Information and Privacy Commissioner,
Ontario, Canada

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

PHIPA DECISION 153

Complaint HR18-118

Quinte Health Care

July 27, 2021

Summary: The hospital reported three privacy breaches to the Information and Privacy Commissioner of Ontario (IPC). Despite efforts at the intake and investigation stages of the IPC's process to obtain complete and clear information about the breaches, the IPC was not satisfied with the response of the hospital and commenced a review into the circumstances. After a review, the adjudicator concluded that the hospital failed in its duty to notify the affected patients of unauthorized uses of their personal health information, as required by the *Personal Health Information Protection Act, 2004*. Given the passage of time and the relatively benign circumstances of the privacy breaches, no useful purpose would be served by ordering notification at this time.

Statutes Considered: *Personal Health Information Protection Act,* 2004, S.O. 2004, c. 3; sections 12(1), 12(2)(a).

INTRODUCTION

[1] During its investigation of a complaint alleging unauthorized accesses by an employee to a patient's health information, Quinte Health Care (the hospital) conducted an audit of the employee's uses of the hospital's electronic medical records (EMR). This audit led the hospital to identify additional accesses of concern. The hospital reported these accesses to the Information and Privacy Commissioner of Ontario (the IPC or this office) as privacy breaches.

[2] After an initial review of the breaches at the intake stage, the IPC referred them to an investigator for further investigation. The investigator sent several requests for information to the hospital. The hospital provided responses and, despite attempts to clarify those responses, the investigator was not able to obtain a complete and clear answer to her requests for information.

[3] This matter was thus referred to the adjudication stage of the IPC's processes. As the adjudicator, I reviewed the file and was satisfied that there were reasonable grounds to review the subject-matter of the complaint under the *Personal Health Information Protection Act, 2004* (the *Act*). I issued a Notice of Review, inviting the hospital to respond to the issues, as well as to answer specific questions arising from the material before me.

[4] As described below, while I find that the hospital failed in its duty to notify the affected patients of uses of their personal health information which the hospital concluded were unauthorized, I see no useful purpose in directing that such notice be given at this time. Apart from the failure to notify, I also find that the hospital's response to the breaches was adequate.

BACKGROUND

[5] 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, unless the *Act* permits or requires this to be done without consent (section 29).

[6] Section 12(2)(a) of the *Act* requires notification to patients of unauthorized accesses to their personal health information, among other things:

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

[7] As a preliminary matter there is no dispute, and I find, that the person who operates the hospital is a "heath information custodian" within the meaning of section 3(1) of the *Act*.

[8] A health information custodian that is permitted to use personal health information may permit its agents to use that information as necessary to carry out their duties [sections 17 and 37(2) of the *Act]*. It is not in dispute that at all relevant times, the employee in question was acting as an "agent" of the hospital within the meaning of the *Act*.

Did the hospital comply with section 12(2)(a) of the *Act*?

[9] In this case, as a result of an earlier incident involving this employee, the hospital issued a new job description for the role, setting out the processes to be followed by staff fulfilling the duties of the role and the accesses to personal health information permitted for the role. It also trained employees, including this one, on the new processes. The audit referred to above showed accesses to three patients' records by the employee in question, which appeared to be inconsistent with the new directions issued by the hospital. This prompted the hospital to report these to the IPC, as privacy breaches.

[10] At the conclusion of the IPC's investigation stage, the material before the investigator still did not clearly establish the dates of the purported unauthorized accesses to the three affected patients' health information, and was unclear about other aspects of the events. The hospital has, in response to the Notice of Review, explained the reasons for the unclear information, and has confirmed that the accesses occurred in November and December of 2017. It has also clarified other information provided to the investigator about the circumstances of the apparent breaches.

[11] The hospital states that as part of its investigation into the audit results, it interviewed the employee about the accesses. This individual stated that she did not recall the accesses to the health records of the three patients, it was a mistake, and she was trying to stay within the new protocol while fulfilling her duties. Based on its investigation, including a review of other accesses shown in the audit, the hospital accepted this explanation. The hospital states that the actions of the employee were not malicious and the explanation given pointed to a circumstance where the employee had adopted the new processes but had made a mistake.

[12] The hospital informed the IPC, however, that as a result of these accesses and an unrelated unauthorized disclosure of personal health information by this employee, the hospital imposed a 5-day unpaid suspension and reported her to the College of Nurses of Ontario (CNO). The hospital also advised the employee that further unauthorized access to patient files would result in termination of employment.

[13] The hospital's actions were somewhat contradictory: although it accepted that the accesses were genuine mistakes, it also viewed them as serious enough to warrant, in conjunction with another incident, disciplinary action. Further, it reported these as privacy breaches to the IPC. Notwithstanding the actions of the hospital, which appear to treat the incidents as unauthorized uses of personal health information, it did not notify the affected patients.

[14] In answer to the question in the Notice of Review regarding the requirements of section 12(2)(a), the hospital indicated that it believed notice to patients was not required in the circumstances before it as "this was not a snooping (use) incident. These were instances of a nurse not adhering fully to a new internal hospital process".

[15] I find that, in the particular circumstances of this case, the hospital was obligated to notify the affected patients.

[16] Section 12(2)(a) requires health information custodians to notify individuals at the first reasonable opportunity of unauthorized uses of personal health information in the

custodian's custody or control. These requirements are not limited to instances of "snooping", by which I understand the hospital to mean deliberate, intentional misuses of personal health information. They can apply to privacy breaches which occur without such intent.

[17] On the other hand, this office has also recognized that agents engaged in the delivery of health care may on occasion access personal health information of individuals to whom they are not providing care, without leading to the conclusion that such accesses are "unauthorized." In PHIPA Decision 44, for instance, this office found certain unnecessary but incidental accesses to personal health information, as described in that decision, to be authorized as part of normal workplace practices in the process of delivering health care. Further, this office has advised the public that mistakes such as brief accidental entries into the wrong patient's electronic medical record do not trigger the obligation to notify patients under section 12(2)(a), and I agree with this interpretation of section 12(2)(a).[1]

[18] In this case, while the facts bear some indicia of the types of authorized accesses described above, the hospital seems to have concluded that the accesses in question were unauthorized. Certainly, it regarded them as contrary to its own policies and as meriting discipline and other remedial action. It also reported them to the IPC.

[19] In these particular circumstances, I find that the hospital was obligated to comply with section 12(2)(a).

[20] While I conclude that the hospital should have notified the affected patients of uses of their personal health information which it had concluded were unauthorized, I see no reason to order it to do so now. Given the passage of time and the relatively benign circumstances, I see no purpose in directing that such notice be given.

Did the hospital respond adequately to its discovery of the unauthorized access to three patients' personal health information?

[21] The hospital's responsibility to investigate and respond to a privacy complaint arises from its obligations under section 12 of the *Act*. Section 12(1) 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] The duty to take reasonable steps to protect personal health information in the hospital's custody or control, including against unauthorized disclosure, includes a duty to respond adequately to a complaint of a privacy breach. Among other things, a proper response will help ensure that any breach is contained and will not re-occur.[2] This office has stated that the standard in section 12(1) is "reasonableness". It does not require

---

[1] IPC Webinar: Reporting Health Privacy Breaches to the IPC, June 22, 2018: https://www.youtube.com/watch?v=6IzrkjIWGs8

[2] PHIPA Decision 44, at para 140.

perfection, and the section does not provide a detailed prescription for what is reasonable.[3]

[23] As described above, when the hospital's audit identified some questionable accesses to patients' health records by the employee in question, it interviewed the employee to obtain an explanation. Following this (and partly as a result of another incident), the hospital imposed an unpaid suspension, reported the employee to the CNO, and advised her that further unauthorized accesses would result in termination of employment. The hospital also implemented a learning plan for the employee, which included content directed at privacy obligations and processes. The hospital informed the IPC that the learning plan consists of high level goals and guiding principles, then more detailed goals, learning objectives and success indicators. In this particular case, the detailed goals consisted of: privacy and confidentiality, accountability, professional standards, ethics, circle of care and leadership. The employee completed this learning plan by February 2018.

[24] Also as a result of this incident, the hospital audited this employee's accesses to the EMR every 2-3 months to confirm that the individual is following its processes.

[25] In the circumstances, I find that the hospital responded adequately to the apparent privacy breaches by investigating the circumstances, and taking remedial action.

Conclusion

While I have determined that the hospital failed to comply with section 12(2)(a) of the *Act*, I find it unnecessary to issue any orders.

Original Signed by: July 27, 2021

Sherry Liang
Assistant Commissioner Tribunal Services

[3] PHIPA Decision 44, at para. 141.