Information and Privacy Commissioner,
Ontario, Canada

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

PHIPA DECISION 74

HC15-4

Sault Area Hospital

August 10, 2018

Summary: A physician accessed records of personal health information of a deceased individual contrary to the *Personal Health Information Protection Act*. The hospital initially failed to identify the unauthorized accesses, but took appropriate action over time to investigate the privacy breach, notify the deceased individual's estate and improve its practices with respect to the protection of personal health information in its electronic medical record. Further, while there was no dispute that most of the physician's accesses to the individual's personal health information were unauthorized, the evidence does not establish that the physician also disclosed the personal health information in contravention of the *Act*. In view of the steps taken to respond to the privacy breach, the IPC determines it is not necessary to issue any orders against the hospital or the physician.

Statutes considered: *Personal Health Information Protection Act, 2004*, S.O 2004, c.3., Sched. A, sections 2 (use), 2 (disclose), 6(1), 12(1), 23(1)4.

Orders and Investigations Reports Considered: Order HO-010

BACKGROUND:

[1] In the fall of 2014, a family member of a deceased individual raised suspicions with the Sault Area Hospital about the possibility that a physician had accessed the personal health information of the deceased individual, without authority and contrary to the *Personal Health Information Protection Act, 2004* (the *Act*). The deceased individual was a patient of the hospital and had died earlier in 2014. At the time of the

events, the physician was a coroner in the area served by the hospital, and also had privileges at the hospital. The physician is related by marriage to the deceased individual.

[2] The family member was not satisfied with the hospital's response to his concerns, and filed a complaint with this office, alleging inappropriate collection, use and disclosure of the deceased individual's health information. On the information before me, I find the family member to be a person with authority to make this complaint in place of the deceased individual under section 23(1)4 of the *Act*. In this decision, I will refer to the family member as the "complainant".

[3] Mediation through this office did not resolve the complaint and it was therefore transferred to the adjudication stage of the complaint process. I decided to conduct a review of the issues raised by the complaint and received written submissions from the hospital, the physician and the complainant. I have not identified the physician in this decision, as doing so may lead to identification of the deceased individual.

DISCUSSION:

Introduction

[4] Broadly speaking, the *Act* regulates the activities of a group of persons described as "health information custodians" and their agents, with respect to personal health information. One of the purposes of the *Act* 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 the *Act* 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. The *Act* also permits certain collections, uses and disclosures of personal health information without the consent of the individual to whom the information relates.

[5] Under sections 17 and 37(2) of the *Act*, a health information custodian which is permitted to use personal health information may permit its agents to use that information in order to carry out their duties.

[6] It is not in dispute, and I find, that the hospital is a health information custodian. The hospital states that the physician was an "agent" of the hospital within the meaning of the *Act* in relation to the accesses at issue in this complaint. The physician does not disagree, stating that although the relationship had not to date been formalized in writing, he is likely an agent of the hospital. I am satisfied that the physician was an agent of the hospital within the meaning of the *Act* with respect to the accesses at issue in this complaint, with the exception of one access which I will discuss separately below.

[7] It is also not in dispute, and I find, that the information at issue in this complaint is the personal health information of the deceased individual, within the meaning of section 4 of the *Act*.

The physician's accesses to the deceased individual's personal health information

[8] Section 2 of the *Act* defines "use" and "disclose" 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 handle or deal with the information, subject to subsection 6 (1), but does not include to disclose the information, and "use", as a noun, has a corresponding meaning;[1]
>
> "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, and "disclosure" has a corresponding meaning;

[9] Section 6(1) clarifies that the provision of personal health information by a health information custodian to its agents is a "use" and not a "disclosure" under the *Act*:

> For the purposes of this Act, the providing of personal health information between a health information custodian and an agent of the custodian is a use by the custodian, and not a disclosure by the person providing the information or a collection by the person to whom the information is provided.

[10] When the complainant raised his concerns about a potential privacy breach with the hospital, it conducted an audit of its electronic medical record to determine whether the physician had accessed the deceased individual's information. The hospital's privacy officer concluded, and advised the complainant, that the physician accessed the deceased individual's information on only one occasion, on the date of her death. The hospital's view was that this access was authorized, in that it was done in connection with the physician's role as coroner.

[11] After the family member filed his complaint with this office, the hospital's new privacy officer conducted additional audits. These further audits revealed that, in addition to the one access previously detected, the physician viewed the deceased individual's personal health information on a number of occasions in 2011 and on an

---

[1] This definition of "use" was in force at the time of these events, and has since been amended. The change has no bearing on the outcome of this complaint.

additional occasion on the date of her death, in 2014. After reviewing these accesses, the hospital concluded that apart from the first access on the date of death in 2014, the accesses were not authorized under the *Act*.

[12] The hospital notified the complainant of its findings, and of its view that these additional accesses were unauthorized. Initially, it provided this information orally and then, later, in a letter detailing the results of its audit.

[13] The physician has reviewed the results of the hospital's audits. He states that he has no memory of them, but has no reason to dispute the information in the audits.

[14] The physician states that he was never the family physician for the deceased individual, although he also states that over the years, she asked him to be involved in her health care at times, such as to facilitate referrals and to "provide episodic care". He does not assert that any of the accesses in question were for the purpose of providing health care to the individual.

[15] With respect to the first access on the date of the individual's death, the physician states that he was the coroner on call and viewed the individual's information in connection with his role. Initially, he was unaware of the identity of the patient. Once the physician determined the identity of the deceased individual, and given the familial relationship, the physician arranged to have the case transferred to another coroner.

[16] However, following that transfer, the audit shows an additional access later in the same day. As stated above, the physician does not dispute that any of the accesses occurred. Apart from the first access on the date of the individual's death, the physician does not take the position that the accesses were authorized under the *Act*.

[17] There is conflicting information in the material before me about the number of accesses occurring in 2011. The hospital has, at different times, stated that its audit revealed 16 or 57 accesses by the physician, in 2011. The physician has reviewed the audit results and believes they show 13 accesses. The hospital's reference to 57 accesses appears to be a mistake as it provided this office with a detailed explanation of the audit results and the basis for its conclusion that there were 16 accesses over a little more than a week. On my review of the material before me, including the summary of the audit results and the hospital's explanations of those results during the course of the IPC's investigation, I find that the accurate number is 16 accesses, occurring over a period of approximately one week in 2011.

[18] As indicated above, I accept and agree with the hospital's assertion that the physician was an agent of the hospital with respect to most of the accesses in question. Those accesses are, having regard to section 6(1) above, "uses" within the meaning of the *Act*.

[19] One access, however, on the date of the deceased individual's death, was in connection with the physician's role as a coroner. It is open to question whether the

physician was acting as an agent of the hospital on this occasion. If he was not, then this access was a "disclosure" of personal health information by the hospital, and not a "use." The parties did not address this in their submissions and it is not necessary to come to a definitive conclusion on this question because I am satisfied that whether this access is characterized as a disclosure of personal health information by the hospital, or a use, it was authorized under the *Act*.[2]

[20] There is no evidence that the physician viewed the personal health information with consent, or (apart from the access discussed above) for a purpose permitted without consent by the *Act*. I find that, apart from the first incident on the date of the individual's death, the accesses by the physician were unauthorized uses under the *Act*.

The allegation that the physician disclosed the personal health information of the deceased individual

[21] The complainant alleges that the physician disclosed the deceased individual's personal health information to a named family member. There is no dispute that if it occurred, such a disclosure was not made with consent or otherwise authorized under the *Act*.

[22] The complainant's submissions in support of the allegation refer to incidents that formed the basis of another complaint before this office. They relate to events that occurred in a different time period from the ones covering these accesses.

[23] The physician has submitted affidavits from himself and the family member to whom he is alleged to have disclosed the information. The family member states that the physician has never disclosed personal health information of the deceased individual to her. In the physician's affidavit, he denies disclosing this individual's health information to anyone. Among other things, he states,

> I believe that it must have been my concern about [the deceased individual's] well-being that led me to access her EMR [electronic medical record].
>
> ….
>
> I know now that proceeding in this way was misguided and wrong. While I obviously proceeded with ignorance, it would never have been with the intention of causing any harm or of using the information to [the deceased individual's] detriment in any way, nor would it have been in order to disclose it to anyone.

---

[2] See section 43(1)(g) of the *Act*, and the provisions of the *Coroners Act*, R.S.O. 1990, c. C.37.

> I never disclosed or shared any of [the deceased individual's] personal health information with anyone, including [family members]. This would have been a breach of confidentiality. While I did not fully understand the related but distinct concept of patient privacy, I have always understood and respected doctor-patient confidentiality.
>
> I graduated from medical school in 1973 and have always understood and taken doctor-patient confidentiality very seriously. It is sacrosanct and I have never disclosed information from anyone's medical records to a third party without authorization. However, I did not fully appreciate the related but distinct concepts of patient privacy, the circle of care and the "need to know" principle.

Analysis

[24] The complainant's submissions do not provide direct evidence that the physician disclosed the personal health information at issue to the other family member. Given that they relate to other events, in another timeframe, and not with respect to the personal health information viewed by the physician in 2011 and 2014, I do not find them compelling evidence in this complaint.

[25] Despite the lack of direct evidence, however, I can appreciate the complainant's suspicion, given the number of accesses and the familial relationships involved, that the physician disclosed the personal health information. With this in mind, I turn to the physician's affidavit evidence.

[26] In assessing the reliability of the affidavit statements, I take into account the physician's own acknowledgements about the events, and his willingness to accept responsibility for the unauthorized accesses. I consider the physician's acknowledgement that he did not fully understand his obligations under *PHIPA* regarding patient privacy, while understanding and respecting the importance of doctor-patient confidentiality. On balance, I accept the physician's sworn statement on the allegation of disclosure. It provides direct evidence in support of his position and in all the circumstances, I find it persuasive.

Duty to protect personal health information

[27] Section 12(1) requires custodians to take reasonable steps to protect personal health information in their custody or control against unauthorized uses or disclosures. 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.

[28] 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.

[29] The complainant believes that the hospital's response to the complaint of unauthorized access fell short of the standards required by the *Act*. First, the complainant believes that the hospital failed to adequately investigate the complaint when it was first brought to its attention. As described above, the hospital's initial audit and investigation led it to inform the family that there was only one access, in the early morning of the date of the individual's death. The hospital's representative informed the family of the hospital's view that this access was authorized.

[30] After the complaint was filed with the IPC, the hospital ran further audits which revealed additional accesses, in 2011 and 2014. The complainant believes that the fact that he did not learn of these additional accesses until he filed this complaint demonstrates the hospital's lack of commitment to responding to the complainant's concerns.

[31] The complainant also believes that the discipline imposed on the physician for the incidents (see below) was inadequate. Given the number of unauthorized accesses, he suggests that a more severe discipline was warranted.

[32] The hospital described the manner in which it investigated the complaint of unauthorized access when it was brought to its attention. It does not disagree that it informed the complainant initially that it had not found any unauthorized accesses and that the only access it detected was within the scope of the physician's role as coroner on the day of the individual's death. The hospital states that it conducted a further audit, which led it to meet with the individual's family to share the results. At that time, it also apologized to the individual's family.

[33] The hospital states that it launched a full investigation and brought the matter to the Medical Advisory Committee. This Committee recommended to the Board of Directors that the physician's privileges be suspended for three months, that the hospital conduct enhanced monitoring of the physician's access to the electronic medical record for three years, and that, on his return to practice, the physician be required to present at Grand Rounds on the topic of privacy. The Board accepted all the recommendations, and implemented them.

[34] The hospital's submissions describe administrative and technical changes it has made to better protect the privacy of the personal health information of its patients. During my review, it committed to a firm date by which it will implement annual electronic privacy training for its agents, which will include privacy training for physicians as part of their reappointment process.

[35] With respect to the complainant's submissions about the alleged inadequacy of the three-month suspension, the physician submits that the sanctions imposed on him by the hospital were significant. A three-month suspension of privileges is not an inconsequential penalty. Further, he states that he has made two presentations on privacy at the hospital, in which he spoke candidly about his personal experience. The physician states that he has turned his situation into an opportunity to teach other colleagues about his mistakes and how to avoid making these mistakes. The physician also states that he has also undergone instruction in medical ethics as it relates to patient privacy, at his own expense.

[36] The physician also submits that IPC does not have jurisdiction to come to a disposition regarding the severity or appropriateness of sanctions taken by the hospital in response to these events, relying on IPC Orders HO-002 and HO-010.

Analysis

[37] I share the complainant's concern about the hospital's initial investigation into his allegations. The hospital has not given a satisfactory answer for why its initial audit, or the hospital's interpretation of that audit, failed to reveal any unauthorized accesses. As a result of this failure, it was not until about a year later, following a further audit, that the complainant's suspicions were confirmed. Although the hospital met with the complainant to share its findings from the additional audit, it did not provide this information in writing until many months after this. One consequence of the lack of written confirmation was a lack of clarity about what information the hospital conveyed during the meeting, with the complainant ultimately left without an understanding of the details of the privacy breaches until well into the IPC's investigation of his complaint.

[38] Whether the lapse in the hospital's initial response was due to technical error or human failings, and could on its own be considered a failure to properly safeguard patient information, I am satisfied that the hospital has taken adequate steps since then to meet its obligations under the *Act*. Among other things, the hospital has installed a new auditing program that considerably enhances its ability to detect unauthorized accesses. It updated its Privacy and Confidentiality Policy, which applies to all agents of the hospital. As described above, the hospital has developed a yearly electronic privacy training program for all staff, volunteers and learners and will require all credentialed physicians to complete this training as part of the annual reappointment process. The hospital also strengthened the privacy warning on its electronic system, which warns users that unauthorized use of personal health information may result in disciplinary

action.

[39] As indicated above, the hospital imposed a sanction on the physician that the complainant believes was inadequate in the circumstances. This office has stated, in similar circumstances, that the focus of this office is not the severity or appropriateness of the sanctions taken by a health information custodian against its agents; this is not part of the Commissioner's statutory role. Rather, the issue for this office is whether the actions taken provide adequate safeguards in accordance with section 12(1) of the *Act*.[3]

[40] In this case, the hospital took disciplinary action in conjunction with the adoption of additional or enhanced technical and administrative measures to safeguard personal health information in its custody or control. The physician delivered presentations to his colleagues at the hospital in which he was frank about his role in and responsibility for the privacy breach. Taken as a whole, I am satisfied that the hospital has taken adequate steps to respond to the issues raised by this complaint and there is no need for me to order additional measures against either the hospital or the physician.

NO ORDER:

1. For the foregoing reasons, no order is issued.

Original Signed by: August 10, 2018
Sherry Liang
Assistant Commissioner

[3] See Order HO-010.