Information and Privacy Commissioner,
Ontario, Canada

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

PHIPA DECISION 155

Complaint HC17-64

Quinte Health Care

July 28, 2021

Summary: In this decision, the adjudicator determines that Quinte Health Care (the hospital) breached the *Personal Health Information Protection Act, 2004* in permitting staff fulfilling a designated role to access personal health information not reasonably necessary to the role. The inadequacies of the hospital's processes and policies in defining the access to patient information appropriate to this role resulted in unauthorized accesses to the complainant's personal health information. This decision also finds that an investigation of allegations of breaches of the complainant's privacy was conducted in a manner contrary to the hospital's privacy policies, resulting in other unauthorized accesses. The adjudicator concludes, taking into account a second investigation, that the hospital's response to the privacy breach was adequate. The hospital has taken steps to remedy the deficiencies in its processes and policies and no orders are necessary.

Statutes Considered: *Personal Health Information Protection Act, 2004, S.O. 2004, c. 3; sections 12(1), 17(1) and (3), 30(2).*

Decisions Considered: PHIPA Decision 44.

INTRODUCTION:

[1] The complainant is a nurse at Quinte Health Care (the hospital), who alleges that some of her colleagues (including a supervisor and a manager) accessed her personal health information without authorization and, in one case, disclosed such information about her to another colleague.

[2] Mediation did not resolve the complaint and it was referred to adjudication. As the adjudicator, I decided to conduct a review of the issues raised by the complaint. I issued a Notice of Review to the hospital, initially, inviting it to respond to the issues. Its representations were shared with the complainant's counsel, who submitted representations in response. I invited the hospital to provide reply representations, which I

also have before me.

[3] For the reasons below, I find that the hospital breached section 30(2) of the *Personal Health Information Protection Act* (the *Act*) in using more of the complainant's health information than reasonably necessary to meet the purpose of that use. It also failed to take reasonable steps to ensure that nurses fulfilling a specific role did not use personal health information unnecessary to their duties. I also find that an initial privacy investigation into allegations of breaches of the complainant's privacy resulted in additional unauthorized uses of her health information, in that the investigation was conducted in a manner contrary to the hospital's own policies. I conclude, however, taking into account a second investigation, that the hospital responded adequately to the breaches, and no orders are necessary.

BACKGROUND:

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

[5] 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*. There is also no dispute that the complainant works at the hospital, and at the relevant time, also became a patient. As a result of the hospital's provision of health care to the complainant, the hospital has custody or control of her personal health information.

[6] 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 individuals named in the complaint were acting as "agents" of the hospital within the meaning of the *Act*.

[7] Section 17 of the *Act* addresses the circumstances in which a hospital may permit its agents to collect, use, disclose, retain or dispose of personal health information on its behalf, and restrictions on the agent's handling of such information:

> 17 (1) A health information custodian is responsible for personal health information in the custody or control of the health information custodian and may permit the custodian's agents to collect, use, disclose, retain or dispose of personal health information on the custodian's behalf only if,
>
> (a) the custodian is permitted or required to collect, use, disclose, retain or dispose of the information, as the case may be;

> (b) the collection, use, disclosure, retention or disposal of the information, as the case may be, is necessary in the course of the agent's duties and is not contrary to this Act or another law; and
>
> (c) the prescribed requirements, if any, are met.
>
> (1.1) A permission granted to an agent under subsection (1) may be subject to such conditions or restrictions as the health information custodian may impose.
>
> (2) Subject to any exception that may be prescribed, an agent of a health information custodian may collect, use, disclose, retain or dispose of personal health information only if,
>
> (a) the collection, use, disclosure, retention or disposal of the information, as the case may be,
>
> (i) is permitted by the custodian in accordance with subsection (1),
>
> (ii) is necessary for the purpose of carrying out his or her duties as agent of the custodian,
>
> (iii) is not contrary to this Act or another law, and
>
> (iv) complies with any conditions or restrictions that the custodian has imposed under subsection (1.1); and
>
> (b) the prescribed requirements, if any, are met.

[8] The *Act* states that "use", in relation to personal health information in the custody or under the control of a health information custodian, means to "view, handle or otherwise deal with the information" (section 2).[1] It also provides that the provision of personal health information by a custodian to its agents is a "use" and not a "disclosure" (section 6(1)).

[9] Finally, section 30(2) of the *Act* sets out a "limitation principle" on the collection, use or disclosure of personal health information:

> A health information custodian shall not collect, use or disclose more personal health information than is reasonably necessary to meet the purpose of the collection, use or disclosure, as the case may be.

[10] With this background, I turn to the facts of this complaint.

The events and investigation in 2016

[11] The complainant became unwell while working a shift at the hospital in February 2016. She attended the hospital's emergency department and was registered by triage

[1] The definition of "use" was amended on June 3, 2016, but this legislative change has no impact on my decision. I have quoted from the current version.

staff at 9:33pm on February 16, 2016. Shortly after this incident, the complainant left the workplace for a maternity leave, and did not return until about a year later.

[12] After the complainant left the workplace and unknown to her, her colleagues reported to a manager that the complainant's supervisor (Nurse A) and another nurse (Nurse B), had inappropriately viewed the complainant's personal health information on February 16. As a result of this report, Nurse A's manager (Manager A) investigated the allegation. Manager A's investigation, which was aided by another manager as well as a member of the hospital's human resources department, included an audit of the complainant's electronic medical records. The investigation also included interviews with four ICU staff members.

[13] Manager A concluded from her review of the audit that accesses to the complainant's personal health information by Nurse A were authorized. The audit did not confirm any accesses by Nurse B to the complainant's information. The investigation did, however, determine that Nurse A verbally disclosed the complainant's health information to Nurse B without authority, on February 16.

The investigation in 2017

[14] The complainant states that when she returned to work in early 2017, her colleagues told her about their allegations against Nurse A and Nurse B. After learning of these allegations, the complainant raised her concerns to the hospital and the hospital's privacy office initiated its own investigation. This investigation determined that, contrary to the hospital's policies, the manager had not forwarded the original complaint from the complainant's colleagues in February 2016 to the privacy office. Instead, as described above, Manager A oversaw the investigation.

[15] The complainant subsequently also alleged that Manager A accessed her records without authority under the *Act*.

[16] The 2017 investigation by the privacy office included another audit of Nurse A's accesses, a review of the audit results with the complainant, and an analysis of work schedules and the authority for any accesses shown in the audit results. This investigation led to disciplinary action against Nurse A. This second investigation concluded that there was no evidence to indicate that Nurse B had viewed the complainant's records.

[17] As stated above, the complainant also alleged unauthorized accesses to her records by Manager A, which the hospital also investigated. The hospital concluded that these accesses were authorized.

ALLEGATION OF UNAUTHORIZED ACCESSES BY NURSE A AND NURSE B

[18] Although Nurse A's particular role is relevant to this complaint, in that her specific role requires her to access patient information in certain situations, the hospital has asked that I not refer to that role in my decision. My understanding is that the hospital's request is based on concerns for the privacy of this individual. While I am not convinced that these privacy concerns are justified, I have decided to agree to its request. The result is that I

have left some details about this role out of my decision. The complainant is aware of these details, through her work at the hospital.

[19] The complainant alleges that Nurse A, Nurse B and Manager A used her health information without authority under the *Act* when they viewed her records in the hospital's electronic medical records system (EMR). She submits that although there is no documentary evidence that Nurse B also viewed this information, one of her colleagues reported to her that they had observed Nurse A showing this information to Nurse B on the computer screen. The complainant also submits that another colleague reported to her that she overhead Nurse B and Nurse A discussing the complainant's health information.

[20] The complainant submits that it is clear from the facts that she did not consent to the use of her personal health information by any of these individuals. She states that none of these individuals were providing health care to her, and had no reason to view this information.

[21] The complainant states, with respect to Nurse B, that even if it is found that this individual did not view her health information through the EMR, Nurse B breached the *Act* when Nurse A improperly disclosed it to her verbally.

[22] In response to this complaint, the hospital acknowledges that the specific role filled by Nurse A did not require access to all of the complainant's health information shown in the audit report as having been viewed by this nurse. The hospital also states that its staff did not have training on appropriate access to personal health information for this role. It states that there was lack of clarity within the hospital on the appropriate processes for this role and in response to the complaint, it has documented and standardized its processes. These new processes are now included in the training of nurses for this role.

[23] The hospital states that it trained nurses working in this role on the new processes in August 2017, March 2018 and October 2018. As well, it informed all staff involved with related responsibilities of these changes. Managers reviewed these processes in one-on-one meetings with staff. In its submissions, the hospital states that these events happened some years ago and its privacy and security maturity level has greatly improved since then.

[24] The hospital also submits that its review of the audits indicated that Nurse A used the same process consistently across patients and did not single out the complainant. The hospital concluded, however, that Nurse A had disclosed the complainant's health information without authority, to Nurse B. The hospital advised that, as a result of this unauthorized disclosure and other events unrelated to this complaint, Nurse A received an unpaid suspension of five days and was reported to the College of Nurses of Ontario (the College).

[25] Following these events, the hospital instituted regular audits on Nurse A's activity in its electronic medical records to monitor for appropriate access, and has not identified any further privacy breaches. Nurse A was also provided with additional privacy training, and training on her role. The new processes for this role were included in a learning plan for Nurse A in February 2018.

[26] With respect to the complaint against Nurse B, the hospital reviewed its audit logs

and saw no evidence that Nurse B had accessed the complainant's health record. Nurse B denied having viewed the information, and Nurse A denied having shown it to Nurse B on the screen.

[27] The complainant submits that none of the individuals about whom she complains had her consent to access her personal health information. She states that the hospital's acknowledgements regarding its past processes are not convincing, and that Nurse A should have been aware of her obligations under the *Act*. She submits that the evidence supports her belief that Nurse A accessed her medical record to check on her because Nurse A did not believe her when she reported feeling unwell before going to the emergency department. Among other things, she states that Nurse A accessed her records on a computer normally used by the ICU, and not by her in the discharge of her role, as claimed by the hospital.

[28] The complainant submits that even if the facts show that Nurse A did not single her out, Nurse A would still be in breach of the *Act* given that it was unnecessary to her role, relying on sections 30(2) and 17(2).

[29] With respect to Nurse B, the complainant submits that two witnesses told her that they saw this nurse viewing the screen with her health information, along with Nurse A. She states that the hospital's Privacy Officer refused to interview these individuals. She states that even if it cannot be established that Nurse B accessed her information in this manner, she "used" the complainant's information when Nurse A disclosed it to her.

[30] In reply, the hospital explained, among other things, that Nurse A's use of the ICU computer would not have been inconsistent with her responsibilities on that date, which included acting as the ICU supervisor. It also states that the two witnesses referred to by the complainant were interviewed in the 2016 investigation and the hospital decided it was unnecessary to interview them again. On the basis of the evidence before it, the hospital concluded that there was no solid or objective evidence to support this allegation.

Findings

[31] As indicated above, the hospital has acknowledged that Nurse A's role in February 2016 did not require access to all of the complainant's health records as shown in the audit results. It also acknowledges that its training and documentation in relation to the appropriate use of personal health information for this role were inadequate. Given these acknowledgements, I find that the hospital, through its agent, Nurse A, used more of the complainant's personal health information than reasonably necessary to the purpose of that use, contrary to section 30(2) of the *Act*. The failure to adequately set limits on the use of personal health information appropriate to this role was not in keeping with the hospital's obligations under sections 17(1) and (3), which require it to take reasonable steps to ensure its agents' collection, use and disclosure of personal health information comply with the *Act*.

[32] I make no finding about whether Nurse A was in breach of her responsibilities as an agent, under section 17(2) of the Act. She was not a party to this complaint, and I find it more likely than not that these accesses resulted from a systemic failure to clearly define the role and the use of personal health information appropriate to this role, rather than individual wrongdoing.

[33] I have reviewed the hospital's response to these events and, in particular, the steps it took to document and detail the appropriate use of personal health information for nurses filling the particular role in question, as well as provide training to those nurses. Having regard to these steps, I find it unnecessary to order any additional measures.

[34] With respect to Nurse B, I am satisfied with the hospital's account of its investigation, and its efforts to determine whether Nurse B had also accessed the complainant's health information in the EMR without authority. On the basis of the evidence before me, I have no reason to question the hospital's conclusion that this allegation could not be established. I do not uphold the allegation that Nurse B breached the *Act* when Nurse A verbally disclosed information to her, or the theory that this amounts to an unauthorized "use" of the complainant's personal health information by Nurse B. On the facts before me, the only involvement of Nurse B in this interaction was as a passive receiver of verbal information. The definition of "use" under the Act means to "view, handle or otherwise deal with the information." Beyond the assertion that the receipt of verbal information was a "use", I was given no further argument or authority to suggest that any of these terms apply to the facts before me, and I decline to make such a finding.

ALLEGATION OF UNAUTHORIZED ACCESSES BY MANAGER A

[35] The hospital also investigated the allegation regarding Manager A, and concluded that Manager A's access to the complainant's health record was authorized pursuant to section 37(d) (risk management) of the *Act.* It determined that Manager A accessed the complainant's health record to complete an audit in response to the allegations against Nurses A and B. The hospital states that Manager A viewed the patient care inquiry section of the complainant's chart, which was necessary in order for Manager A to cross- reference who was on staff the night of February 16, 2016, against the audit of the complainant's record.

[36] The hospital explained that Manager A completed the audit because she would be most aware of the activities of her staff (schedules, documentation, necessary data fields for ICU, etc.) and what records staff should and should not have accessed. The hospital noted that the review of audits is conducted by the subject matter expert, with interpretation from the individual who created the audit report.

[37] The hospital also submits that, since these events, it has changed its process for investigating privacy complaints so that managers may not participate in audits of their own staff who are also patients.

[38] The complainant submits that even if Manager A accessed the complainant's medical records for use in the investigation, she was not the appropriate person to conduct the investigation. The hospital's privacy policies state that her obligation was to report the complaint or a privacy breach to the hospital's Privacy Officer for investigation. By conducting her own investigation, she breached the hospital's policy as well as the *Act*.

[39] The hospital accepts that the allegations in February 2016 ought to have been reported to its Privacy Officer, and that the Manager did not comply with the hospital's Privacy Operations Manual (the Manual), which requires breaches or suspected breaches

to be reported to that officer. In this case, the Manager reported the issue to the hospital's human resources department and neither, it appears, reported it to the Privacy Officer. The hospital states that it has reminded the Manager, the human resources department, and other managers of the importance of reporting suspected privacy breaches to the hospital's privacy office.

Findings

[40] This office has found that the investigation of an allegation of a privacy breach is an activity covered by section 37(1)(d) of the *Act*, which permits use of personal health information without consent (see PHIPA Decision 44). Ordinarily, this would dispose of the allegation that Manager A's accesses to the complainant's records were authorized under this section of the *Act*. The hospital has the right and the duty to investigate such an allegation. However, in this case, it is not in dispute that the hospital's Privacy Operations Manual requires that privacy complaints be reported to its Privacy Officer, and it is that individual who is responsible for conducting an investigation and responding to a complaint.[2] It is not in dispute that the allegations should have been reported to that officer in February 2016.

[41] The Manual also states that audits of patient records are the responsibility of the Privacy Officer, who will review and interpret the audit results and follow up with managers. It may well be that this Manager was the best person to review and interpret the audit results, and that the Privacy Officer would have consulted with her (as is permitted under the Manual), as part of an investigation. However, the investigation in 2016 was carried out in a way which was a considerable departure from its Manual. It is not hard to imagine the rationale for the requirement to report privacy complaints to the hospital's privacy office, and for giving overall responsibility for privacy investigations and auditing of patient records to the Privacy Officer. Among other things, such a policy helps to avoid a situation where a privacy complaint itself results in a privacy breach, if any number of managers at the hospital initiate and conduct investigations into potentially sensitive matters without overarching direction.

[42] I conclude that the accesses to the complainant's personal health information as part of the investigation in 2016 were not authorized under section 37(1)(d). That investigation was not sanctioned under the hospital's Manual, and the departure from the Manual was not trivial. I make no finding about whether the Manager (and indeed others involved in the 2016 investigation) were in breach of their duties as agents of the hospital, under section 17(2). They are not parties to this complaint and on the evidence before me, the breach was more of a systemic one, rather than the result of individual wrongdoing.

[43] Given the hospital's actions following these events to remind its managers of the hospital's policies for investigating privacy complaints, I find it unnecessary to order any additional measures.

[2] I was provided with two versions of the hospital's procedures for investigating privacy breaches, one of which appears to have come into force in March 2017. Both versions require that privacy complaints be reported to the Privacy Officer, who has responsibility for conducting the investigation.

ADEQUACY OF THE HOSPITAL'S RESPONSE TO THE PRIVACY COMPLAINT

[44] The hospital's responsibility to investigate and respond to a privacy complaint arises from its obligations under section 12(1) of the *Act*, which 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.

[45] 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.[3]

[46] I have already discussed the hospital's failure to follow its Manual in 2016, in response to the allegations made by the complainant's colleagues. In addition to the fact that the complaint should have been reported to the hospital's Privacy Officer, the complainant submits, rightly, that the failure to follow the Manual also included a failure to notify the complainant once a privacy breach (the verbal disclosure by Nurse A) had been confirmed. In fact, and contrary to its obligations under section 12(2) of the *Act*, the hospital did not make the complainant aware of the unauthorized disclosure of her health information and it was only upon her return to work in 2017 that she learned of this from her colleagues.

[47] The complainant alleges that the Privacy Officer's response to the complaint in 2017 was also deficient. She alleges that his investigation was "biased and incomplete", stating, for example, that he refused to interview the two nurses who originally reported the privacy concern in 2016 and that he provided the complainant with only cursory results of the investigation months after it was completed.

[48] The hospital denies that it "refused" to interview the two nurse witnesses, and states that the Privacy Officer made the decision it was unnecessary, given that the Manager had already interviewed them in 2016. The hospital states that the Officer's investigation in 2017 included interviews with Nurse A, Nurse B, the complainant, and others knowledgeable about Nurse A's role.

Findings

[49] This office has stated that the standard in section 12(1) is "reasonableness". It does not require perfection, and the section does not provide a detailed prescription for what is reasonable.[4]

[50] There were flaws in the hospital's response to the complaint about unauthorized access to and disclosure of the complainant's medical records and, in particular, the initial

[3] PHIPA Decision 44, at para. 140.
[4] PHIPA Decision 44, at para. 141.

investigation in 2016 which occurred outside of its policy for such matters. However, I am satisfied that the hospital's actions ultimately met the standard in section 12(1). In the second investigation, the Privacy Officer reviewed audit results, met with the complainant to review them, and obtained information in order to determine whether individuals shown as having accessed the complainant's records had the authority to do so. The investigation also included interviews with relevant staff. The decision not to re- interview two nurses, a year after the events, does not suggest a lack of impartiality nor an incomplete investigation.

[51] Further, the Privacy Officer's investigation resulted in recommendations aimed at improving the privacy practices of the hospital, which were adopted: formal definition of the role filled by Nurse A and its permitted accesses to patient health information, accompanying training, and a change to the privacy audit processes to avoid having managers involved in the investigation of privacy complaints initiated by their own staff.

[52] I have reviewed the documents provided by the Privacy Officer to the complainant at the completion of the investigation and they do not support the complainant's contention that they provided only "cursory" results. They describe the investigation in some detail, and its outcomes, including informing the complainant about the discipline imposed on Nurse A and changes to the hospital's processes.

CONCLUSION

[53] As described above, I find that the hospital breached the *Act* in using the complainant's personal health information when it was not reasonably necessary to fulfill the purpose for which it was accessed, contrary to section 30(2). It also failed to take reasonable steps to ensure that its agents did not use personal health information contrary to the *Act*, as required by sections 17(1) and (3). I find, on the whole, that the hospital complied with section 12(1) in its response to the breaches. Given the hospital's actions in remedying the deficiencies in its processes and policies, I find it unnecessary to issue any orders.

Original Signed by: July 28, 2021

Sherry Liang
Assistant Commissioner Tribunal