Information and Privacy Commissioner,
Ontario, Canada

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

PHIPA DECISION 86

Complaint HC16-80

A public hospital

February 8, 2019

Summary: This office received a complaint from the mother of a deceased individual that a privacy breach occurred because the hospital was unable to locate records relating to her son's hospitalization. Given the steps taken by the hospital to respond to the complaint, the adjudicator determines that no review is warranted in accordance with sections 57(3) and 57(4)(a) of *PHIPA*.

Statutes Considered: *Personal Health Information Protection Act, 2004*, sections 2 (definition of "use"), 3(1), 4(1), 10(1), 10(2), 12(1), 37(1)(a), 57(3) and 57(4)(a).

Orders and Investigation Reports Considered: Orders HO-004 and HO-013; PHIPA Decisions 29, 50 and 74.

BACKGROUND:

[1] An individual made a request to a public hospital (the hospital) under the *Personal Health Information Protection Act* (*PHIPA* or the *Act*) for records relating to her deceased son.

[2] The hospital issued a decision, informing the requester that it could not fulfill a portion of her access request because it was unable to locate certain paper records in her son's medical file. The complainant filed a complaint with this office and a mediator was appointed to explore resolution. During mediation, the mediator had discussions with the parties about the hospital's search efforts and response to the loss of records.

[3] At the end of mediation, the complainant advised that she was not satisfied with

the hospital's explanation and response relating to her son's lost records. The complainant asserted that she wanted the hospital to be held accountable for losing her son's medical records and requested that its response to this privacy breach be an issue at the adjudication stage.

[4] After reading the complaint file, I sent a letter to the complainant's lawyer advising that it was my preliminary view that the complaint did not warrant a review under sections 57(3) and (4) of *PHIPA*. I invited the complainant to provide submissions to explain why her complaint should proceed to a review under *PHIPA*, if she disagreed with my preliminary view. The complainant was advised that I would consider any submissions provided in response to the letter before I made a final decision. The complainant did not respond to the letter or provide any written submissions. Accordingly, I did not seek submissions from the hospital before making this final decision.

[5] In this decision, I find that there are no reasonable grounds for a review under sections 57(3) and (4) on the basis that the hospital has responded adequately to the complaint under section 57(4)(a).

DISCUSSION:

Introduction

[6] Broadly speaking, *PHIPA* regulates the group of persons described as "health information custodians" and their agents, with respect to personal health information. One of the purposes of *PHIPA* is to establish rules for the collection, use and disclosure of personal health information by these persons, which protect the confidentiality of that information and the privacy of individuals while facilitating the effective provision of health care. One of the ways in which *PHIPA* achieves this purpose is by requiring that collections, uses and disclosures of personal health information occur with the consent of the individual to whom the information relates.[1]

[7] Sections 37 and 38 of *PHIPA* permit the use and disclosure of personal health information without the consent of the individual to whom the personal health information relates in specific circumstances.

[8] Further, sections 10(1) and (2) provides that health information custodians shall have in place information practices that comply with the requirement of *PHIPA*. In addition, section 12(1) requires health information custodians to take reasonable steps to ensure that personal health information in its custody or control is protected against,

---

[1] PHIPA Decision 74.

among other things, loss.

[9] There is no dispute between the parties, and I find, that the information at issue in this complaint is the personal health information of the complainant's son, within the meaning of section 4(1) of *PHIPA*. In addition, I am satisfied that the complainant is acting for her deceased son and that her request to the hospital for information relating to her son is to be treated as a request for access under section 52(1) of the *Act*.[2]

[10] Finally, it is not in dispute, and I find that, the hospital is a "health information custodian" as defined in section 3(1) of *PHIPA*.

The complaint and the hospital's response

[11] The complainant made an access request under *PHIPA* to the hospital for records relating to her son's hospitalization from the date of his admission until his death two days later. The hospital issued a decision, informing the complainant that it could not fulfill a portion of her access request because it was unable to locate certain paper records in her son's medical file. The hospital advised that it could not locate the discharge summary or the nursing and physician notes.

[12] In its decision to the complainant, the hospital advised that when it became aware that records that should exist were missing, it:

- initiated an incident review with its senior management;
- reported the loss to this office; and
- conducted searches on at least three occasions.

[13] The hospital states in its decision letter that "we believe these records to be permanently lost but have no reason to believe they were improperly accessed or disclosed."

[14] As noted above, the complainant raised concerns about the hospital's inability to locate the missing records during mediation. In response, the hospital confirmed that it took the following steps:

---

[2] Section 23(1)(4) of *PHIPA* sets out the authority of a deceased person's estate trustee (or the person who assumed responsibility for the administration of the estate, if there is no estate trustee) to exercise powers with respect to a deceased person's personal health information. These powers include the authority to make a request for access to the personal health information of the deceased person.

- its Manager of the Emergency Department conducted searches for the missing records on three separate occasions.[3] In addition to searching the Emergency Department, the manager searched on-call rooms, research areas and areas designated for hospital fellows and medical residents. The manager also had all hospital staff and the Coroner's Office search their files. However, no records were located.

- it contacted the third-party vendor, who is responsible for scanning its paper records and converting them into electronic records. The hospital advised that it had the vendor search all paper records that were received during the period the missing records were created but no records were located.

- it provided the mediator with a copy of the processes[4] it has in place with the vendor, including the roles and responsibilities of the hospital and the vendor during the medical record conversion process, including transport, scanning, storage and destruction.

- it conducted an audit of the patient's electronic health record, at the request of the mediator. This audit concluded that only individuals in the patient's circle of care accessed the complainant's son's electronic records.

[15] Also during mediation, in response to the complainant's concerns that a privacy breach had occurred, the hospital:

- issued an apology to the complainant's family regarding the missing records.

- confirmed that its Breach Management Procedure[5] is still in place. This document describes the steps that are to be taken in the event of a privacy breach, and includes identifying the scope of the breach, containing the breach, notifying affected parties, and investigating the breach;

- advised that as a result of this incident, it conducted a review of its record management practices and recommended that patient charts be kept in a locked cabinet when they are not in use. The hospital also advised that it created a logbook to be used by medical staff to sign patient records in and out;

---

[3] I note that the hospital's decision letter indicates that searches were conducted on June 29, July 12 and August 3, 2016 whereas during mediation, the hospital advised that four separate searches were conducted on June 29, July 12, July 22 and August 4, 2016.
[4] The hospital provided a 13-page document prepared by the vendor, dated February 2015.
[5] The hospital provided a copy of its three-page "Breach Management Procedure" to this office.

- sent out communications to all of its medical staff, reminding them of the importance of keeping track of patient records. The hospital also discussed the incident with its Quality of Care Committee; and

- advised that it has been meeting with its vendor to better ensure the security of all personal health information sent for scanning – from the time the paper records are picked up by the vendor at the hospital, until the records have been scanned and destroyed. In addition, the hospital advises that its Health Records Services Department now reviews the vendor's manifest to ensure that records logged for offsite scanning appear on the manifest.

The Hospital's Duty to Protect Personal Health Information

Information Practices

Did the hospital have in place information practices that comply with the requirements of section 10(1)?

[16] Sections 10(1) and (2) of *PHIPA* states:

> 10(1) A health information custodian that has custody or control of personal health information shall have in place information practices[6] that comply with the requirements of this Act and its regulations.
>
> 10(2) A health information custodian shall comply with its information practices.

[17] In PHIPA Order HO-004, this office stated:

> Health information custodians should review their information practices regularly to ensure that they remain appropriate for their operations. As the health information custodian's operations evolve and grow, and as a result of the introduction of new information technology, it is important to update information practices to reflect these changes. A health information custodian should take steps to ensure that the contents of its policies and procedures are kept current to reflect actual practices. In addition, a health information custodian should keep abreast of

---

[6] Section 2 of the Act defines "information practices" 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,
>
> (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.

> developments relating to safeguards to ensure that they comply with the *Act*.
>
> In addition, when adopting policies and procedures, a health information custodian needs to ensure that staff members and independent contractors are made aware of new policies and procedures by proper notice, either through the use of the internal mail system, electronic mail and/or educational sessions.

[18] The reasoning in PHIPA Order HO-004 was adopted in PHIPA Order HO-013 in which this office also stated:

> Privacy policies and procedures on their own, however, are not sufficient. Health information custodians must also take steps to ensure that agents are aware of and understand their obligations and limitations under [*PHIPA*] and under the privacy policies, practices and procedures that custodians have implemented and that agents are aware of and understand the consequences of failing to comply with these obligations and limitations.

[19] I adopt the reasoning in PHIPA Orders HO-004 and HO-013 and apply it to the circumstances of this complaint. Having reviewed the details of the complaint along with the hospital's response, I am satisfied that the hospital presently has information practices in place that are relevant to the circumstances of this complaint which comply with the requirements of *PHIPA* and its regulations.

[20] Before the loss occurred, the hospital already had a Breach Management Procedure in place, which identified the steps to be taken to ensure the proper identification, reporting, containment, notification, investigation and remediation of privacy breaches. The hospital also had a process in place with the third-party vendor that identified their joint responsibilities. Upon becoming aware of the loss, the hospital:

- notified the complainant that it could not locate some of her son's medical records as required under the notification provisions of its breach management procedure and as required under *PHIPA*;
- revised its record keeping practices to ensure that additional precautions are taken to safeguard patient charts by creating a logbook and keeping the charts in locked cabinets when not in use. In addition, its Health Record Services Department now reviews the vendor's manifest to ensure all records being transported offsite are properly logged;
- sent communications to staff to remind them of their responsibilities regarding patient files; and

- facilitated meetings and discussions with its Quality of Care Committee and the third-party vendor about issues relating to not being able to locate the complainant's son's records.

[21] In my view, the hospital's response demonstrates that it complied with its pre-existing information practices, which included notifying the complainant and this office about the loss and taking steps to ensure that its staff and vendor understood their obligations under *PHIPA*. Upon becoming aware of the loss, the hospital also reviewed its existing policies and practices and added additional safeguards to its information practices. Accordingly, I am satisfied that the hospital took adequate steps to ensure that it has in place information practices that comply with the requirements of section 10(1).

[22] The hospital's information practices before the loss may also have complied with section 10(1). However, it is not necessary for me to make a finding on whether the hospital was in compliance with section 10(1) at the time of the loss because I am satisfied that its response to the complaint demonstrates that its information practices, as relevant to the circumstances of this complaint, now comply with section 10(1). In this context, therefore, I have decided that no order against the hospital is warranted.

Security

Did the hospital comply with section 12(1) by taking reasonable steps to ensure that personal health information in its custody or control is protected against theft, loss and unauthorized use or disclosure?

[23] Section 12(1) states:

> 12 (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.
>
> (2) 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,
>
> - notify the individual at the first reasonable opportunity of the theft or loss or of the unauthorized use or disclosure; and
>
> - include in the notice a statement that the individual is entitled to make a complaint to the Commissioner.

> (3) If the circumstances surrounding a theft, loss or unauthorized use or disclosure referred to in subsection (2) meet the prescribed requirements, the health information custodian shall notify the Commissioner of the theft or loss or of the unauthorized use or disclosure.

[24] In PHIPA Decision 50, regarding the obligations of health information custodians with respect to protecting personal health information, this office stated:

> Taken together, sections 12(1) and 13(1)[7] of the *PHIPA* impose significant obligations on health information custodians to protect personal health information in their custody or control. One of the most important ways that health information custodians can protect this information, particularly in a multi-party relationship, is by clearly setting out roles and responsibilities in writing. At the most basic level, this includes addressing who is the health information custodian assuming the responsibilities under sections 12(1) and 13(1), and who is responsible for personal health information in the event of a change of practice. All too often, individuals and organizations report privacy breaches to the IPC where, at their core, the issues in dispute stem from a failure of the parties to properly clarify and document their own relationship and obligations.

[25] In PHIPA Decision 74, this office concluded that a hospital took adequate steps to respond to a complaint though it originally failed to identify a doctor's unauthorized access to an electronic medical record. In that decision, Assistant Commissioner Sherry Liang stated:

> The duty to take reasonable steps to ensure that personal health information in the hospital's custody or control is protected against theft, loss and unauthorized use or disclosure includes a duty to respond adequately to a complaint of a privacy breach. A proper response will, among other things, help to ensure that a breach, if any, is contained, and will not re-occur. The standard in section 12 is "reasonableness". It does not require perfection, and the section does not provide a detailed prescription for what is reasonable.

[26] I adopt and apply the reasoning in PHIPA Decisions 50 and 74 to the circumstances of this complaint. Having regard to the details of the complaint and the hospital's response, I am satisfied that upon becoming aware of the breach, the hospital took reasonable steps to ensure that records of personal health information in its custody or control are protected as required under section 12(1) of the *Act*.

---

[7] Section 13(1) of the *PHIPA* requires that health information custodians retain, transfer, and dispose of records of personal health information in a secure manner.

[27] As mentioned above, the hospital and third party vendor have a written process in place that predates the events from which this complaint arose that identifies their joint responsibilities with regard to the transport, scanning, storage and destruction of medical files. After notifying the complainant of the loss, the hospital reviewed and revised its policies and procedures and created additional safeguards to protect the personal health information in its custody or control. In addition, the hospital facilitated meetings and discussions with its Quality of Care Committee and the third party vendor. Finally, the hospital took steps to educate its staff about their responsibilities regarding patient records.

[28] Given my conclusion that the hospital took reasonable steps to safeguard the personal health information in its custody or control in response to the complaint, I find that there is no need for me to order the hospital to comply with additional measures. As I have decided against making an order against the hospital, it is not necessary that I also make a determination as to whether the hospital was in compliance with section 12(1) at the time of the loss of records.

Other Issue

[29] I note that in the complaint form submitted to this office the box entitled "The institution has inappropriately disclosed [personal health] information" was checked off. However, it does not appear that this issue was pursued or discussed at mediation. In any event, when I wrote to the complainant to share my preliminary view that the complaint did not appear to warrant a review, I also advised her that there appeared to be insufficient evidence to substantiate a complaint that her son's personal health information was "disclosed" within the meaning of section 2.[8] In addition, I advised the complainant that I also reviewed the particulars the hospital provided about its contractual relationship with the third party vendor regarding the transportation, scanning, storage and destruction of medical records and that my preliminary view was that the arrangement appeared to be a permitted "use" under sections 37(1) and (2).

[30] Sections 37(1)(a) and (2) read:

> 37(1) A health information custodian may use personal health information about an individual,
>
> > (a) for the purpose for which the information was collected or created and for all the functions reasonably necessary for carrying

---

[8] Section 2 of *PHIPA* defines the terms "disclose" and "use", as follows:

> "disclose", in relation to personal health information in the custody or under the control of a health information custodian or a person, means to make the information available or to release it to another health information custodian or to another person, but does not include to use the information.

> out that purpose, but not if the information was collected with the consent of the individual or under clause 36(1)(b) and the individual expressly instructs otherwise;
>
> (b) for a purpose for which this Act, another Act or an Act of Canada permits or requires a person to disclose it to the custodian;
>
> 37(2) If subsection (1) authorizes a health information custodian to use personal health information for a purpose, the custodian may provide the information to an agent of the custodian who may use it for that purpose on behalf of the custodian.

[31] Section 2 of PHIPA defines the term "use", as follows:

> "use", in relation to personal health information in the custody or under the control of a health information custodian or a person, means to view, handle or otherwise deal with the information, subject to subsection 6 (1), but does not include to disclose the information …

[32] PHIPA Decision 29 considered the question of whether a medical records storage company, acting an as agent to a hospital, acted lawfully under the *PHIPA*. The decision found that a health information custodian may delegate its responsibilities for health records to an agent, like the third party vendor in this complaint, subject to the requirements set out in section 17(1).[9] In that order, Assistant Commissioner Sherry Liang stated:

> Among the purposes of the *Act* are the establishment of rules, in section 1(a),
>
> > ...for the collection, use and disclosure of personal health information about individuals that protect the confidentiality of that information and the privacy of individuals with respect to that information, <u>while facilitating the effective provision of health care</u> [emphasis added in original]
>
> It is evident that having accurate and complete records of personal health information facilitates the effective provision of health care. The *Act* should not be interpreted so that health information custodians are unable to upgrade or improve the format in which their records are retained. The *Act* plainly permits health information custodians to use electronic means

[9] Section 17(1) provides that a health information custodian is responsible for personal health information in its custody or control and may permit its agents to collect, use, disclose, retain or dispose the personal health information on its behalf in certain circumstances.

> to collect, use, modify, disclose, retain or dispose of personal health information. I find that the ability to scan a paper record into electronic format is necessarily ancillary to the ability to keep electronic records of personal health information. As such, this use is permitted by section 37(1)(b)…

[33] I agree with the reasoning in PHIPA Decision 29, and apply it to the circumstances of this complaint. First, I am satisfied that the third party vendor is an agent of the hospital and, similar to PHIPA Decision 29, that the hospital's delegation of its responsibilities over health records to the vendor for the purpose of scanning and converting them to electronic format is authorized under section 17(1). Finally, I accept that the medical record conversion process carried out on the hospital's behalf by its agent includes the transport, scanning, storage and destruction of its paper records and is necessarily ancillary to the provision of health care. I find, therefore, that the arrangement between the hospital and the third party vendor is a permitted "use" under section 37(1)(a).[10]

[34] Additionally, in the absence of submissions from the complainant or evidence otherwise, I also find no basis upon which to make a finding that an unauthorized "disclosure" under section 38 has occurred in the circumstances of this complaint.

DECISION:

[35] Sections 57(3) and 57(4)(a) of *PHIPA* set out my authority to decline to review a complaint as follows:

> 57(3) If the Commissioner does not take an action described in clause 1(b) or (c) or if the Commissioner takes an action described in one of those clauses but no settlement is effected within the time period specified, the Commissioner may review the subject-matter of a complaint made under this Act if satisfied that there are reasonable grounds to do so.
>
> 57(4) The Commissioner may decide not to review the subject-matter of the complaint for whatever reason the Commissioner considers proper, including if satisfied that,
>
> > (a) the person about which the complaint is made has responded adequately to the complaint;

---

[10] I agree with the reasoning in PHIPA Decision 29 but find that section 37(1)(a), rather than (b), is applicable to this type of situation.

[36] For the reasons stated above, I have decided not to review this complaint on the basis that the hospital has responded adequately to the complaint. I issue this decision in satisfaction of the notice requirement in section 57(5).

NO REVIEW:

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

Original signed by: February 8, 2019

Jennifer James
Adjudicator