeted auditing.

[67] Prior to the scheduled return date, the department manager met with the employee to ensure the employee:

i. reviewed the privacy expectations to ensure that she had a full understanding of the requirements and protocols relating to patient records;

ii. was instructed to review the privacy policies, and subsequently signed acknowledgements that she had done so;

iii. was notified that she would be subjected to targeted audits; and

iv. re-signed and completed a privacy e-learn course.

[68] The employee's access to PCI was audited regularly (weekly, then biweekly then monthly) for almost a year after her return. The hospital submitted that it has not noted any inappropriate accesses by this employee.

[69] The hospital has also continued to conduct random audits, and have not noted any inappropriate accesses. The hospital submitted that random auditing of her accesses would continue.

[70] Since her return to the department, the hospital advised that there has been no inappropriate access and the employee has demonstrated understanding and

compliance with the hospital's privacy policies.

2. Notification of appropriate parties:

[71] The hospital stated that the affected patient was notified by telephone and by letter.

[72] The notification letter to the individual included all of the following information:

i. the details and extent of the breach;

ii. the specifics of the personal health information at issue;

iii. the steps that have been taken/will be taken to address the breach;

iv. that the IPC was notified of the breach and information on how to file a complaint with the IPC;

v. the contact information of the person within the organization the individual should contact if he/she has questions.

3. Remediation

[73] At the time of the breach, the hospital had a policy entitled "Access to PHI of Family/Former Family Members/Co-workers by Clinical Records Staff". The hospital explained that this policy reflected the requirement that department staff are not to work on the records of family members/extended family members/former family members unless it is not possible to transfer the work to a co-worker. If work on such a record is required, the employee must notify the department manager of the details of the access and the manager would maintain a log of such accesses.

[74] As indicated above, upon my recommendation, the hospital created a new snooping policy entitled "Snooping Policy – Unauthorized User Access to Personal Health Information" in February 2021. On February 11, 2021, the hospital also published a snooping article on its internal electronic newsletter to raise awareness regarding snooping and included a hyperlink to the new snooping policy.

[75] The hospital implemented a new EMR and purchased an auditing software from a third party vendor in order to improve its electronic auditing capabilities.

[76] Along with the two changes that have been put in place in Clinical Records with respect to 1) retaining Clinical Records clerks' "work lists", and 2) the creation of a manual Daily Chart Access Log for unusual accesses, the hospital advised that it will be able to better assess accesses by the clinical records clerks. Additionally, the hospital concluded that the new auditing software will offer audit report options in terms of flagging potentially suspicious accesses for further follow up, for example reports that

flag users and patients with the same address; who reside on the same street; and, who have the same next of kin listed.

[77] The hospital also advised that its privacy policies and privacy training materials have been flagged for review and revision, as part of its regular updating and review process, and will incorporate any amendments to *PHIPA*. The hospital also submitted that privacy training related to orientation and the annual privacy learning will be reviewed and revised to be in-line with revisions to the hospital's privacy policies.

[78] In conclusion, I find that although the breach occurred many years ago, it was extremely serious and, in light of the broader context of more recent allegations lodged against the same hospital employee, the hospital took appropriate action. In my view, the hospital has responded adequately to this breach.

Issue 5: Is a review warranted under Part VI of the *Act*?

[79] 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.

[80] In this case, the hospital's previous Meditech system had been in place since 2000 and the hospital acknowledged that it was outdated. The hospital submitted that at the time of the breach, the system did have the ability to perform audits, albeit with limited functionality. However, as previously mentioned, it was through this auditing system that the hospital was able to detect this breach.

[81] Although the hospital's previous Meditech system limited auditing capabilities did not hinder its ability to detect this particular breach, I note that there may be other circumstances where it may have.

[82] In response, the hospital implemented a new Meditech Expanse health information system on October 28, 2019, which will be more useful in the investigation of future suspected breaches. In addition, the hospital also purchased a third party privacy auditing software and continues to work with Iatrics in order to enhance and improve the hospital's auditing capabilities.

[83] In accordance with my delegated authority to determine whether a formal review should be conducted under section 58(1) of the *Act* and for the reasons set out above, I find that a formal review under Part VI of the *Act* 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: October 19, 2021

Soha Khan
PHIPA Investigator